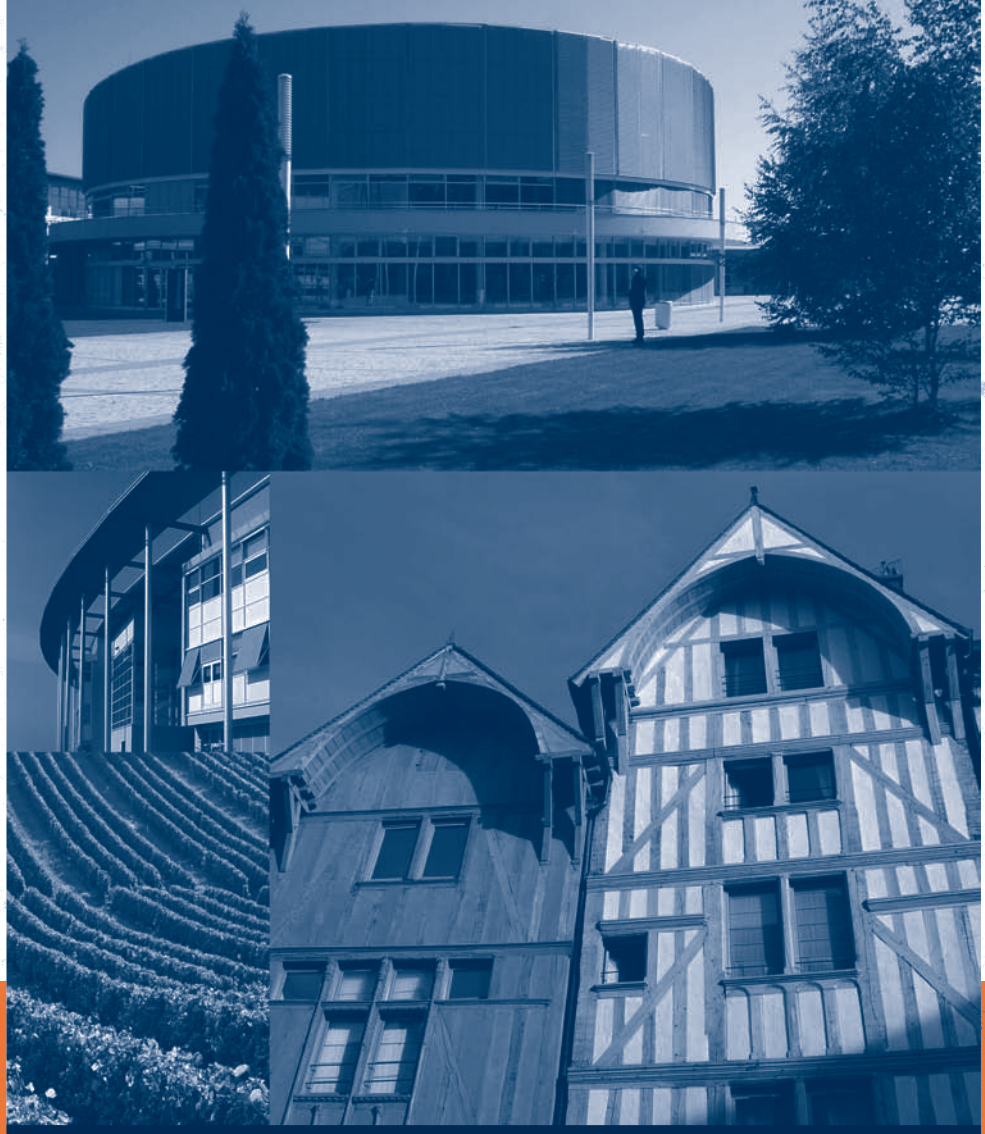
Editors:
Christophe Bérenguer, Antoine Grall & Carlos Guedes Soares



Advances in Safety, Reliability and Risk Management

CRC Press
Taylor & Francis Group
A BALKEMA BOOK

ADVANCES IN SAFETY, RELIABILITY AND RISK MANAGEMENT

This page intentionally left blank

PROCEEDINGS OF THE EUROPEAN SAFETY AND RELIABILITY CONFERENCE, ESREL 2011, TROYES, FRANCE, 18–22 SEPTEMBER 2011

Advances in Safety, Reliability and Risk Management

Editors

Christophe Bérenguer & Antoine Grall
Troyes University of Technology, France

C. Guedes Soares
Instituto Superior Técnico, Technical University of Lisbon, Portugal

CRC Press
Taylor & Francis Group
Boca Raton London New York Leiden

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A BALKEMA BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150226

International Standard Book Number-13: 978-0-203-13510-5 (eBook - PDF)

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Table of contents

System reliability analysis

Critical infrastructures

Energy

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Preface

This book contains the proceedings of the ESREL 2011 Conference, held in Troyes, France and organised by the Université de Technologie de Troyes and the European Safety and Reliability Association (ESRA).

ESREL is a series of annual conferences promoted by ESRA, which dates back to 1989 (in La Baule, France), but was not referred to as an ESREL conference before 1992 (in Lyngby, Denmark). The Conference has become well established in the international community, attracting a good mix of academic and industry participants that present and discuss subjects of interest and application across various industries in the fields of Safety, Reliability and Risk. Being associated with ESRA, it has also become traditional that a small sample of the papers presented at the ESREL Conference will be revised and sometimes expanded and published in a special issue of the Reliability Engineering and System Safety Journal, which is also associated with ESRA.

This conference comes to France for the fourth time (in addition to an earlier one in 1989 in La Baule) but it is the first time that its local organizer is a University, in this particular case in Troyes, just southeast of Paris. *Troyes University of Technology*, established in 1994, has developed undergraduate and graduate programs in reliability and safety engineering and risk management. An important part of the research developed at UTT is organized around "Sciences and Technologies for Risk Management", following a multidisciplinary approach.

This year the theme of the Conference is "Advances in Safety, Reliability and Risk Management". The Conference covers a number of topics within safety, reliability and risk, and provides a forum for presentation and discussion of scientific papers covering theory, methods and applications to a wide range of sectors and problem areas.

This year the Conference programme includes 393 papers from prestigious authors coming from all over the world. Originally, about 543 abstracts were submitted. After the review by the Technical Programme Committee of the full papers, 405 have been accepted to be included in these Proceedings. The effort of authors and the reviewers are a guarantee of the quality of the work.

The review process was mainly organised by the Technical Area Coordinators (most of which are the Chairmen of the ESRA Technical Committees) and the review process was made by a large number of anonymous reviewers which are gratefully acknowledged for their contributions to the improvement of quality of the papers. The members of the Technical Programme Committee (most of them members of the ESRA Technical Committees) have shared a great part of the review process and are important contributors to the Conference organization.

The review process is an important aspect of the Conference and contributes to the fact that this series of Conferences has been included for the last several years in the ISI citation index, which at least to academics is an important feature.

This book contains the extended abstracts and a CD with the full electronic text of the papers presented at the ESREL 2011 Conference, held in Troyes, France. It is the first time that a formal book with extended abstracts is published together with the CD with the full papers, following a transition solution found in 2010. Before 2010, the full papers were published on paper, leading to proceedings that in the last several years were 3 to 4 volumes. Therefore, the present solution will be the one that will probably be in place for some years to come, following the evolution of substituting paper documents by their electronic counterpart.

We hope that this set of papers can be a useful reference for many readers.

Christophe Bérenguer, Antoine Grall
and C. Guedes Soares
Editors

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Conference organization

Conference Chairman

Antoine Grall — UTT – Troyes University of Technology, France

Technical Programme Committee Chairmen

Christophe Bérenguer — UTT – Troyes University of Technology, France
C. Guedes Soares — IST – Technical University of Lisbon, Portugal

Technical Area Coordinators

Ben Ale, The Netherlands
John Andrews, United Kingdom
Piero Baraldi, Italy
Anne Barros, France
Marko Cepin, Slovenia
Eric Châtelet, France
Michalis Christou, Italy
Vincent Cocquempot, France
Valerio Cozzani, Italy
Laurence Dieulle, France
Pieter van Gelder, The Netherlands
Benoit Iung, France
Stig O. Johnsen, Norway
Céline Kermisch, Belgium
Wolfgang Kröger, Switzerland
Pierre-Etienne Labeau, Belgium
Gregory Levitin, Israel
Jana Markova, Czech Republic
Sebastian Martorell, Spain
Tomasz Nowakowski, Poland
Luiz Oliveira, France
Alberto Pasanisi, France
Kurt Petersen, Sweden
Luca Podofillini, Switzerland
Darren Prescott, United Kingdom
Raphaël Steenbergen, The Netherlands
Stefano Tarantola, Italy
Dominique Vasseur, France
Jin Wang, United Kingdom
Elena Zaitseva, Slovakia

Technical Programme Committee

Tunc Aldemir, USA
Olga Aneziri, Greece
Terje Aven, Norway
Pierre Beauseroy, France
Tim Bedford, United Kingdom
Lola Berrade, Spain
Andrea Bobbio, Italy
Emanuele Borgonovo, Italy
Radim Bris, Czech Republic
Bruno Castanier, France
Inma T. Castro, Spain
Nicolas Dechy, France
Pierre Dehombreux, Belgium
Rommert Dekker, The Netherlands
Estelle Deloux, France
Francesco Di Maio, Italy
Phuc Do Van, France
Mohamed Eid, France
Maxim Finkelstein, South Africa
Roger Flage, Norway
Mitra Fouladirad, France
Olivier Gaudoin, France
Rafael Gouriveau, France
Edith Grall-Maës, France
Michel Kinnaert, Belgium
Krzysztof Kolowrocki, Poland
Frédéric Kratz, France
Yves Langeron, France
Pierre Le Bot, France
Mary Ann Lundteigen, Norway
Myriam Merad, France
Sophie Mercier, France
Vincent Mousseau, France
Anne Muller, France
Martin Newby, United Kingdom
Mustapha Nourelfath, Canada
Ioannis Papazoglou, Greece
Christian Paroissin, France

Hélène Pesme, France
Agapios Platis, Greece
Florin Popentiu, Romania
Marvin Rausand, Norway
Antoine Rauzy, France
Emmanuel Remy, France
Claudio Rocco, Venezuela
Michel Roussignol, France
Philipp Scarf, United Kingdom
Mcarmen Segovia, Spain
Christian Tanguy, France
Jean-Marc Thiriet, France
Atoosa P.-J. Thunem, Norway
Harald P.-J. Thunem, Norway
Paul Ulmeanu, Romania
Ingrid B. Utne, Norway
David Valis, Czech Republic
Jorn Vatn, Norway
Zdenek Vintr, Czech Republic
Wenbin Wang, United Kingdom
Enrico Zio, Italy
Athena Zitrou, United Kingdom

Local Organization Committee (at Troyes University of Technology)

Anne Barros
Pierre Beauseroy
Estelle Deloux
Laurence Dieulle
Yann Dijoux
Phuc Do Van
Delphine Ferry
Stéphane Fleury
Mitra Fouladirad
Edith Grall-Maës
Yves Langeron
Ludovic Stiot
Catherine Yendjadj
with the support of the technical and administrative services of Troyes University of Technology

Conference Secretariat (at Troyes University of Technology)

Marie-José Rousselet
Véronique Banse

Plenary Speakers

Erik Hollnagel, MINES Paris-Tech
Philippe Klein, EDF
Way Kuo, City University of Hong Kong

Website Administration

Alexandre Janeiro, Technical University of Lisbon, Portugal

Organized by

Troyes University of Technology – UTT, France
European Safety and Reliability Association – ESRA

Sponsored by

Région Champagne – Ardenne
Ville de Troyes
CNRS – Centre National de la Recherche Scientifique
EDF – Electricité de France
GIS 3SGS
DNV – Det Norske Veritas
Grand Troyes
GDR MACS – CNRS
MAIF

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Acknowledgements

The conference is organized jointly by Troyes University of Technology and ESRA (European Safety and Reliability Association). The Editors would like to thank the many contributors for their active participation which made the organisation of ESREL 2011 possible.

The joint work of the Technical Area Coordinators, the peers involved in the Technical Programme Committee, the reviewers and the organisers of special sessions have resulted in a number of very interesting sessions. Thanks to all the contributors for the participation and effort in the technical programme settling.

The editors would like to thank all the sponsors of ESREL 2011: Région Champagne-Ardenne, Grand Troyes, Ville de Troyes, CNRS, DNV, EDF, GDR MACS, GIS 3SGS, MAIF. The support of all is greatly appreciated.

We would like to acknowledge specially the conference secretariat, all the administrative and technical support at Troyes University of Technology and the local organising committee. Their many hours of work are greatly appreciated. The support to the website was provided by the Instituto Superior Técnico.

Finally the editors would like to thank the authors, session chairs and conference participants without whom there would not have been any conference.

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Introduction

The ESREL 2011 Conference covers a number of topics within safety, reliability and risk, and provides a forum for presentation and discussion of scientific papers covering theory, methods and applications to a wide range of sectors and problem areas.

THEMATIC AREAS

- Bayesian methods
- Crisis and Emergency Management
- Decision Making under Risk
- Dynamic Reliability
- Fault Diagnosis, Prognosis and System Health Management
- Fault Tolerant Control and Systems
- Human Factors and Human Reliability
- Maintenance Modelling and Optimisation
- Mathematical Methods in Reliability and Safety
- Occupational Safety
- Quantitative Risk Assessment
- Reliability and Safety Data Collection and Analysis
- Risk and Hazard Analysis
- Risk Governance
- Risk Management
- Safety Culture and Risk Perception
- Structural Reliability and Design Codes
- System Reliability Analysis
- Uncertainty and Sensitivity Analysis

INDUSTRIAL SECTORS

- Aeronautics and Aerospace
- Chemical and Process Industry
- Civil Engineering
- Critical Infrastructures
- Energy
- Information Technology and Telecommunications
- Land Transportation
- Manufacturing
- Maritime Transportation
- Mechanical Engineering
- Natural Hazards
- Nuclear Industry
- Offshore Industry
- Policy Making and Public Planning

This page intentionally left blank

Thematic areas

Accident and incident investigation

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A preliminary analysis of the 'News Divine' incident

S. Olmos-Peña & J.R. Santos-Reyes
Seguridad, Análisis de Riesgos, Accidentes y Confiabilidad de Sistemas (SARACS), SEPI-ESIME, IPN, México

ABSTRACT

Crowds are common and occur very often in modern society; for example, crowds occur in major sport events, Metro underground transport systems, transport terminals, entertainment events, to mention a few of them. On the other hand, a number of stampedes have occurred worldwide with undesirable consequences in terms of life loss. However, there is very little evidence in the scientific literature regarding human stampedes. Very often, stampedes are reported in the mass media, such as TV news and newspapers; see for example, The New York Times (2000), Perkins (2004), BBC (2004), but to mention a few of them. Also, a number of studies have been conducted on several issues on 'crowd' management (Fruin, 2002; Fang, et al., 2003; Purser & Bensilum, 2001; Pauls, 1980; Gupta & Yadav, 2004; Vassalos, 2004; Daamen & Hoogendoom, 2003; Nelson & MacLennan, 1988).

The paper presents some preliminary results of the analysis of the 'News Divine' human stampede incident that occurred in Mexico City on June 20th 2008. Twelve people were killed by the stampede. The approach has been the application of the Management Over-sight Risk Three (MORT) technique (Frei, et al., 2002). Some preliminary results of the analysis of what happened during the stampede are reported. More work is needed in order to identify the 'management elements' on the why-branch of the MORT tree that contributed to the particular problems identified in the present analysis. It is hoped that by conducting such analysis lessons can be learnt so that incidents such as the case of the 'News Divine' can be prevented in the future.

REFERENCES

BBC. 2004. Scores die in Argentina club fire. BBC News, December 31, 2004. Retrieved from http://news.bbc.co.uk/2/hi/americas/4136625.stm

Daamen W, Hoogendoom. 2003. Controlled experiments to derive walking behaviour. *European Journal of Transport and Infrastructure Research* SP; 3(1):39–59.

Fang, Z., Lo, S.M. & Lu, J.A. 2003. On the relationship between crowd density and movement velocity, *Fire Safety Journal*, 38:271–283.

Frei, R., Kingston, J., Koornneef, F., Van den Ruit, J. & Schallier, P. 2002. *NRI MORT user's manual. For use with the management oversight and risk tree analytical logic diagram*. Noordwijk Risk Initiative Foundation, 2002, AG Delft.

Fruin, J. 2002. The cause and prevention of crowd disasters. *In proceedings of the First International Conference on Engineering for Crowd Safety*, http://www.crowdsafe.com/

Gupta, A.K. & Yadav, P.K. 2004. SAFE-R: a new model to study the evacuation profile of a building, *Fire Safety Journal*, 39: 539–556.

Nelson, H.E. & MacLennan, H.A. 1988. *Emergency movement*. MA, USA:SFPE Handbook of fire protection engineering, NFPA Quincy.

Pauls, J.L. 1980. Effective width model for evacuation flow in buildings. *In Proceedings, Engineering Applications work-shop, Society of Fire Protection Engineers,* 215–232.

Perkins, L.B. 2004. *Crowd Safety and Survival: Practical Event & Public Gathering Safety Tips*. Lulu Press, 2004, USA. Retrieved from http://books.google.com.mx/books?id=e8ThPTakU_0C&printsec=frontcover&source=gbs_v2_summary_r&cad=0#v=onepage&q=&f=false

Purser, D.A. & Bensilum, M. 2001. Quantification of behavior for engineering design standards and escape time calculations, *Safety*, 26: 157–182.

The New York Times. 2000. Gas Attack in Lisbon Nightclub Leaves 7 Dead and 60 Injured. The New York Times, April 17, 2000. Retrieved from http://www.nytimes.com/2000/04/17/world/gas-attack-in-lisbon-nightclub-leaves-7-dead-and-60-injured.html?pagewanted=1

Vassalos, G.C. *Critical review of data available as input to evacuation simulation tools*. MCA research project 490, Task 3.1a, March 2004, pp. 16–8.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Case study: Do activities and outcomes of the process safety observations match?

Marko Gerbec
Jožef Stefan Institute, Department of Inorganic Chemistry and Technology, Ljubljana, Slovenia

ABSTRACT

Paper describes process of implementation of process safety incident investigation procedure in an SME company involved in LPG and technical gases storage and distribution. Realistic resources available at the SME size company were considered in the process of defining an incident investigation process, and main obstacles, approaches and solutions are briefly introduced. Further on, safety activities observations/monitoring in terms of SMS audit (EC, 1996), ARAMIS safety culture (ARAMIS, 2006) and violation motivation (Mason, 1997) surveys results were compared with three incident cases analyzed (safety outcomes) according to the 3CA (Kingston, 2002) and NRI MORT (Frei, 2002) methods.

Summaries of the results of the internal SMS audit carried out by the author, as well as results of both questionnaire surveys on multiple company sites among 58 workers/supervisors are presented.

It was found that there is an issue related to the relationships between safety activities topics categorizations compared to the categorizations selected for safety outcomes and author's interpretations/reflections were needed.

However, generally, deficiencies revealed in activities monitoring were correspondingly found also in incidents caused (and vice versa), subject to suitable categorizations both using 3CA and NRI MORT methods/approaches.

Using 3CA method, from a total 20 Generic Organizational Systems (GOS) 11 were found somehow deficient by at least one incident, six by all three incidents, and four by at least two incidents analyzed. Comparison of the activities (using all three methods/approaches) to the outcomes categories for all three incidents analyzed, revealed that the deficient GOS could be "anticipated" by at least one activity monitoring approach, and eight of eleven by at least two or three approaches.

Using NRI MORT method, similar conclusions were derived, however, MORT proved being more useful in terms of better and precisely defined categories of the deficiencies/root causes/events to be revealed in the incident analysis.

However, "translation" of MORT root causes/events to the related activities methods and related topics/outcomes again remains a difficulty requiring interpretation/reflections by the author (potential cause of some subjectivism).

Details of the analyses carried out are given in the paper in two figures and seven tables.

Thus, empirically in a case study, usefulness of the preventive safety activities (observations) was confirmed. Safety activities and outcome observations, e.g., in terms of the safety culture categories, etc., can be operatively used as safety performance indicators (e.g., OECD, 2008), as well as for planning of the suitable corrective actions by the management.

REFERENCES

ARAMIS Project, 2006. Workpackage 3 - Prevention management efficiency, Deliverable D3B - Annex B (available at: http://mahb.jrc.it/index.php?id=442).

EC, 1996. EU directive 96/82/EC, Annex III, available at: http://mahbsrv.jrc.it/Framework-Seveso2-LEG-EN.html#Annex3.

Frei R., Kingston J., Koornneef F. & Schallier P., 2002. *NRI MORT User's Manual*, NRI-1, ISBN 90-77284-01-X (http://www.nri.eu.com).

Kingston J., 2002. *Control Change Cause Analysis (3CA)*, NRI-3, ISBN 90-77284-03-6, (http://www.nri.eu.com).

Mason S., 1997. Violations - costs, causes and cures. Chapter in F. Redmill & J. Rajan (eds), *Human Factors in Safety Critical Systems*, Butterworth-Heinmann, ISBN 07506 2715 8.

OECD, 2008. Guidance on developing safety performance indicators related to chemical accident prevention, preparedness and response, guidance for industry, OECD Environment, Health and Safety Publications, Series on Chemical Accidents, No. 19, Paris (http://www.oecd.org/dataoecd/6/57/41269710.pdf).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Definition of an algorithm for accident identification

M. Nombela & E. Boix
Applus+ IDIADA, Santa Oliva, Tarragona, Spain

ABSTRACT

Worldwide, 1.2 million people die in road crashes yearly; 43,000 in Europe alone. This implies a cost to European society of approximately 160 billion euros, and takes up 10% of all healthcare resources. To reduce these rates, new active and passive safety technologies which help to minimize the severity of injuries to vehicle occupants have been developed. However, studies have shown that most deaths due to road accidents occur in the time between the accident and the arrival of emergency medical services.

The aim of this study is to define an algorithm (and basically a methodology) which allows the vehicle to recognize when an accident has occurred and what kind of accident has taken place (frontal, side, roll-over or rear-end collision).

The project is based on the idea that each kind of impact shows a "typical" acceleration (lineal or angular) which is specific to each type of accident (frontal, lateral, roll-over, etc.). The methodology developed is based on the recording of the damaged vehicle's acceleration when a collision occurs. To perform this study, a complete database including information of the accelerations in different sorts of collisions is necessary. For each class of vehicle (supermini, small family car, large family car, small MPV, large MPV, executive, roadster sports, small off-road 4 × 4, large off-road 4 × 4, pick-up), accelerations corresponding to the same kind of collision were grouped, and studied in order to define same acceleration patterns. From those patterns, and for each type of vehicle and type of accident, an acceleration characteristic pulse and corresponding thresholds for each scenario (severe/slight accident, no accident) were defined.

The innovative aspects of this methodology are basically that, for each type of accident (frontal, side, rear-end) and for each class of vehicle, a maximum and minimum level of vehicle accelerations (linear or angular) are defined for the SEVERE ACCIDENT, SLIGHT ACCIDENT and NO ACCIDENT scenarios. A direct application of this algorithm could be to include it in an onboard unit on vehicles, and use it in emergency call applications (eCall). eCall devices have been developed to automatically notify emergency services in the event of an accident, in which a fast and efficient rescue operation can significantly increase the chances of survival of the severely injured. In order to reduce response time and improve the efficiency of the medical and technical services, fast and accurate accident identification is required. This on-board algorithm makes it possible to identify the type and severity of the accident allowing emergency services to respond accordingly; and as such could contribute to saving lives.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Feasibility of railway suicide prevention strategies: A focus group study

H. Rådbo, B. Renck & R. Andersson
Faculty of Social and Life Sciences, Karlstad University, Sweden

ABSTRACT

Suicide is a major public health concern, both nationally and internationally. In Sweden, more than 1200 people commit suicide every year, amounting to about 25% of all injury deaths. Five percent of these suicides occur on railways. From a railway safety perspective, suicide constitutes a clear majority (about 75%) of all Swedish railway-related fatalities. Several studies describe the frequency and characteristics of railway suicide in different countries. Some of them also discuss various preventative possibilities. However, fewer studies, if any, analyze and evaluate such strategies in more detail. In Sweden, a comprehensive research program in this field is now underway. The ultimate goal is to develop a set of preventative strategies against railway suicide that can be used by the railway transportation providers themselves, as an integral part of their regular safety work.

The overall goal of this study is to explore preferences for preventative strategies against railway suicide among relevant professional groups. For the above purpose, a focus group approach was chosen. Focus group interview is a qualitative method based on group dynamics intended to gain non-quantitative in-depth understanding of a certain phenomenon, not obtainable from individual interviews. In total, 22 interviewees were selected and divided into four groups. Each interview session began with a brief presentation of the results so far accumulated from the ongoing research programme. Thus, all participants were given a common platform for the discussion. The discussions were centred on railway suicide and possibilities for prevention, with special focus on possible environmental and technical changes in the railway system.

The content analysis resulted in 16 categories, here structured and presented under themes identified through the analysis process. Theme 1: Measures reducing the attractiveness of railway as a means of suicide. Theme 2: Measures obstructing the accessibility to the track area. Theme 3: Measures influencing the victim's determination while awaiting train. Theme 4: Early warning systems, enabling the train to brake sufficiently or the victim to be removed before collision. Theme 5: Measures to make the collision less violent and thereby less fatal and injurious.

Our results show that there is general acceptance and understanding among practitioners of our proposed strategies to prevent railway suicide, although individual participants expressed some scepticism regarding how far one can reach in hindering individuals who are really determined to kill themselves in front of a train. Several concrete proposals were met with optimistic expectation and support.

The results also support the validity of the proposed model for railway suicide prevention. All the principles encompassed by the model were considered relevant, although some of them were perceived to be more realistic than others as regards practical implementation. No major additional categories were identified from the interviews that were not already covered by the model.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Major accidents and their consequences for risk regulation

I.B. Dahle, G. Dybvig, G. Ersdal, T. Guldbrandsen, B.A. Hanson & J.E. Tharaldsen
Petroleum Safety Authority Norway, Stavanger, Norway

A.S. Wiig
Petroleum Safety Authority Norway, Stavanger, Norway
Department of Health Studies, Faculty of Social Sciences, University of Stavanger, Stavanger, Norway

ABSTRACT

The purpose of this paper is to study four major accidents in the petroleum industry and their effects on Health Safety and Environment (HSE) regulatory regimes and lessons learnt at an industrial and company level. Our cases are the following four major accidents: Piper Alpha (1988), Texas City refinery (2005), Montara (2009), and Deepwater Horizon (2010). Criteria for case selection: Accidents of major historical influence, new accidents with an assumed high influence on regulatory approaches and lessons learnt for the industry; Petroleum related accidents and accidents which we have the potential of gaining insights into development of regulatory regimes over time.

Main aims of the paper are to examine implications for HSE regulatory regimes and industrial actors. In the paper we draw upon theories on risk regulation, systemic learning, safety culture and organizational reliability. Our methodological approach mainly relies on literature studies of accident investigation reports, but we have also applied other data material in our study such as written material, documents and documentaries.

The results show that the examined major accidents have had and will most likely still have an impact on regulatory regimes. Changes are being made with regards to risk regulation practices and the organization of safety and energy departments, lessons are tried learnt across industrial sectors and shelves, safety management systems and technological solutions are improved, and higher degree of employee participation and involvement is often called for. Regulatory regimes are often changed from a prescriptive to a goal setting regime, the energy and safety division within the regulatory authority are being separated, safety case regime are being introduced, better formal and informal employee involvement is recommended, improvements of procedural and safety management systems and lessons are learnt with regards to improvement of barriers technical solutions.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Prevention of atypical accident scenarios through the use of resilience based early warning indicators

N. Paltrinieri & V. Cozzani
Dipartimento di Ingegneria Chimica, Universita Bologna, Bologna, Italy

K. Øien & T.O. Grøtan
SINTEF Technology and Society, Safety Research, Trondheim, Norway

ABSTRACT

An "atypical" accident scenario is a scenario deviating from normal expectations and, thus, not deemed credible by common processes of risk assessment. Past experience shows that non identified accident scenarios as such represent a latent risk for industry and society and sometimes their occurrence can lead to consequences of unexpected extent. An evident example of an atypical accident was the major accident occurred at Buncefield on 11th December 2005. A detailed analysis of this and other cases in literature has shed some light on the complexity of their causal factors, demonstrating that an atypical major accident is not only the consequence of a single uncommon event, but rather the final result of deficient background conditions, such as the organizational failures represented in Figure 1.

Thus, it has been a big challenge to foresee combinations of such failures and corresponding unidentified accident scenarios. Two complementary approaches to deal with this challenge are: i) improved identification of atypical scenarios, to reduce the occurrence of unforeseen events; ii) improved early detection, to reduce the possibility of remaining unforeseen events leading to an accident. For this reason the Resilience based Early Warning Indicator (REWI) (Øien et al., 2010) method has been considered in this contribution. In fact, the concept of resilience refers to the capability of recognizing, adapting to, and coping with the unexpected and one of its key characteristics is the interaction and interchange between different (organizational) system layers, levels, and focal points. The REWI method allows to establish a set of early warning indicators on the basis of issues of contributing success factors (CSFs) being attributes of resilience. The main aim of this work is to show the preliminary results of the application of this method to the site at Buncefield

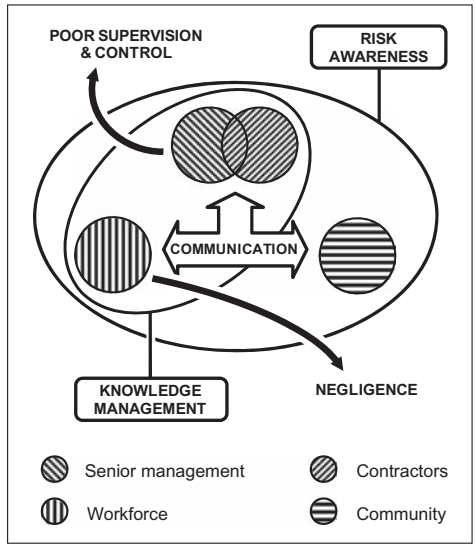


Figure 1. Scheme of organizational failures collected in the analysis of the accident at Buncefield (Paltrinieri et al., 2010).

Table 1. Resilience based early warning indicators for a Buncefield-like oil depot referring to the CSF "Anticipation".

CSF Anticipation—Indicators	
1	Portion of operating personnel participated in HAZID
2	Fraction of operational procedures that have been risk assessed
3	No. of reviews of safety reports in the last 5 years
4	Fraction of internal past events considered in safety report review
5	Fraction of external past events considered in safety report review

(Tab. 1), obtained by adapting the candidate set of REWI indicators to the oil depot characteristics and defining new indicators on the basis of the accident causes. In this way it has been also possible to understand the relevance of these resilience based indicators as early warnings of the atypical scenario and to demonstrate, by the correspondence of the defined indicators with the accident causes, that this major accident would have been likely prevented by the application of the REWI method.

REFERENCES

MIIB – Buncefield Major Incident Investigation Board 2008. The Buncefield Incident 11 December 2005, Final Report, HSE Books.

Øien K., Massaiu S., Tinmannsvik R.K. & Størseth F., 2010a, Development of Early Warning Indicators based on Resilience Engineering, PSAM 10, June 7–11 2010, Seattle, USA.

Paltrinieri N., Wardman M., Dechy N., Salzano E. & Cozzani V., 2010, Atypical major hazard scenarios and their inclusion in risk analysis and safety assessments, Proceedings of the European Safety and Reliability Conference, ESREL 2010, Rhodes, Greece.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Suicide and the potential for suicide prevention on the Swedish rail network: A qualitative multiple case study

H. Rådbo, I. Svedung & R. Andersson
Faculty of Social and Life Sciences, Karlstad University, Sweden

ABSTRACT

Suicide prevention deserves urgent attention. In Sweden, with a population of about 9 million, 1200–1400 individuals commit suicide annually, with about 5% of these events occurring on railways. Although the leading railway safety problem today (in terms of human loss) in many European and other countries, suicide is still a surprisingly neglected aspect of railway safety, and very little research is carried out on the problem. However, there is now a growing interest in the field and increasing attention is being paid to the suicide issue in railway safety circles. In Sweden, the Swedish National Rail Administration, has initiated a research program to achieve a broader understanding of the suicide problem in connection with the railway system and of the possibility of applying a systems-oriented approach to preventing railway suicide.

The aim of this study is to evaluate the content of existing reports on railway suicide incidents from a preventive perspective and to identify and categorise additional preventive-oriented information obtainable from independent site investigations.

This study is based on all police-reported cases of railway suicide (22 cases in total) during 2003–2004 in a defined geographical area. Data on each case were also collected from standard reports by the Swedish National Rail Administration (Banverket). In addition, all sites were visited for complementary data collection, resulting in both written and photographic documentation.

There are both similarities and differences between the police and rail administration reports. The two organizations record information regarding background data on the victim and train involved, as well as the place and time of occurrence. Location characteristics are important for the identification of features favouring the choice of a certain place for suicide. Our analysis points to common traits in terms of conditions offering seclusion. Among our 22 cases, it is obvious that most victims sought seclusion for their final preparation.

In summary, neither police, nor railway administration reports include many of the relevant details for the prevention of suicide on the Swedish Railways. There is major uncertainty regarding the exact time and place of the occurrence, and little or no information on victim behaviour and other circumstances preceding the collision is given, with the exception of the last few seconds as observed by train drivers.

Structured in-depth investigations of railway suicide incidents may contribute considerably to the learning process regarding this phenomenon and how it can be prevented. To improve railway safety, more detailed information on the behavioural, technical and environmental circumstances characterising railway suicide incidents needs to be systematically collected and analysed on a regular basis.

Bayesian methods

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

An AHP-based approach of risk analysis in Bayesian belief networks

Bin Xie
Gexcon AS, Bergen, Norway

Jørn Vatn
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

The aim of this paper is to present a new approach to integrate expert judgments into Bayesian Belief Networks. An approach is proposed for updating the conditional probability tables (CPT) when new soft evidence is obtained from expert judgment exercises. In the elicitation of beliefs from the experts, elements of the Analytic Hierarchy Process (AHP) are applied to reduce the work load.

A section of BBN is shown in Figure 1. CPT, for node X for the various combinations given parent nodes, will contain m columns and p rows.

Let Ci represent the ith combination of the parent vector of X. Element a_{ij}, $1 \le j \le m$, $1 \le i \le p$, in the CPT is the probability that X takes the jth value given the ith combination of the parent vector. The objective is then for each combination, Ci, to use the expressed knowledge by the experts to update a_{ij}.

Similar pairwise comparison in AHP is created in the following likelihood matrix. Let A_1 represents the situation that X takes the first value given C_1, A_2 represents the situation that X takes the second value given C_1 and so on. Matrix **A** is denoted with i as the row index, and j as the column index. Let b_{ij} represent $\Pr(X = A_i|C_1)/\Pr(X = A_j|C_1)$, $i,j \le m$, $i \ne j$. The diagonal elements equals 1 and $A_{ij} = 1/A_{ji}$.

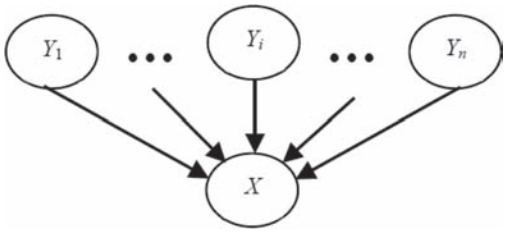


Figure 1. Section of the BBN for demonstration of the update in the CPT.

$$A = \begin{array}{c} \\ A_1 \\ A_2 \\ \bullet \\ \bullet \\ \bullet \\ A_m \end{array} \begin{array}{c} \begin{array}{cccccc} A_1 & A_2 & \bullet & \bullet & \bullet & A_m \end{array} \\ \begin{pmatrix} 1 & b_{12} & \cdots & \cdots & \cdots & b_{1m} \\ \frac{1}{b_{12}} & 1 & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & 1 & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & 1 & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & 1 & \cdots \\ \frac{1}{b_{1m}} & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix} \end{array}$$

The principal eigenvectors corresponding to pairwise comparisons in this approach are explained and discussed as the "relative likelihood". This is different from the "relative importance" already known in AHP. Moreover, not only is the consistency ratio of judgments within an interval demonstrated by AHP, but it can contribute to weighting. To combine expert judgments, an iterative process is carried out to create the "updated belief". In addition, computational procedures can be simplified with the Matlab code. A case study of the hydrogen vehicle explosion is shown to illustrate the direct instruction of this approach. This comprehensive methodology can be applied to any industrial case to improve risk analysis.

REFERENCES

Saaty, T.L. 1988. The Analytic Hierarchy Process., McGraw-Hill, New York.

Saaty, T.L. 2000. Fundamentals of Decision Making with the Analytic Hierarchy Process. Pittsburgh, *PA: RWS Publications*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An optimizational resource allocation method for series system reliability life test

Qi Liu, Xiaoyue Wu & Jianrong Ding
College of Informational Systems and Management, National University of Defense Technology, Changsha, P.R. China

ABSTRACT

Testing and demonstrating the system's reliability is often a costly and difficult undertaking. And sometimes, because of the constraints of cost and available products, cannot reach at a desirable target. To series system which all the subsystems have life time and follow exponential distributions, a Probability Constraint Programming Model for Life System (PCPMLS) is proposed for the verification of system failure rate. In PCPMLS, a statistical hypothesis of system's failure rate is constructed, the null hypothesis is that system's failure rate should be equal or greater than a given value. The objective of PCPMLS is to minimize the total reliability test cost. In PCPMLS, the total reliability test cost is supposed to be a linear function of subsystems' (system's) sample sizes and test durations. Considering the principle of small-probability event and reliability test requirement, the constraint conditions include posterior probability of null hypothesis should be equal or greater than a given confidence level, every subsystem (system) life test duration should be equal or greater than its given minimize test duration and be equal or less than another given maximum test duration, and single product's reliability test duration shouldn't be longer than its given longest test duration.

In order to make full use of the prior information of subsystems and system, the Bayesian Optimum Resource Allocation Model (BORAM) is developed to calculate the prior distribution of system's failure rate and posterior probability of null hypothesis. By BORAM, under the assumption of all subsystems are independent and exponential distributed, the expectation and variance of system's failure rate are deduced. Under the assumption of subsystems' prior distributions and actual test results are the only sources of system's prior information, the moment method is used to calculate the hyper-parameters of the prior distribution of system's failure rate. And, to given actual system's reliability test result, the posterior probability calculation formula is given, and it is the function of subsystem's (system's) actual test results and hyper-parameters of subsystems' prior distribution.

Because subsystems' (system's) reliability test durations are continuous variables, so it is impossible to list all the possible values of each variable and calculate all the possible posterior probability of null hypothesis, then find the optimum resource allocation plan. The grid based numerical algorithm (GBNA) for the solution of resource allocation plan is introduced to find the satisfactory solution. GBNA splits the solution space into small grids. The intersecting points of different grids are treated as temp feasible solutions. The purpose of GBNA is to find an optimum solution from all the temp feasible solutions, and based on the optimum solution, construct another solution space, and so on, the optimizational solution can be found out. Under the assumption that every subsystem (system) has no failure during its reliability test, the initial test plan calculation steps were given. And considering the possible failure during reliability test, the calculation method of sequential test plan was given.

At last, considering a rocket engine, it consists of one thrust chamber (subsystem 1), one tank (subsystem 2), a feed mechanism (subsystem 3), a power source (subsystem 4), suitable plumbing or piping (subsystem 5), a structure (subsystem 6), and control devices (subsystem 7). The rocket engine is supposed to be series system, every subsystem (system) reliability test results are exponential distributed, and all subsystems are independent. For given constraint conditions, prior distributions of subsystems' failure rate, initial test costs, unit product test costs and unit time test costs of subsystems (system), the initial test plan calculation process is presented, and the optimizational initial test durations are carried out. Compare with other test plan, it is obvious that the optimizational test combination is the optimum test plan which satisfies the constraint conditions and its test cost is the lowest one.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Assessing risk based on Bayesian networks and FMECA: A case study

L.M. Pedersen & M.H. Saltnes
Safetec Nordic, Norway

ABSTRACT

In this paper a Bayesian network-based method, used to assess the fire risk in relation to a product installed in houses, is presented. The paper uses a new approach where the Bayesian belief network (BBN) model is based on a failure mode, effect and criticality analysis (FMECA). The node probabilities in the BBN are determined from the frequency classes and consequence classes defined in the FMECA. The goal was to obtain knowledge of the risk affect of installing a product, as well as providing decision support on risk reducing measures.

Knowledge of the fire risk for a product for installation in or on houses was needed in order to minimise the risk of fire, fatalities and damage to property. Furthermore, if the product catches fire and the fire propagates to the house, the reputation of the product and the producer will be damaged and the producer may be held responsible for death of people. Hence, the producer had a request for increased knowledge of the magnitude of the fire risk and how the risk can be reduced before manufacturing the product for sale. As the product is to be integrated in houses, a larger amount of combustible material will be present than for earlier products not integrated in houses. The complexity of the fire risk is due to where the fire arc and heating may appear in addition to a wide variety of combustible materials that may be present. The method used for the original case is presented by application on a simplified case.

An FMECA was performed on the product to identify 1) where the ignition points could be and 2) where the combustible material may appear. Fire may appear when combustion material is close to ignition points. FMECA is not suitable for identification of combinations of failures, such as combinations of ignition and combustible material. A BBN model was therefore developed to explain the combinations between ignition sources and presence of combustible material that may initiate a fire. The frequency classes and severity classes from the FMECA were used to set the probability on each of the nodes in the Bayesian network. The model calculates the probability of initiated fire based on background knowledge and the assumptions made in the analysis by the specialists.

FMECA is a systematic method to identify possible failure modes of a system and their effect on the system, but FMECA is not suitable for identification of combinations of failures. However BBN modelling is well suited for analysing the combinations between failures such as in this example.

The method presented in this paper uses FMECA to identify possible failures and uses BBN to analyse the combinations of these failures. This method is useful when performing an FMECA and the analysis identifies combinations of failures that may be dangerous and must be further analysed. The method is also useful when performing a BBN without accurate input data. An FMECA could then be a good method to estimate classes of failure rates to use as input data.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Bayesian network for decision making on ageing facilities

P.A.P. Ramírez & I.B. Utne
Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ABSTRACT

Extension of the design lifetime of ageing installations has become a crucial issue for several oil and gas (O&G) companies. Even though large repairs and modifications may be required, keeping in operation the existing installations beyond the design lifetime will often be economically advantageous. A major concern regarding the life extension of the facilities is that safety and regularity should not be compromised. This can be achieved by implementing ageing management programmes to control and mitigate the degradation of the facilities (Brurok et al., 2010). Ageing management comprises physical ageing, obsolescence, and human and organisational issues (Petersson 2006). This paper focuses on physical ageing, which deals with degradation of systems, structures and components (SSCs).

An effective management of ageing includes assessing the actual condition of the SSC and deciding what actions must be taken for ensuring safe and cost effective operation of the SSC. Usually, four possible alternatives can be considered for handling SSCs subject to ageing (Hokstad et al., 2010): (i) use-up (i.e. using the equipment until the end of service life), (ii) refurbishment (i.e. the existing equipment is overhauled and restored with old technology), (iii) replacement, and (iv) modification. In addition to these alternatives, other measures can be taken for controlling or mitigating the ageing of the SSCs, such as increasing the preventive maintenance, improving the condition monitoring, and changing the operating conditions. Therefore, these measures may also affect the final decision. The objective of this paper is to introduce a procedure for applying Bayesian Networks (BN) to support decision making about equipment subject to physical ageing, taking into account the factors that influence the safety, production assurance/availability and costs.

The paper describes the procedure for developing and applying the BN model using historical data and expert knowledge. The application of the model consists of five main steps: i) customization of the BN, ii) specification of the variables, iii) quantification of the strength of the relationships, iv) utilization of the model for analysing the alternatives selected, and v) ranking of the alternatives. The utilisation of the model is based on analysing different alternatives and ranking them according to their effectiveness. The effectiveness of the alternatives is calculated with respect to safety, availability and costs. A simplified example of a heat exchanger is used to illustrate the application of the model.

The model proposed improves the basis for the decision making with respect to ageing management of SSCs, and ensures that important factors are not unintentionally omitted during the analysis. In addition, the results of the BN can be tracked back; hence the variables that affect negatively the technical performance of a component and the safety can be identified and improved.

The work is carried out as part of the Gassco Research Programme on Ageing Management together with MARINTEK. Further work includes a full case study using the BN model on equipment installed in an O&G facility.

REFERENCES

Brurok, T., Valland, A., Rødseth, H., Åhren, T., Ramstad, L.S., Gibson, A., Ose, G.O., Brembo, J.C., Onsøyen, E. & Dyrkoren, E. 2010. Gassco Ageing Management Programme, Internal work and reports (confidential). MARINTEK, Trondheim.

Hokstad, P., Håbrekke, S., Johnsen, R. & Sangesland, S. 2010. *Ageing and life extension for offshore facilities in general and for specific systems*. SINTEF, Trondheim.

Petersson, L. 2006. *Ageing of components and systems: An ESReDA working group report*. Det Norke Veritas, Norway.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Comparison of fault tree and Bayesian Networks for modeling safety critical components in railway systems

Q. Mahboob
Pakistan Railways Lahore, Pakistan

D. Straub
Engineering Risk Analysis Group, TU München, Germany

ABSTRACT

Modern railway systems are equipped with automatic signaling as well as Train Protection and Warning Systems (TPWS) that control train movement and ensure the attention of the driver. In spite of reliable signaling and TPWS, trains are still passing red signals. These so-called SPAD events can lead to train derailment, head on collision with another train, collision with infrastructure and other adverse consequences. Investigations have been carried out to identify the critical components that lead to SPAD and subsequent train derailment. The classical way of modeling such events is by means of Fault Tree (FT) analysis. However, the FT methodology has limitations when modeling complex systems, which motivates the investigation of using Bayesian Networks (BN) for modeling and analyzing SPAD and other safety critical events in railway systems.

BN allows combining systematic, expert and factual knowledge about the system and is a flexible and compact form of system representation. In this paper, it is studied whether the use of BN provides significant advantages over the FT methodology for the railway systems. The causes of train derailment due to SPAD are analyzed and the safety risk model for train derailment due to SPAD is constructed using FT and then translated into the BN shown in Figure 1. The two methods are compared with respect to different modeling and analysis aspects that are relevant for railways.

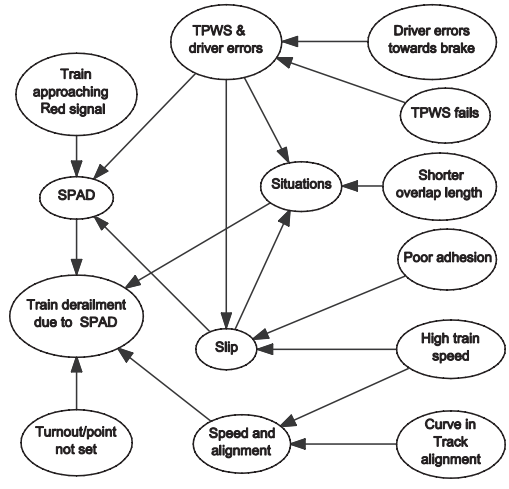


Figure 1. Bayesian Network for train derailment due to SPAD.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Establishing prior probability distributions for probabilities that pairs of software components fail simultaneously

M. Kristiansen
Østfold University College, Remmen, Halden, Norway

R. Winther
Risikokonsult, Oslo Area, Norway

B. Natvig
Department of Mathematics, University of Oslo, Norway

ABSTRACT

One possible way to assess and include dependency aspects in software reliability models is to find upper bounds for probabilities that software components fail simultaneously and then include these into the reliability models. In Kristiansen, Winther & Natvig 2011, a Bayesian hypothesis testing approach for finding upper bounds for probabilities that pairs of software components fail simultaneously is described in detail. This approach consists of two main steps: 1) establishing prior probability distributions for probabilities that pairs of software components fail simultaneously and 2) updating these prior probability distributions by performing statistical testing. In this paper, the focus is on the first step in the Bayesian hypothesis testing approach, and two procedures for establishing a prior probability distribution for the simultaneous failure probability q_{ij} are proposed. Both procedures consist of two main steps, the first step being common for both of them.

1. Establish a starting point for q_{ij} based on a transformed beta distribution.
2. Adjust this starting point up or down by applying expert judgement on relevant information sources available prior to testing.

In the first procedure, the prior probability distribution for q_{ij} is determined by letting experts adjust the initial mean and variance of q_{ij} in the transformed beta distribution based on relevant information sources. In the second procedure, the prior transformed beta distribution for q_{ij} is adjusted numerically by letting experts express their belief in the total number of tests and the number of simultaneous failures that all relevant information sources correspond to.

The main motivation for establishing a prior probability distribution for q_{ij} is to utilise all relevant information sources available prior to testing in order to compensate for the enormous number of tests which is usually required to satisfy a predefined confidence level $C_{0,ij}$. In the case where reasonable prior information is available, the number of tests which mustbe run to achieve $C_{0,ij}$ can be greatly reduced.

Both procedures assume that relevant information sources can be assigned values in the interval [0, 1]. A value close to 0 can for example indicate substantial difference in development methodologies, great diversity between development teams or low complexity of the interface between the software components. On the other hand, a value close to 1 can for example indicate use of identical development methodologies, extreme complexity of the interface between the software components or that components are developed by the same development team. The idea is that the larger (closer to 1) the values of the relevant information sources I_i are, the larger is the mean for the simultaneous failure probability in the first procedure and the number of simultaneous failures in the second procedure.

REFERENCE

Kristiansen, M., Winther, R. & Natvig B. (2011). A Bayesian Hypothesis Testing Approach for Finding Upper Bounds for Probabilities that Pairs of Software Components Fail Simultaneously. *To appear in International Journal of Reliability, Quality and Safety Engineering (IJRQSE)*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Parameter estimation in a reservoir engineering application

A.M. Hanea
Institute of Applied Mathematics, Delft University of Technology, The Netherlands

M. Gheorghe
iBMG / iMTA, Erasmus University Rotterdam, The Netherlands

ABSTRACT

Reservoir simulation models are used not only in the development of new fields, but also in developed fields where production forecasts are needed to help make investment decisions. When simulating a reservoir one must account for the physical and chemical processes taking place in the subsurface. Rock and fluid properties are very important when describing the flow in porous media.

In this paper the authors are concerned with estimating the permeability field of a reservoir. The problem of estimating model parameters such as permeability is often referred to as a history matching problem in reservoir engineering.

Currently, one of the most widely used methodologies which address the history matching problem is the Ensemble Kalman filter (EnKF) (e.g. (Aanonsen, Naedval, Oliver, Reynolds & Valles 2009; **?**)). EnKF represents the distribution of a system state using a collection of state vectors, called an ensemble. EnKF is a Monte-Carlo implementation of the Bayesian update problem. The Bayesian update is combined with advancing the model in time, incorporating new data when available. Traditional EnKF requires the assumption of joint normality. Moreover, when the size of the ensemble used is much smaller than the size of the state vector, unreal/spurious correlations between variables may be noticed. Given the dimension of the reservoir engineering applications, this is often the case. The methods used to eliminate spurious correlations introduce other inconsistencies in the modelled system. Considering these limitations of the EnKF method, a new approach based on graphical models is proposed and studied.

The graphical model chosen for this purpose is a non-parametric Bayesian network (NPBN) (Hanea 2008). A NPBN consists of nodes which represent random variables and arcs which represent direct dependencies among the variables. The arcs of a NPBN are associated with conditional copulae (Joe 1997). These conditional copulae, together with the one-dimensional marginal distributions, and the conditional independence statements implied by the graph uniquely determine the joint distribution, and every such specification is consistent. Inference in NPBNs also uses the Bayesian update. If the NPBN does not depend on time it is called a static NPBN. For time series modelling a dynamic NPBN (Hanea 2009) is more appropriate. One can interpret a dynamic NPBN as instances of a static NPBN connected in discrete slices of time. The data provided by the reservoir model at a given time is represented as a static NPBN. Production data is used to update the joint distribution of the variables of interest. The new joint distribution is modified further in time using the reservoir model. In this way, the reservoir model provides the connection between discrete slices of time and data is assimilated at every time step by conditioning the joint distribution on the values of the measurements.

The NPBN based approach will be compared with the EnKF method. A two phase, 2D flow model was implemented for a synthetic reservoir simulation exercise and the results of both methods for the history matching process of estimating the permeability field are illustrated and compared.

REFERENCES

Aanonsen, S., Naedval, G., Oliver, D., Reynolds, A. & Valles, B. (2009). The Ensemble Kalman Filter in Reservoir Engineering. *SPE Journal*.

Hanea, A. (2008). *Algorithms for Non-parametric Bayesian belief nets*. Ph. D. thesis, TU Delft, Delft, the Netherlands.

Hanea, A. (2009). *Tackling a Reservoir Engineering Problem with a NPBN Approach*. Lecture notes, Summer School on Data Assimilation: Section 3.

Joe, H. (1997). *Multivariate Models and Dependence Concepts*. London: Chapman & Hall.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability based design of engineering systems with monotonic models

M. Rajabalinejad & C. Spitas
Department of Engineering Design, Delft University of Technology, Delft, The Netherlands

ABSTRACT

A computationally efficient Bayesian Monte Carlo for Monotonic (BMCM) models for reliability based design of engineering systems is described in this paper. The model employs Gaussian distribution and monotonicity principles that have been implemented in the Dynamic Bounds (DB) method (Rajabalinejad 2009) integrated with a Bayesian Monte Carlo (BMC) technique. Signficant improvements in the computational speed of coupled DB and BMC methods are realized by incorporating a weighted logical dependence between neighboring points of the limit-state equation (LSE) as prior information and global uncertaintiy concept for quantifying variations of the controlling input variables. The outcomes of preceding simulations are factored in subsequent calculations to accelerate computing efficiency of the Monte Carlo method. The theory and numerical algorithms of the BMCM are described in this paper, and extension of the BMCM to multi-dimensional problems is provided.

The DB and BMC techniques are combined and used in this research to assess reliability of e engineering systems. We investigate in this paperpotential merits of using Gaussian distribution with monotonic models in reliability engineering. The system parameters can be classified as control and noise factors. The controlgroup includes parameters that can be controlled by designer. Those that are difficult or expensive to control are the noise factors. In this paper, a statistical decision theory is applied to increase the performance by integrating different types of prior information. This motivated the development of an approach that could take advantages of DB and BMC methodsusing monotonic models. Since the Gaussian distribution is widely used in engineering to characterize variations of system parameters, it is implemented in the proposed approach for error modeling. For acceptable accuracy levels in reliability assessment works, the proposed modeling approach for calcualting failure probabilities of systems and components is shown here to substantially reduce computational simulation effort. The likelihood of each parameter set is employed to generate a probability distribution of each parameter and the covariance among parameters. These distributions are utilized to estimate uncertainty in model predictions.

The theoretical formulation and numerical implementation details of a novel Bayesian interpolation method for a monotonic models are provided in this paper. The proposed modeling approach is an integrated model that employs a Bayesian interpolation, a Gaussian density function and the DB method to efficiently calculate an unbiased estimate of failure probability of complex structural systems. The proposedmodeling approach also includes a new concept that relates global and local uncertainties (Rajabalinejad 2009). With these features, this novel approach makes it possible to obtain an unbiased estimatesusing the Monte Carlo methods. This integrated approach preserves fundamental properties of the classical MC method, while it greatly improves the computational efficiency by using prior information in a monotonic limit state equation (Rajabalinejad and Mahdi 2010).

REFERENCES

Rajabalinejad, M. (2009). *Reliability Methods for Finite Element Models*. Amsterdam, the Netherlands, IOS Press.

Rajabalinejad, M. and Mahdi, T. (2010). "The inclusive and simplified forms of Bayesian interpolation for general and monotonic models using Gaussian and Generalized Beta distributions with application to Monte Carlo simulations." *Natural Hazards* 55(1): 29.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Towards a Bayesian Network methodology to improve maintenance of complex semiconductor systems

M.F. Bouaziz & E. Zamaï
G-SCOP, Grenoble INP, Grenoble, France

S. Monot & F. Duvivier
PROBAYES, Montbonnot, France

S. Hubac
ST Microelectronics, Crolles, France

ABSTRACT

Today, it is a well-known fact that the evolution of microelectronics is characterized by an intense competitive environment between manufacturers in different regions of the world. The semiconductor industry must be able to produce Integrated Circuit (IC) with reduced cycle time, improved yield and enhanced equipment effectiveness. Besides these challenges IC manufacturers are required to address the products scrap and equipment drifts in a complex and uncertain environment which otherwise shall severely hamper the maximum production capacity planned. The study presented in this paper is supported by European project IMPROVE (Implementing Manufacturing science solutions to increase equiPment pROductiVity and fab pErformance). This project includes several industrial partners such as ST Microelectronics, Austria Micro Systems, LFoundry; industrial solution providers as Probayes Company and academic partners such as G-SCOP laboratory, EMSE-CMP school … It aims to improve European semiconductor fabs efficiency by providing methods and tools to act in complex and uncertain contexts.

The objective of this paper is to propose a generic method to develop a model to predict the Equipment Health Factor (EHF) which will define decision support strategies on maintenance tasks to increase the semiconductor industry performance. Firstly, this paper presents a literature review about maintenance and risk analysis methods. Giving the system characteristics, Bayesian Network techniques are the special focus in this paper. BNs are capable of modeling causal dependency even if information are imperfect or missing and could incorporate the expert judgments (Murphy 2002). Then, a methodology (Figure 1) to develop a model is proposed. The EHF model is based on statistic and probabilistic calculations. Following the proposed methodology, industrial case study benchmarked on a semiconductor manufacturing industry is performed. It led us to design prototypes

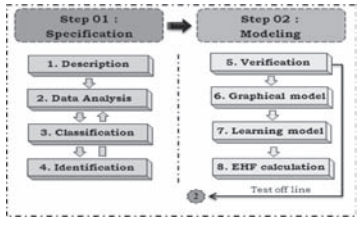


Figure 1. Proposed methodology.

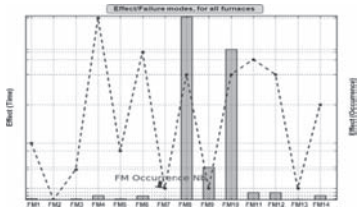


Figure 2. Failure modes frequency.

of data extraction and processing which allow identify the potential Failure Modes (Figure 2) and instantiate the first Bayesian models. EHF results allow appropriate decisions on the preventive maintenance to avoid unscheduled equipment down. So, EHF results are elements of decision support and it can be further used to improve the reliability of manufacturing processes, optimize maintenance tasks (Bouillaut et al., 2008) and increase the production equipment availability.

REFERENCES

Bouillaut, L. Leray, P. Aknin, P. François, O. & Dubois, S. 2008. Dynamic Bayesian Networks Modelling Maintenance Strategies: Prevention of Broken Rails. WCRR'08 World Congress on Railway Research. Séoul.

Murphy, K. 2002. Dynamic Bayesian Networks: Representation, Inference and Learning. Phd, University of California, Berkeley, USA.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Work time loss prediction by exploiting occupational accident data

E.C. Marcoulaki, I.A. Papazoglou & M. Konstandinidou
System Reliability and Industrial Safety Laboratory, NCSR "Demokritos", Athens, Greece

ABSTRACT

According to EUROSTAT (2007) 3.2% of workers in the EU-27 had an accident at work during a one year period, which corresponds to almost 7 million workers. Manufacturing, which covers a large portion of industrial production, is third in the ranking of occupational activities in what concerns the accidents rate. Among workers who had an accident, 73% reported lost work days after the most recent accident, and 22% reported time off that lasted at least one month. Hence, due to an accident at work, 0.7% of all workers in the EU-27 took sick leave for at least one month.

Some of these accidents require several days leave before the worker recovers and can return to work. Clearly, work time losses are directly related to financial losses for the company. Work time loss estimations cannot be based only on the number of accidents, since the total loss is a function of accident frequency as well as accident severity. For instance, accidents resulting to very minor injury may be dealt within the company premises with negligible loss of work time.

The present work considers Bayesian models for the prediction of work time losses due to occupational accidents occurring in an industrial workplace. Meel & Seider (2006) developed a Bayesian approach to estimate the dynamic probabilities of accident sequences, tailored to chemical industries, and applied it on the analysis of incident databases. Marcoulaki et al. (2011) applied these tools to investigate the frequency of equipment failures and occupational accidents in Greek industrial sites.

Bayesian inference methods are hereby used for the analysis of occupational accidents recorded in accident databases, to derive probability distributions for the prediction of:

i. the number of accidents occurring over a given time period in a company workplace
ii. the duration of the recovery period following an accident
iii. the percentage of time that the workers are recovering from accidents, so they are unavailable to perform the work they are paid for.

The paper discusses the analytical models for calculations (i) and (ii). Worker unavailability statistics are derived considering a two-state stochastic model, with the use of Monte Carlo simulations.

The Bayesian models are updated using available evidence from real accident data. The derived posterior distributions embed knowledge on the system, model its future behavior, and support predictions for accident occurrences and durations, and work time loss. The sufficient statistics for the models include accident occurrences and their recovery times, as these are recorded in the company databases. The present analysis is based on 140 non-fatal accidents, which occurred at two major petrochemical companies in Greece (Konstandinidou et al., 2006).

Large sites, where more accident reports are available, enable more accurate predictions of their future behavior. The opposite holds for sites with fewer employees, when the number of recorded accidents is poor, and/or if the period of observation is short. Ongoing research considers the development of more advanced Bayesian models, able to integrate data collected at different sites.

REFERENCES

EUROSTAT: Labour Force Survey 2007 ad hoc module on accidents at work and work-related health problems, EUROSTAT publication 63/2009.

Konstandinidou, M., Nivolianitou, Z., Markatos, N. & Kiranoudis, C. 2006, Statistical analysis of incidents reported in the Greek Petrochemical Industry for the period 1997–2003, *Journal of Hazardous Materials*, A135, 1–9.

Marcoulaki, E.C., Konstandinidou, M. & Papazoglou, I.A. 2011. Dynamic failure assessment of incidents reported in the Greek Petrochemical Industry. *Computer-Aided Chemical Engineering*, accepted for publication.

Meel, A. & Seider, W.D. 2006. Plant-specific dynamic failure assessment using Bayesian theory, *Chemical Engineering Science*, 61, 7036–7056.

Crisis and emergency management

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Functional safety requirements for active protection systems from individual and collective risk criteria

J.E. Kaufman & I. Häring
Fraunhofer Ernst-Mach-Institut, Efringen-Kirchen, Germany

ABSTRACT

Active protection systems are designed to protect vehicles against impact threat, e.g., from high-speed armor-piercing kinetic energy projectiles, shaped charges, explosively formed projectiles or improvised devices. Active protection systems provide an essential addition to the protection spectrum, hitherto made up of passive and reactive protection (e.g., armor). Active protection systems can be classified into three categories according to the distance from the vehicle that the incoming threat is physically intercepted and mitigated: close-in, middle-range and far-range. In any case, an active protection system intercepts an incoming threat prior to the threat is making contact with the outer surface of the vehicle platform.

Using an on-board computer system and sensors, approaching threats are detected, tracked, classified and then mitigated if found to be a critical threat. In particular, in the event of interception of close-in threats in an urban setting, the question arises which safety requirements have to be fulfilled to avoid unintended functioning, possibly resulting in casualties.

The paper presents a general approach that applies to any hard-kill active protection system that has to react in a very short time without assuming specific technical system details. Figure 1 shows the top-view of a vehicle outfitted with an active protection system consisting of n separately deployable countermeasures (singular: CM, plural: CMs). This two-dimensional representation enables a quantitative risk assessment for persons located within the dangerous area of one or more CMs. The term countermeasure, CM, as used in the paper, is a conceptual unit of the physical mechanism that intercepts an incoming threat. Each CM_i has a corresponding dangerous area, which is depicted by a rectangle labeled DA_i, $1 \le i \le n \in \mathbb{N}$. The CMs are assumed to be arranged on the vehicle, possibly with some spacing between adjacent CMs or superposed. For the purposes of generality, the direction of action of the CMs is arbitrary but fixed for a given system. Modern systems are capable of responding to threats having a large range of speeds, as low as 100 m/s in the case of RPG-7, up to over 2000 m/s for EFPs (Walters and Zukas 1989), (Haug and Wagner 2009).

The presented approach determines the overall functional safety requirements of a generic active protection system by evaluating individual and collective risk quantities. Annual individual risk and collective risk, i.e., F-N curves, were utilized. If critical risk values are given, respectively, the necessary overall reliabilities of the functional safety functions are determined. We discuss alternative derivations of the requirements and their implicit assumptions. We show which requirements have to be fulfilled in typical scenarios and propose ranges for critical values as appropriate.

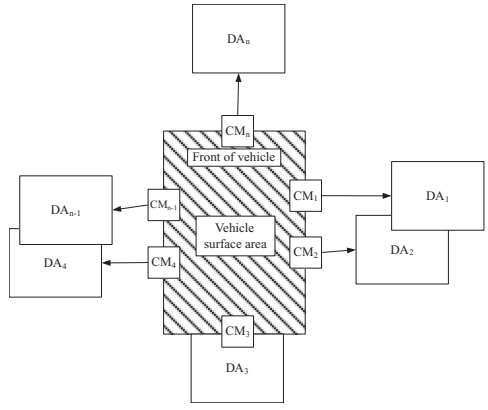


Figure 1. Top-view of vehicle equipped with n CMs. Each CM_i has its own dangerous area DA_i.

REFERENCES

Haug, D. & Wagner, H.J. (2009). Active Hardkill Protection Systems. Defence Technology Review: 38–42.

Walters, W.P. & Zukas, J.A. (1989). *Fundamentals of Shaped Charges*. New York City, John Wiley and Sons, Inc.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

How the use of modelled scenarios can improve risk awareness and risk control in complex environments

J.M. Hagen, B.O. Knutsen, T. Sandrup & M. Bjørnenak
Norwegian Defense Research Establishment, Norway

1 INTRODUCTION

Modelled scenarios depict how a variety of incidents occur and the ways in which preparedness is challenged. In these scenarios, both security and safety issues are addressed, and the timeline is stretched through the phases "crisis preface", "crisis peak" and "post crisis normalization". We developed 20 modelled scenarios which can be further analysed and used for table top exercises and for crisis management and emergency preparedness planning, including evaluation and exercises with particular weight upon analysis of the latter. The use of scenarios contributes to increased security and safety awareness, assisting researchers in identifying mitigating measures and enhanced risk control. The paper presents the applied method for developing such modelled scenarios.

Systematizing the feedback received from senior advisors at Norwegian Ministries of government revealed a low awareness of rare disasters. First we found that risk awareness varies among the different Ministries. Common threats are perceived to be more relevant as compared with more spectacular and rare threats. We also found that the perception of relevance varied among the different Ministries. Since this scenario package was in particular developed to trigger civil-military co-operation and to invite to cross-sector co-ordination, we found, surprisingly enough, that the Ministry of Defence did not see the relevance of more than just every fourth scenario, while the Ministry of Justice saw the relevance of just about half of the scenarios.

Furthermore, dilemmas were encountered regarding scenario quality versus the ethical challenges and risks of displaying and thereby compromising national vulnerabilities. We also found that modelled scenarios can contribute to raising risk awareness and aid in extending the mental perception of threats among the different actors. The aim has therefore been to enhance a broader understanding of the threats that should also form the baseline in any risk analysis. The modelled scenarios can also be used for table-top exercises and workshops with the aim of analysing emergency preparedness and collaboration needs across sectors.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Interdependency-based approach of complex events in critical infrastructure under crisis: A first step toward a global framework

Babiga Birregah & Anne Muller
CREIDD, UMR STMR, University of Technology of Troyes, France

Eric Châtelet
LM2S, UMR STMR, University of Technology of Troyes, France

ABSTRACT

One of the major challenges in the management of critical infrastructures under major crisis is that complexity is intimately coupled with emergence of intrinsic properties. Any disturbance, even insignificant, can lead to widespread and compound crisis when some conditions are met. In most cases, accidents are modelled as a chain of discrete events which occur in a particular temporal order. The principle of domino effect, introduced by Heinrich in the 1940's (Ferry 1988), has been used successfully in relatively simple systems for losses caused by failures of physical components or human errors. One other aspect for an efficient application of domino effect assessment is that the chosen events must be easy to handle and model. In addition, these models are sometimes limited to some complex systems (Hollnagel, Woods & Leveson 2006). The reasons can be the subjectivity or the incompleteness in the selection of the events and the conditions. Systemic approach of accident in critical infrastructures reveals that it is necessary to take into account not only the succession of events, trigged by specific conditions, but also their "combinations". These events combinations involve the interdependencies between the subsystems of the system. In this paper we define a critical infrastructure as a complex interconnected system of sub-systems (CI-SoS) connected by dependencies such as geographical, physical, cyber and logical—these last dependencies are usually called "functional" in risk assessment (Du-denhoeffer, Permann & Manic 2006, Rinaldi, Peeren-boom & Kelly 2001, Briš, Soares & Martorell 2009). We propose that the critical events, observed at the system level, must be regarded as complex events (CE), which actually result from the "combination" of interrelated elementary events (EE) that occur in the subsystems. Since it is still complicated to define how complex events emerge in critical infrastructures, we propose an attempt that uses an interdependency-based approach to determine the manner in which elementary events are combined to lead to complex events. To do so we associate to each interdependency a set of operators that will help us to translate the combination of events into rules. These rules take then the form of equations using interdependency operators such as "implication", "mitigation", "aggregation", etc. The latter approach is then illustrated on a simple case study concerning fire emergency introduced in (Muller 2010). This case study constitutes the first step toward a global framework.

REFERENCES

Briš, R., Soares, C. & Martorell, S. (2009). *Reliability, Risk, and Safety: Theory and Applications*. Number vol. 1. CRC PR INC.

Dudenhoeffer, D., Permann, M. & Manic, M. (2006). CIMS: a framework for infrastructure interdependency modeling and analysis. In *Proceedings of the 38th conference on Winter simulation*, pp. 478–485. Winter Simulation Conference.

Ferry, T. (1988). *Modern accident investigation and analysis*. Wiley.

Hollnagel, E., Woods, D. & Leveson, N. (2006). *Resilience engineering: concepts and precepts*. Ashgate.

Muller, A. (2010). *Développement d'une méthode de modélisation pour l'évaluation de la performance de stratégies de mise en sécurit incendie dans les bâtiments*. Ph. D. thesis, Universit de Haute-Alsace.

Rinaldi, S., Peerenboom, J. & Kelly, T. (2001, December). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems Magazine, IEEE 21*(6), 11–25.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Learning decision making: Some ideas on how novices better can learn from skilled response personnel

M. Sommer
University of Stavanger, Stavanger, Norway

ABSTRACT

Decision making is a critical task of crisis and emergency management, and it is widely acknowledged that the response personnel's decision making during a response is important for the outcome. Learning to make adequate decisions in operational, high-risk settings is essential in developing competence and professional capability. Naturalistic Decision Making has contributed to new and better understanding of decision making in operational environments. This perspective focuses on experienced personnel operating in real life settings, trying to understand how people make decisions under time-pressured, stressing, risky, and dynamic situations.

Even if commanders and leaders normally undergo formal training and education, "on-the-job" training appears to be invaluable and decisive in development of expertise in decision making (Flin & Arbuthnot, 2002). According to experienced practitioners (Lloyd & Somerville, 2006), "real learning" occurs when novices engage in actual practice, giving the novice access to information through physical practice, actual experiences and provision of information offered by experienced personnel.

To improve learning processes and performance, areas for learning, how information is made available and accessed, and individuals' embodiment, must all be part of the analysis (Sommer & Njå, 2011). By using a combined approach to learning (combining socio-cultural elements and individual aspects) novices can better get access to and acquire skilled person's "wisdom".

There are two major challenges related to learning from skilled response personnel. The first challenge is that skills in situation assessment, and decision making in general, mainly rely on intuition and tacit knowledge. The second challenge is to present information (feedback, instructions, explanations, etc.) to novices in such a way that they can utilize it.

The key to understand how skilled persons think (and see/understand situations) is to make explicit the critical cues that guide them and the judgements they make. But, because skilled person's performance largely relies on intuition and tacit knowledge, imparting their knowledge is not an easy task. As a first step to better impart skilled person's knowledge, both skilled persons and novices have to acknowledge that skilled persons know more than they can express clearly. Second, and more crucial, the novices themselves have to be active in "pulling out" information from skilled persons. When doing this, the focus should mainly be on the situation assessment.

To better impart knowledge from skilled response personnel, and to help novices develop decision making abilities, both individual aspects and socio-cultural elements need to be considered. Debriefs should be arranged after responses, and the context surrounding these debriefs must promote dialogue and interaction. In addition, debriefs need to reveal the critical cues that guide the skilled persons and the judgments they make. To structure debriefs and storytelling, Endsley's (1995) model of situation awareness may be helpful to use as a guide. Asking questions according to this model's three phases will help clarify *why* skilled persons do as they do.

REFERENCES

Endsley, M.R. (1995). Toward a theory of situation awareness in dynamic systems. Human factors, 37(1), 32–64.

Flin, R. & Arbuthnot, K. (2002). Incident command: tales from the hot seat. Aldershot: Ashgate.

Lloyd, A. & Somerville, M. (2006). Working information. Journal of Workplace Learning, 18(3), 186–198.

Sommer, M. & Njå, O. (2011). Learning amongst Norwegian fire-fighters. *Journal of Workplace Learning*, accepted for publication.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Performance evaluation of organizational crisis cell: Methodological proposal at communal level

D. Lachtar & E. Garbolino
Crisis and Risk Research Centre, Mines ParisTech, Sophia Antipolis, France

ABSTRACT

Crisis management has become an essential activity for all public and private organizations. It is most often based on a specific tool called "crisis cell" which aims to implement precautions of anticipation, vigilance and intervention to meet the targets.

In 2004, the French state established a legislation to modernize the civil defence to organize and manage crises (Bill to modernize the civil security, Senate, N°277). This law allows a municipality to establish a crisis cell to protect people and safeguard the environment.

However, these plans do not guarantee optimal performance of crisis units. Crisis cells may become particularly vulnerable, and unable to fulfill their missions according to the event.

The estimation of the decisions consequences in a risky situation will be delicate because of the complexity of urban land in question (physical structure, networks, etc.) and environment on which these decisions must be taken.

This fact underlines the importance of the implementation of a comprehensive approach for decision making, particularly on indicators ensuring an effective management of emergencies in terms of space and time.

The objective of this paper is to present a methodology for the analysis of the vulnerability of the crisis cell and assess the performance of crisis management at the municipal level.

The performance is defined as a weakness, tenderness, defect or flaw in a defense system that might endanger the integrity of this system and what it protects, under the action of internal or external constraints (Wybo 2010).

The methodology developed in this paper is primarily based on systems thinking. The systemic approach aims to understand and simulate the operations of the crisis management, including the interactions between actors which are complex. This model describes the functions and resources of communal safeguard plan. It represents an approach particularly suited to understand the behaviour of a system. This model is also applied to give a formal reflection frame in order to analyse the potential failures of the crisis cell.

The proposed methodology includes five steps: observations, systemic exploration, risk analysis, qualitative modeling and simulation. The steps will be detailed in the article.

This subject is a research project on the systems approach to formalize the decision in an emergency situation within a complex urban area. It is subsidized by a shcolarship from the PACA (Provence-Alpes-Côte d'Azur) Region with the partnership of CRC (Centre for Research on Risk and Crisis) and security centre of a French city. The objective of this paper is to present a methodology for the analysis of the vulnerability of the crisis cell and assess the performance of crisis management at the municipal level.

This methodology is a decision support toolbox that can be used to help the managerial decisions and/or guide decision-making processes in organized systems.

REFERENCES

Wybo, J.-L. (2010). « L'évaluation de la vulnérabilité à la crise: le cas des préfectures en France », Télescope, vol. 16, n° 2, pp. 173–193.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Quantitative approach of organizational resilience for a Dutch emergency response safety region

J.M.P. van Trijp
Libertas in Vivo v.o.f., Utrecht, The Netherlands

M. Ulieru
University of New Brunswick, Fredericton, NB, Canada

P.H.A.J.M. van Gelder
Delft University of Technology, Delft, The Netherlands

ABSTRACT

Resilience is an important concept to determine how well a Dutch Emergency Response Safety Region behaves under stress. The main objective of this study is to determine the intrinsic value "Resilience". It is concluded that according to literature the concept of "Resilience" can be best described by the generic approach "Operational Resilience" and is defined as: -The ability of an organization to prevent disruptions in the operational process from occurring; -When struck by a disruption, being able to quickly respond to and recover from a disruption in operational processes. The following four items from literature are derived: Situation Awareness (***awa***); Management of Keystone Vulnerabilities (***kv***); Adaptive Capacity (***ac***) *and* Quality (***q***).

A large scale survey among safety stakeholders in The Netherlands was conducted where those items were explored. The function of Resilience on the defined items can be described as:

$$f(R_{ero}) = R_{ero}(R_{awa} + R_{kv} + R_{ac} + R_q + \varepsilon) \quad (1)$$

where R_{ero} = Resilience of Dutch Emergency Response Safety Region; R_{awa} = Resilience is a function of Awareness; R_{kv} = Resilience is a function of Keystone Vulnerabilities; R_{ac} = Resilience is a function of Adaptive Capacity; R_q = Resilience is a function of Quality; and ε = unspecified data and items which are also a function of Resilience. $f(R_{ero})$ may also be defined as Dynamic Operational Resilience as it dynamically describes the actual state of resilience of the organization.

Stolker (pp. 46, 2008) uses a Value Tree based on the Multi-Attribute Utility Theory (MAUT) developed by Goodwin & Wright (2004) to measure the resilience index which may be considered similar to the postulated Dynamic Operational Resilience index. MAUT uses so called "Utility Values" which measures performance of the respective attributes which are part of the resilience items. A value tree may be constructed (Van Trijp, 2010). When adding Utility Values (***UV***) to equation (1) equation (2) may be derived:

$$f(R_{ero})_{UV} = (R_{ero})_{UV}\,(R_{awa} + R_{kv} + R_{ac} + R_q + \varepsilon)_{UV} \quad (2)$$

where $f(R_{ero})_{UV}$ = Unique Dynamic Operational Resilience of an Emergency Response Safety Region; and UV = Utility Value. It is clear from the designed Value Tree Maximum Achievable Dynamic Operational Resilience is reached when all Utility Values equal 1.00.

When ε is nullified:

$$f(R_{ero})_{max} = \mathbf{22.31\ AU} \quad (3)$$

where $f(R_{ero})_{max}$ = Maximum Achievable Dynamic Operational Resilience.

Hence, it is concluded the postulated equation calculating the Unique Dynamic Operational Resilience index presents a quantitative approach of organizational resilience for a Dutch Emergency Response Safety Region

REFERENCES

Goodwin, P. & G. Wright. 2004. *Decision Analysis for Management Judgment*, John Wiley and Sons, Chichester.

Stolker, R.J.M. 2008. *A generic approach to assess operational resilience*; Technische Universiteit Eindhoven (TUE). Capaciteitsgroep Quality and Reliability Engineering (QRE), Eindhoven.

Van Trijp & John. 2010. An attempt to quantify resilience of emergency response organizations - results from a large scale survey among safety stakeholders in the Netherlands, Master thesis Delft TopTech/Delft University of Technology, Delft, Netherlands; published by Libertas in Vivo v.o.f., Utrecht, Netherlands.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Security incidents and subsequent adaptations of disaster response in complex humanitarian emergencies

B.I. Kruke
University of Stavanger, Stavanger, Norway

ABSTRACT

Humanitarian workers in complex emergency areas face an increasing number of security challenges in their daily operations. Mark Duffield (1994) defines a complex emergency as "*a major humanitarian crisis of a multi casual nature that requires a system wide response*". Russell R. Dynes calls this a conflict disaster (2004). Thus, the lack of security in complex emergencies may put humanitarian workers at risk, and thereby influence humanitarian operations. Responses to security challenges vary to a great extent from emergency to emergency, and from agency to agency. The same is the case with how agencies work to understand the security situation in the emergency area. Where military forces invest a substantial part of their operations in assessing the current situation in the emergency area, humanitarian agencies do not have similar capacities.

This paper highlights four topics on security and humanitarian operations in complex emergency areas. Firstly, what is the trend on attacks on humanitarian workers? We learn from newspaper articles and reports from the field of security related incidents directed towards humanitarian workers. However, we need a more thorough understanding of the size of the problem and also of who are targeted. Secondly, how is security assessments and operational security decision-making conducted across the aid sector? Thirdly, are local organisations and people involved in security assessments? The locals normally have a good understanding of the situation in their neighbourhood. They may at the same time be in a very exposed position. Fourth, how do humanitarian agencies adapt their responses to the security situation in complex emergency areas?

The paper draws on some of the latest developments on security incidents and subsequent humanitarian adaptations in disaster response. The article also draws on experiences gained by the author especially during fieldwork in South Darfur in 2005, but also in Khartoum in 2007.

The paper concludes that an increasing number of security incidents have a massive impact on humanitarian operations. The responsibilities to protect humanitarian workers, the humanitarian agencies security systems, and the tools on how to assess the security situation in conflict areas are in place. All the same, we have seen a trend of increased attacks on aid workers, and in particular on local staff and partners. Thus, humanitarian agencies must balance the humanitarian impact of their operations in conflict areas with the duty to take care of staff and partners.

Stricter security regulations and remote management are humanitarian agencies' responses to incidents directed towards humanitarian workers. These approaches may be criticised for several reasons: 1) Increased involvement of local staff and partners pose an ethical dilemma because they are put at risk when international staffs are withdrawn; 2) A dynamic environment in conflict areas increases the need for field-level presence to assess the situation and to maintain an updated threat profile. The higher the organisational risk the higher the levels involved in the decision-making process. However, decision-makers at higher hierarchical levels need updated information from the field to conduct reliable decision-making. Thus, remote management and stricter security regulations may worsen the potential for risk assessments as foundations for reliable decision-making; 3) Relations with local actors and communities must be cultivated to obtain the consent and security guarantees of the various parties of the conflict.

Thus it is a need to continue and to speed up a process of professionalization of humanitarian agencies on how to continuously assess and handle security threats at field level in complex emergency areas. Remote management and stricter security regulations may worsen the potential for risk assessments as foundations for reliable decision-making to adapt to the dynamic situation and needs at field level.

This page intentionally left blank

Decision making under risk

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A guidance for implementing decision-aiding in risk management

F. Beaudouin
EDF R&D, Chatou, France

M. Merad
INERIS, Verneuil-en-Halatte, France

ABSTRACT

The justification of decisions in risk management is of paramount importance. How to rank risky actions or making tradeoffs between conflicting objectives are typical questions? Addressing such questions entails stringent basis in order to gain confidence and acceptance from decision-makers or stakeholders. However, decision-aiding is often confused with and reduced to a problem of assessment. The pivotal principle of "bounded rationality" due to H. Simon helps to understand that decision-aiding cannot be reduced to a problem of optimization: a decision process encompasses indeed additional tasks that are often overlooked. The purpose of this paper is to establish a complete canonical model that provides guidelines to the decision-analyst. It falls into five steps ranging from 'stating and framing the problem' to 'working out a recommendation'. The kernel of the canonical model relies on two main tasks: 'choosing the paradigm and building the model' and 'eliciting subjective information', though often disregarded.

As far as risk management is concerned, the uncertainty that impacts consequences of actions raises the following difficulty: how to take into account the nature of assessments (i.e. in particular the property of scales) and process it in a consistent manner? It is up to the analyst to grasp properly the context and implement appropriate models to represent and elicit subjective information (judgmental information, tradeoffs, attitude towards risks). This paper shows therefore that resorting to techniques from decision-aiding and economics of risk is here valuable.

Elements of guidance are based on the authors' experience as practitioners. They are exemplified through two full-scale cases experienced at EDF and INERIS. The first case consists in choosing investments of prevention facing uncertainty of outcomes and multiple conflicting objectives, for hydropower plants. According to Roy' taxonomy, it amounts to a ranking problem. This case inspired by the American School of Decision-Aiding is based on the multiattribute utility paradigm. It is best suited to allocate resources with respect to risks. In this frame, risks are represented by discrete random variables on each criterion. The second case (sorting problem) aims at assigning geographical zones exposed to mining subsidence hazards, to ordered classes of risks. This case inspired by the European School of Decision-Aiding, is based on the 'outranking' paradigm. Risks are here modeled as multidimensional vectors endowed with properties of ordinal or interval scales.

It is noteworthy that the canonical model provides a relevant framework of analysis that is independent of the paradigms considered. When dealing with risks, elements of guidance are of crucial importance to avoid the so-called 'black box' syndrome.

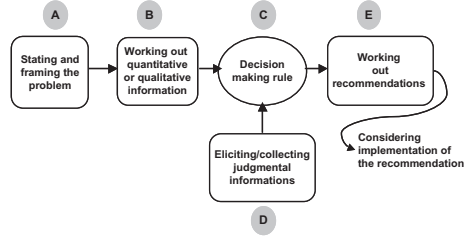


Figure 1. Canonical description of the decision-aid method.

REFERENCES

Beaudouin, F., Munier, B. & Serquin, Y. 1997. Multiattribute utility theory: towards a more general framework, proceedings of the ESReDA Seminar on Decision Analysis and Its Applications in Safety and Reliability.

Keeney, R.L. & Raiffa, H. 1976. Decision with multiple objective: preferences and value tradeoffs, Wiley, New York.

Merad, M., Verdel, T., Roy, B. & Kouniali, S. 2004. Use of multi-criteria decision-aids for risk zoning and management of large area subjected to mining-induced hazards. Tunnelling and Underground Space Technology. Volume 19, Issue 2, March 2004, Pages 125–138.

Roy, B. & Bouyssou, D. 1993. Aide Multi-criteria à la Décision: Méthodes et Cas. Paris, Economica, 695 pages.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Dealing with uncertainties in long term investment planning of electricity distribution systems with distributed generation

M.D. Catrinu, M. Istad & D.E. Nordgård
SINTEF Energy Research, Trondheim, Norway

ABSTRACT

This paper discusses the uncertainties in electricity distribution system investment planning for integrating small-scale generation units (distributed generation- DG) in low and medium voltage electricity networks.

Traditionally, distributions systems where intended for unidirectional power flow to connect end-users and the main uncertainty in planning was related to electricity demand estimation (in terms of location, timing of new connections and load).

This situation has changed dramatically the last 15 years or so when the amount of renewable distributed generation increased tremendously due to countries commitments to cut greenhouse emissions by using all available renewable resources, including small scale energy generation potential. This trend is expected to continue as the technologies for small scale renewable power production are advancing and becoming more affordable.

In Norway, the main part of DG are small scale hydro (from kW to 10 MW)—which are being built by private actors owning the rights to a small river or waterfall suitable for installation of a DG unit. The DG-units will often be located in remote places with a relatively weak electricity grid, with low local load and long distances to the main grid. Distribution companies have through their network license an obligation to connect all distributed generation units to the network, assuming that certain requirements are fulfilled. Network reinforcements are often necessary to integrate the DG units without compromising network power quality.

The presence of distributed generation changes the way distribution systems should be planned and built. With such a rapid increase in the number of distribution generation units being installed in some networks, planners need proactive and robust planning techniques.

REFERENCES

Coster, E.J., Myrzik, J.M.A., Kruimer, B. & Kling, W.L. 2011. Integration Issues of Distributed Generation on Distributed Grids. *Proceedings of the IEEE* 99(1): 28–39.

Dugan, R. & Price, S. 2005. Including distributed resources in distribution planning. *Electricity Distribution, 2005. CIRED 2005. 18th International Conference and Exhibition on.*

EPRI 1999. Technical Assessment Guide - Distributed Resources: DRAFT REPORT. EPRI Licensed Material.

Hammons, T.J. 2008. Integrating renewable energy sources into European grids. *Electrical Power and Energy Systems* 30: 462–475.

Hatziargyriou, N., Asano, H., Iravani, R. & Marnay, C. 2007. Microgrids - An Overview of Ongoing Research, Development, and Demonstration Projects. *IEEE power & energy magazine* July/August 2007.

Kouvelis, P. & Yu, G. 1997. *Robust discrete optimization and its applications*. Dordrecht, The Netherlands, Kluver Academic Publishers.

Martinez, J.A., de León, F. & Dinavahi, V. 2010. Simulation tools for analysis of distribution systems with distributed resources. Present and future trends. *Power and Energy Society General Meeting, IEEE*.

Mendez, V.H., Rivier, J., de la Fuente, J.I., Gomez, T., Arceluz, J., Marin, J. & Madruga, A. 2006. Impact of distributed generation on distribution investment deferral. *Electrical Power and Energy Systems* 28: 244–252.

Pecas Lopes, J.A. 2002. Integration of dispersed generation on distribution networks - impact studies. *In Power Engineering Society Winter Meeting, 2002. IEEE* 1: 323–328.

Pecas Lopes, J.A., Hatziargyriou, N., Mutale, J., Djapic, P. & Jenkins, N. 2007. Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities. *Electric Power Systems Research* 77: 1189–1203.

Pepermans, G., Driesenb, J., Haeseldonckxc, D., Belmansc, R. & D'haeseleer, W. 2005. Distributed generation: definition, benefits and issues. 33(Energy Policy): 787–798.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Forming risk clusters in projects to improve coordination between risk owners

F. Marle & L.A. Vidal
Ecole Centrale Paris, France

ABSTRACT

Projects are facing an ever-growing complexity, with more and more interdependencies between its elements, and thus its risks. Since project risks have increased in number and criticality, lists thus need to be broken down into smaller, more manageable clusters. Classical clustering techniques are generally based on a single parameter, like risk nature, criticality or ownership. Risk interactions are therefore not properly considered when building up clusters. That is why our objective is to group risks so that the interaction rate is maximal inside clusters and minimal outside. This will facilitate the communication and coordination between the actors who are committed in the management of the project and its risks.

In this paper, we propose to capture the potential interactions between project risks by a mix of expertise and experience. Then, we propose an algorithm based on the combined use of heuristics and optimization software in order to propose a configuration that maximizes the objective while respecting the constraints. Finally, we propose an application to a real project.

The first constraint of the optimization problem is the size of the cluster, that is to say the maximum number of risks inside a cluster. But, depending on the assignment of actors to risks, we may have for the same number of risks n between one and n different risk owners, which does not have the same sense and the same implementation difficulty. This paper thus focuses on the addition of a constraint on the number of different owners inside each cluster. It shows how the addition of this constraint enables to propose meaningful and operationally realistic clusters, regarding not only the interaction rate between risks but also the relationships between risk owners. Indeed, it has to be noted that the clustering decision involves human group management, since the people behind the risks will make meetings or task forces or phone calls to coordinate their decisions related to the risk(s) they own.

Finally, we test the sensitivity of the solution to the parameters of the decision-maker, while including or not of this additional constraint and while making this constraint vary within a pre-determined interval.

The originality of this work is to suggest to decision-makers an organization which is complementary to the existing one, and which enables risk owners to coordinate their decisions with people they may not have been in touch with given the current communication paths through the existing project organization.

KEY REFERENCES

Chen, S.-J., & Lin, L. (2003). Decomposition of interdependent task group for concurrent engineering. Computers and industrial engineering.

Eckert, C., Clarkson, J. & Zanker, W. (2004). Change and customisation in complex engineering domains, *Research in Engineering Design* 15:1–21.

Edmonds, B. (1999). Syntactic measures of complexity, in faculty of arts. Ph.D. Thesis. University of Manchester: Manchester.

Eppinger, S., Whitney, D., Smith, R. & Gebala, D. (1994). A model-based method for organizing tasks in product development. Research in Engineering Design, (6): pp. 1–13.

Marle, F., Vidal, L.A. & Bocquet, J.C. (2010). Interactions-based risk clustering methodologies and algorithms for complex project management. *International Journal of Production Economics*, In Press, Accepted Manuscript, Available online 7 December 2010, doi:10.1016/j.ijpe.2010.11.022.

Schaeffer, S.E. (2007). Graph clustering Computer Science Review I, 27–64.

Simon, H. (1981). The Sciences of the artificial. Cambridge The MIT Press.

Steward, D. (1981). The Design Structure Matrix: a method for managing the design of complex systems. IEEE Transactions in Engineering Management, 28(3): pp. 71–74.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

On the use of value of information measure in decision making—A drilling jar case

J.T. Selvik
University of Stavanger and IRIS (International Research Institute of Stavanger), Norway

H.P. Lohne
IRIS (International Research Institute of Stavanger), Norway

T. Aven
University of Stavanger, Norway

ABSTRACT

A decision problem is considered in which it is questioned whether to collect some further information prior to making the decision. The information relates to aspects of cost, benefits and uncertainties. A common tool used for meeting this challenge is the Value Of Information (VOI) measure. This tool compares the costs of the acquisition to the added expected utility (or expected monetary value) produced by a specific improvement of the decision basis. The purpose of the present paper is to discuss the use of the VOI measure in a decision making context. To what extent does this measure provide an adequate decision making basis?

A case from the oil and gas industry, a drilling jar case is used to illustrate the discussion. The drilling jar case relates to possible reliability testing before making a decision on which jar to select for a tender. A standard VOI analysis is performed using a relatively simple model based on expected monetary values to assess the optimal jar alternative for this tender. The limitations of using the results for decision support are discussed, and an extended VOI decision process is suggested. The process highlights that uncertainty assessments should be conducted that see beyond the probabilistic analysis. The VOI results alone are not sufficiently informative to guide the decision maker on which jar to choose. However, placed in the wider process, also involving managerial review and judgements, the VOI measure may provide useful support to the decision making.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Performance-based fire safety—risk associated with different designs

H. Bjelland & O. Njå
University of Stavanger, Stavanger, Norway

ABSTRACT

Fire safety in buildings is based on long traditions with prescriptive regulations and prescribed solutions. A prescribed solution is to be understood as a building design concept that fulfills the minimum requirements in the building regulations. Such solutions are generally based on previous experience with fires and building traditions. After major fires, measures were introduced into the regulations to prevent the experienced consequences in future fires, i.e. a reactive regulation approach.

However, during the last decades a performance-based regulation approach has been introduced in many countries, including Norway. This approach makes it possible to justify alternative designs, if it can be verified that the safety level is in accordance with the functional requirements in the regulation (Meacham 1996). Prescribed, or pre-accepted, solutions still exists as an alternative to the performance-based approach. Thus, pre-accepted solutions often constitute a definition of what is safe enough. The design practice of today is heavily influenced by comparisons with pre-accepted solutions in efforts to qualify designs. If the safety level of the alternative design is equivalent or higher than the pre-accepted solution, the design is considered to comply with the regulation (IRCC 2010).

Looking at the different editions of the Norwegian regulations from early 20th century, we find that the means of egress has been the major remedy when providing fire safety in multi-storey residential buildings. While the residential building and apartments have remained quite the same, there have been a number of different escape staircase concepts (Bjelland 2009). A fundamental question in this paper is whether this focus on staircases could be justified, if the goal is to reduce risk to the occupant's lives?

In the paper we examine fire safety designs based on risk analyses, with the purpose of investigating the safety level of pre-accepted solutions and alternative designs. Our case study is Norwegian multi-storey residential buildings. We have chosen 40 different fire safety concepts for our study. The main variable is the means of egress, and the expected annual number of fatalities as output. Different active fire safety measures are added as sub-variables. We hypothesized large differences in the level of fire safety of the pre-accepted concepts, where the main distinction should be made between the solutions with and without automatic fire sprinkler systems.

Our analysis is based on a standard approach and data within the fire safety community. The calculations show large inconsistencies on safety level for different pre-accepted solutions. This is problematic, since the pre-accepted solutions are being used as tolerance limits in equivalence analyses, and is thus a measure of good fire safety. The analysis shows, however, that this is not the case. We conclude that fire safety regulators, fire safety consultants, building owners and contractors have limited knowledge of what is good fire safety. In cases where prescriptive solutions are being built, or used solely for qualitative comparisons, the fire safety level will vary considerably.

REFERENCES

Bjelland, H. (2009). Fire safety concepts for residential apartment buildings - Fire safety measures and risk (in Norwegian). Stavanger, M.Sc. thesis, University of Stavanger.

IRCC (2010). Performance-Based Building Regulatory Systems - Principles and Experiences. Inter-jurisdictional Regulatory Collaboration Committee (IRCC).

Meacham, B.J. (1996). The Evolution of Performance-Based Codes & Fire Safety Design Methods. Boston, MA USA, Society of Fire Protection Engineers.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Sequential optimization of oil production under uncertainty

Arne B. Huseby & Nikita Moratchevski
University of Oslo, Norway

ABSTRACT

Optimization is an important element in the management of multiple-field oil and gas assets, since many investment decisions are irreversible and finance is committed for the long term. Recent studies of production optimization include (Horne, 2002) and (Neiro & Pinto, 2004).

(Huseby & Haavardsson, 2009) considered the problem of production optimization in an oil or gas field consisting of many reservoirs sharing the same processing facility. In order to satisfy the processing limitations of the facility, the production needs to be choked. Thus, at any given point of time the production from each of the reservoirs are scaled down so that the total production does not exceed the processing capacity. (Huseby & Haavardsson, 2009) developed a general framework for optimizing production strategies. In (Huseby & Haavardsson, 2010) this work was extended to cases where the production is uncertain.

In the present paper we consider a new variant of this problem where the oil production from a given single reservoir is described relative to a sequence of time periods. In each time period the production is limited by two factors: the potential production volume and the amount of oil that can be processed at the processing facility. At the start of each period one needs to book a certain processing quota. This quota has a cost which is proportional to the size of the quota. At the same time the production generates an income proportional to the processed volume. If the quota is greater than the potential production volume, one ends up with paying too much for the quota. On the other hand, if the quota is less than the potential production volume, the income from the period is reduced. If the latter situation occurs, this implies that same the oil have to be produced in a later period. From an economical point of view, this reduces the present value of the oil production. Thus, for each period the aim is to find the optimal processing quota, i.e., the quota that maximizes the revenue. If the potential production volume is known, this is trivial since the obvious choice is to choose a quota that is equal to this volume. However, the potential production volume typically depends on a number of uncertain reservoir parameters. Thus, in order to choose the optimal quota, one has to take this uncertainty into account.

The uncertainty about the reservoir parameters is expressed in terms of a suitable prior distribution. As the production develops, more information about the production parameters is gained. Hence, the uncertainty distributions need to be updated. In the present paper we show how this updating can be accomplished. Moreover, we show how to find the optimal quota using Monte Carlo simulation.

REFERENCES

Horne, R.N. 2002. *Optimization applications in oil and gas recovery*. Handbook of Applied Optimization, Oxford University Press.

Huseby, A.B. & Haavardsson, N.F. 2009. Multi-reservoir production optimization. *European Journal of Operational Research*, 199, 236–251.

Huseby, A.B. & Haavardsson, N.F. 2010. Multi-reservoir production optimization under uncertainty. In *Reliability, Risk and Safety. Theory and Applications*, CRC Press, 407–413.

Neiro, S.M.S. & Pinto, J.M. 2004. A general modelling framework for the operational planning of petroleum supply chains. *Computers & Chemical Engineering*, 28, 871–896.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Shared collaboration surfaces used to support adequate team decision processes in an integrated operations setting

M. Kaarstad & G. Rindahl
Institute for Energy Technology, Halden, Norway

ABSTRACT

The petroleum industry is undergoing a transition made possible by new and powerful information technology. Traditional work processes and organizational structures are challenged by more efficient and integrated approaches to offshore operations. Several companies on the Norwegian continental shelf have implemented integrated operations (IO) as a strategic tool to achieve safe, reliable and efficient operations (Ringstad & Andersen, 2007). In integrated operations, traditional work processes and organizational structures are challenged by more efficient and integrated approaches to offshore operations. The new approaches make it possible to reduce the impact of traditional obstacles, e.g., geographical, organizational or professional, to efficient decision-making (Ringstad & Andersen, 2007).

Integrated operations are both a technological and an organizational issue, and imply both the use of new technology and new work processes. The IO technology consists of high-quality video conferencing, shared workspaces and data sharing facilities and involve people in discussions both onshore and offshore. The shared workspaces include so-called collaboration rooms (operation rooms) for rapid responses and decision-making.

In an operational context, a number of decisions are required, the decisions are interdependent, the environment changes, both autonomously and as a consequence of the actions taken by the decision maker; and the decisions are made in real time. Because the successful performance of many important tasks requires skillful decision-making, the identification of forms of decision support for dynamic decision-making has become a research priority. However, this identification process has proven to be very challenging (Lerch & Harter, 2001).

Personnel working in an IO setting will often benefit from decision support in different situations. In this paper, we take a look at what decision support is, including examples from observing a dispersed team on a Norwegian oil field (Rindahl et al., 2005), with regard to how decisions may be facilitated through a shared collaboration surface. The literature review in this paper is based on a review of decision support (Kaarstad, 2009) performed within a larger research program (http://www.sintef.no/ Projectweb/Building-Safety/). Knowledge obtained in this research program is currently carried on in a follow-up research program where the obtained knowledge is used when advising on how distributed collaboration could be organized in order to ensure resilience. The current paper focuses on IO settings, and in which situations decision support would be useful in IO.

REFERENCES

Gonzalez, C. (2005). Decision support for real-time, dynamic decision-making tasks. Organisational behaviour and human decision processes 96, 142–154.

Kaarstad, M. (2009). Decision support: using decision support to facilitate adequate team decision processes. In: A.B. Skjerve, M. Kaarstad (Eds.), Building Safety. Literature Surveys of Work Packages 2 and 3: Decision Making, Goal Conflicts, Cooperation, IO Teamwork Training, Decision Support, and the Impact of Resilience of New Technology (IFE/HR/F-2009/1388), Halden, Institute for Energy Technology, pp. 143–175.

Lerch, F.J. & Harter, D.E. (2001). Cognitive support for real- time dynamic decision making. Information systems research, 12 (1), 63–82.

Rindahl, G., Torgersen, G., Kaarstad, M. & Drøivoldsmo, A. (2009). Collaboration and Interaction at Brage. Collecting the Features of Successful Collaboration that Training, Practices and Technology must support in Future Integrated Operations, *IO Center Report No. P4.1-003.*

Ringstad, A.J. & Andersen, K. (2007). Integrated operations and the need for a balanced development of people, technology and organisation. International Petroleum Technology Conference, Dubai, 2007.

www.sintef.no/ Projectweb/Building-Safety/

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Visualization and verification of dependable work processes for stakeholder-driven organizations

Atoosa P.-J. Thunem & Harald P.- J. Thunem
Institute for Energy Technology, Halden, Norway

ABSTRACT

Although some industries still seem to distinguish between the terms "workflow" and "business process" when speaking about their *value chain*, it is almost impossible to justify any fundamental difference between a work process and a business process. When thinking about business processes in today's organizations, they have in fact no meaning if they each do not encompass work states and transitions as well as their prerequisites, all represented by various technological, human and organizational properties of a work process. Individually and jointly, these work processes add value to the products and services "passing through" the processes and offered to all stakeholders (including the employees and customers). In reality, each work process is associated with a certain *value-adding* business sub-goal, which is usually the responsibility of a functional (operational) unit or department.

How the *values* are defined and thus measured is of course different from one enterprise to another, depending on, among others, the types of stakeholders, certain legislations and regulations the enterprise needs to relate to, and cultural factors of the enterprise itself. Therefore, the values also play a significant role in how the sub-goals and therefore work processes achieving each of them are defined, managed and categorized. That is why some organizations consider all their sub-goals as equally value-adding (towards the overall goal and mission of the organization), and therefore place the associated work processes as a part of the value chain, while other organizations operate with two groups of sub-goals, where the primary group is understood to form the organization's value chain. Consequently, only specific, "primary" work processes are placed there. The others are considered as supporting, "secondary" work processes across the mutually parallel primary work processes. In such organizations, the "secondary" work processes add value to the products and services by influencing the primary work processes.

A major problem related to design and change of work processes in implementation and management of Integrated Operations (IO, synonym to other used terms such as e-Field, Future Field, Intelligent Energy, and Digital Energy) within the petroleum industry is how to visualize and keep track of both new and changing elements/properties (including the requirements) of work processes, especially when several parallel work processes fundamentally need to interact with one another. Managing all different types of information related to various stages of each work process in a detailed, traceable and systematic manner will make it possible to unambiguously visualize how a certain task as a part of a certain work process is dependent on and influences other tasks for the same work process or other parallel work processes. At the same time, this will also make it possible to better verify against the desired work processes, and thus to better identify and deal with lack of compliance with certain requirements, or fulfilled but contradicting requirements, which both very often contribute to causes of events and incidents.

Based on experiences from different domains such as telecommunication, transport, energy (including petroleum and nuclear) and health, this paper addresses a variety of challenges that are involved in visualization and verification of dependable (thus also risk-informed) work processes for stakeholder-driven organizations, where the customers constitute one group of stakeholders (often divided into sub-groups). In that respect, the topic and related issues discussed by the paper are a direct contribution to trustworthy solutions for the challenges faced by the petroleum industry in improved implementation and management of Integrated Operations (IO), as well as improved compliance with current and coming generations of IO.

REFERENCES

Abrahamson, Erik, Fairchild & Gregory (1999). Management fashion: lifecycles, triggers, and collective learning processes, *Administrative Science Quarterly*, 44 (4), pp. 708–740.

Atherton, Martin, Collins, Jon, Vile & Dale (2008). BPM: lessons from the real world - Practical ideas to apply to your organisation, Community research report, *Freeform Dynamics Ltd.*

Dynamic reliability

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A comparison of scenario binning methods for dynamic probabilistic risk assessment

K. Metzroth, D. Mandelli, A. Yilmaz, R. Denning & T. Aldemir
The Ohio State University, Columbus, OH, US

ABSTRACT

Dynamic Event Tree (DET) analysis is an effective approach for evaluating plant response during the course of a transient in the presence of modeling or stochastic uncertainties. In addition, it can account for the time or process history dependencies of these uncertainties in a physically consistent way by tracking all generated scenarios using the same simulation tool. DET analysis produces very large output datasets, and one of the biggest challenges in DET analysis is the management and interpretation of the very large amount of data that is generated. A possible approach to analyze DET output data is to place scenarios into groups based on similar characteristics to enable the analyst to better conceptualize the meaning of the results and to reduce the effort required in subsequent stages of the analysis (Mandelli, 2010). However, the question remains as to what scenario characteristics should be used to define "similarity". In classical Level 1 PRA (as outlined in NUREG-1150 (U.S.N.R.C., 1990)) scenarios were grouped mostly according to the states of various active plant systems. Applying such a method directly to DET analysis may not be appropriate since the scenario groupings considered in NUREG-1150 for Level 1 PRA are time-independent and it is possible that the timing of system actuation, failure, or recovery could have a significant impact on the scenario outcome. Hence, it is possible that scenarios with similar active component states have quite different consequences. In addition, DET analysis produces a wealth of data which can be utilized to group scenarios in different ways (e.g. based on actual plant physical variables rather than on inferring the plant physical state based on active component states), depending of the objectives of the analysis. The Mean-Shift-Methodology (MSM) (Mandelli, 2010) is proposed as a means to group DET scenarios based on their physical characteristics. A DET analysis is performed for a Station Blackout (SBO) scenario of a pressurized water reactor with possible AC power recovery using the MELCOR (Gauntt, 2005) code coupled to the ADAPT (Hakobyan, 2006) (Analysis of Dynamic Accident Progression Trees) DET generation tool.

The classical binning methodology used in NUREG-1150 grouped scenarios which have similar plant states. However, the results of the DET analysis show that scenarios with similar plant states may be very different with regards to their temporal evolution which is difficult to capture with the classical binning approach. The MSM tended to yield groups with more similar temporal histories. On the other hand, MSM could not always capture the fact that although certain scenarios may exhibit similar behavior up to a certain point in time, some aspects of the scenarios may diverge if the analysis is continued to later times in the accident.

REFERENCES

Gauntt, R.O., Cash, J.E., Cole, R.K., Erickson, C.M., Humphries, L.L., Rodriguez, S.B. & Young, M.F. 2005. "MELCOR Computer Code Manuals," U.S. Nuclear Regulatory Commission, Washington, D.C. NUREG/CR-6119, Vol. 1, Rev. 3 (SAND97-2398).

Hakobyan, A., Denning, R. & Aldemir, T. "A Methodology for Generating Dynamic Accident Progression Event Trees for Level-2 PRA", Proceedings of PHYSOR 2006, September 2006.

Mandelli, D., Yilmaz, A., Metzroth, K., Aldemir, T. & Denning, R. 2010. "Scenario Aggregation and Analysis via Mean-Shift Methodology in Level 2 PRA," 2010 International Congress on Advances in Nuclear Power Plants (ICAPP'10).

U.S.N.R.C., 1990. "Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants," U.S. Nuclear Regulatory Commission, Washington D.C. NUREG-1150.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A dynamic Level 2 PRA using ADAPT-MELCOR

D.M. Osborn, D. Mandelli, K. Metzroth, T. Aldemir, R. Denning & U. Catalyurek
Nuclear Engineering Program, The Ohio State University, Columbus, OH, US

ABSTRACT

The current approach to Level 2 Probabilistic risk assessment (PRA) using the conventional event-tree/fault-tree methodology requires pre-specification of event order occurrence which may vary significantly in the presence of uncertainties. Manual preparation of input data to evaluate the possible scenarios arising from these uncertainties may also lead to errors from faulty/incomplete input preparation and their execution using serial runs may lead to computational challenges. A methodology has been developed for Level 2 analysis using dynamic event trees (DETs) that removes these limitations with systematic and mechanized methodology as implemented using the Analysis of Dynamic Accident Progression Trees (ADAPT) software (Catalyurek et al., 2010; Hakobyan et al., 2008).

This paper discusses the work which has been conducted for a Level 2 PRA Station Blackout Scenario using a dynamic event tree analysis for a series of MELCOR input decks containing a 3-loop PWR with a steam supply system and a sub-atmospheric dry containment. This work is an extension of past ADAPT-MELCOR dynamic PRA experiments (Hakobyan et al., 2008; Hakobyan et al., 2006a, b) in which additional parameters are considered. Creep rupture distributions for Carbon Steel (CS), Stainless Steel (SS), and Inconel (IS) are considered not only for the pressurizer surge line (SS) and steam generator U-tubes (IS), but also for multiple reactor coolant loops (CS and SS). Additionally, multiple safety relief valve (SRV) failures are considered for a per-demand failure probability (high number of valve cycles) and high temperature cycling failure probability (number of valve cycles above 1,000 K) distributions. To further reduce conservatism, an updated containment fragility curve was incorporated using data from NUREGE/CR-5121 and NUREG/CR-6920. This work allows for better insight into potential structural material timing differences for creep rupture and investigates multiple SRV failures.

REFERENCES

Catalyurek, U. et al., 2010. Development of a Code-Agnostic Computational Infrastructure for the Dynamic Generation of Accident Progression Event Trees, *Reliability Engineering & System Safety*, Volume 95: 278–304.

Hakobyan, A. et al., 2006a. Treatment of Uncertainties in Modeling the Failure of Major RCS Components in Severe Accident Analysis, *Transaction of the American Nuclear Society*, Volume 94: 177–179.

Hakobyan, A. et al., 2006b. Treatment of Uncertainties in Modeling Hydrogen Burning in the Containment during Severe Accidents, *Transactions of the American Nuclear Society*, Volume 95: 683–685.

Hakobyan, A. et al., 2008. Dynamic generation of accident progression event trees, *Nuclear Engineering and Design*, Volume 238: 3457–3467.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A probabilistic model for online scenario labeling in dynamic event tree generation

D. Zamalieva & A. Yilmaz
Photogrammetric Computer Vision Laboratory, The Ohio State University, OH, US

T. Aldemir
Department of Nuclear Engineering, The Ohio State University, OH, US

ABSTRACT

While the traditional Event-Tree/Fault-Tree (ET/FT) approach is still the most popular approach for Probabilistic Safety Assessment (PSA), difficulties arise in the PSA modeling of systems with significant hardware/process/software/firmware/human interactions. Also, it is not clear how passive system behavior can be modeled with the ET/FT approach. Such difficulties may be overcome with the use of Dynamic Event Trees (DETs). A challenge with DETs for realistic systems is computational requirements. Thousand of scenarios may need to be simulated following a single initiating event which leads to long runtimes, high computational complexity of analysis and interpretation of the produced scenarios. However, not all of the scenarios may carry the same significance. In fact, experience shows that a high percentage of the scenarios exhibits normal transient behavior (i.e., does not lead to a situation that has to be avoided) and follow similar evolution pathways. These scenarios can be assigned lower priority, delayed or even discontinued during simulations, allowing more efficient utilization of computing resources. In this paper, we propose a probabilistic approach for classification of each scenario in a DET as non-failure or failure using Hidden Markov Models (HMMs). To address the problems stated above, the classification must be performed online, using only the part of the scenario that is available so far, while its execution still continues.

HMMs have been widely used in a large variety of applications, including manipulations of large sequences of data obtained over a period of time (MacDonald & Zucchini 2009). The main components of a HMM are the unknown or hidden states and the observations generated depending on these states. The transitions from one state to another are controlled by transition probabilities, while the observations are governed by emission probabilities associated with each hidden state. In this case, the hidden states are chosen to represent the underlying physics of the system and the observations are associated with the system variables that characterize the scenarios. Given a set of non-failure and failure scenarios, the parameters of the HMM that captures the behavior of non-failure scenarios are estimated using the well-studied Baum-Welch algorithm (Baum, Petrie, Soules & Weiss 1970). During the execution of the DET generation algorithm, the likelihood of each scenario being generated from this model is computed using the Forward Algorithm (Russell & Norvig 2002) and compared to that of failure scenarios. Depending on the chosen confidence level and the likelihood of a given scenario fitting the model, the scenario is labeled as failure or non-failure.

To measure the performance of the proposed method we use the dataset produced by the RELAP5/3D model of an ABR-1000 utilizing an RVACS (Reactor Vessel Auxiliary Cooling System) passive decay heat removal system. Experiment show that the proposed algorithm is capable of correctly labeling over 80% of non-failure scenarios as non-failure, while not labeling any failure scenario as non-failure.

REFERENCES

Baum, L.E., Petrie, T., Soules, G. & Weiss, N. (1970). A Maximization Technique Occurring in the Statistical Analysis of Probabilistic Functions of Markov Chains. *The Annals of Mathematical Statistics 41*(1), 164–171.

MacDonald, L. & Zucchini, W. (2009). *Hidden Markov Models for Time Series: An Introduction Using R*. London: Chapman and Hall.

Russell, S.J. & Norvig, P. (2002). *Artificial Intelligence: A Modern Approach* (Second ed.). Prentice Hall series in artificial intelligence. Prentice Hall.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Application of the dynamic hazop to an air separation distillation column

J.S.G.C. Matos
White Martins Gases Industriais Ltda. (Praxair Inc.), Rio de Janeiro, RJ, Brazil

P.F. Frutuoso e Melo
COPPE/UFRJ-Programa de Engenharia Nuclear, Rio de Janeiro, RJ, Brazil

M. Nele
Escola de Química/UFRJ, Rio de Janeiro, RJ, Brazil

ABSTRACT

The development of the chemical industry has required larger industries, capable of producing more products in a shorter period of time. To accomplish this goal, chemical process industries became more complex, bringing more hazards to plant operation (e.g.: higher temperatures and pressures). This lead to higher requirements from regulatory agencies and more detailed hazard analysis techniques development.

This work covers the use of dynamic simulation with process hazard analysis (dynamic HazOp) which provides more accurate and trustful information than traditional HazOp, which is a qualitative analysis. This methodology used allows the evaluation of a deviation occurrence, deviation consequences magnitude, time needed for the worst case scenarios to be reached, and actions that should be taken in order to avoid or mitigate the occurrence of the deviation.

For our study case, the lower column of an air separation plant was used. The deviations applied were pressure increase of one inlet stream, external temperature increase (simulating a fire), addition of hydrocarbons to the inlet stream (simulating severe atmospheric pollution) and the increase of the inlet streams temperature. Dynamic profiles showing the variations from the normal operating values of the process variables were calculated to check the impacts of the deviations applied to the system.

The simulations performed are supposed to show not only process safety impacts but also the possibility of performing dynamic simulations associated with the traditional HazOp in order to confirm the results in the analysis. Therefore, the consequences with operation impact were also important for this study.

The results showed the need of checking whether safety relief devices of the system analyzed were capable of relieving the maximum pressure indicated by the simulation. Another result identified was that hydrocarbon analyzers were required in several points of the system and with a certain set point in order to avoid the high concentration of contaminants which could result in an explosion. Each simulation brought different information calling attention for several verifications.

The dynamic simulation associated to the hazard analysis confirmed the need of the protections previously included in the process and instrumentation diagram, but also showed the need of checking several protections and indications locations and set points.

If the dynamic simulation is used in the initial stages of a project redundant protections (safety systems as safety relief valves) or indications (as pressure indicators) can be identified and eliminated during the analysis.In such cases, besides checking whether equipment safety margins are adequate to support possible conditions of process operation, the methodology can also reduce company costs.

REFERENCES

Aspen Tech. Available at www.aspentech.com/core/. Access: Oct 24th, 2009.

Eizenberg, S. et al. Combining HAZOP with Dynamic Simulation – Applications for Safety Education, Journal of Loss Prevention in the Process Industries, v. 19, pp. 754–761, 2006.

Hardeveld, R.M. et al. Investigation of an Air Separation Unit Explosion, Journal of Loss Prevention in the Process Industries, v. 14, pp. 167–180, 2001.

Matos, J.S. et al. Application of the Dynamic HazOp to the Operational Hazard Evaluation of an Air Separation Distillation Column (in Portuguese). 96 s. Dissertation (Master Degree in Chemical and Biochemical Processes Tehcnology) – Escola de Química, UFRJ, Rio de Janeiro, RJ, 2009.

Ramzan, N. et al. Application of Extended HazOp and Event Tree Analysis for Investigating Operational Failures and Safety Optimization of Distillation Column Unit, AIChE J., Process Safety Progress, v. 26 (3), pp. 248–257, 2007.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Capability of the MCDET method in the field of dynamic PSA

M. Kloos
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Germany

1 INTRODUCTION

Motivations for the development of the MCDET method were the deficiencies of the classical PSA approach in modeling complex accident scenarios and the hardly quantifiable uncertainty on its results due to the uncertainty on the concept or completeness of the applied simplified models. The question is, how realistic are probabilistic safety/risk assessments derived from the simplified—mostly static—PSA models?

The accident scenarios to be considered in a PSA are characterized by complex interactions over time between the technical system, the physical-chemical process and operator actions. Due to stochastic influencesa variety of potential event sequences has to be considered, and the assessment of the consequences of an accident scenario can only be probabilistic. It is obvious, that the spectrum of event sequences may be tremendous, if there are aleatory uncertainties in the physical-chemical process (e.g., pressure release rates, coolant or feed-water injections rates, etc.) or in the timing of system function failures and of human actions. Only if a PSA is able to account for all the sequences which may evolve and to rank the sequences according to their likelihood, it can provide a well-founded probabilistic assessment.

The MCDET method developed at the GRS allows for an integral probabilistic modeling of accident scenarios along the time axis. It provides probabilistic assessments for accident sequences which adequately account for the spectrum of sequences which may actually evolve. The combination of Monte Carlo (MC) simulation and the Discrete Dynamic Event Tree (DDET) approach as realized in MCDET is capable of accounting for any aleatory uncertainty at any time without need of significant simplifications.

The implemented MCDET module system can in principal be coupled with any deterministic dynamic code simulating the behavior of a nuclear power plant. Beside aleatory uncertainties, MCDET can also consider epistemic uncertainties which determine how precise probabilistic assessments can only be provided due to the knowledge uncertainties involved in the calculation. Methods were developed to reduce the computational effort of epistemic uncertainty evaluations in the framework of MCDET analyses.

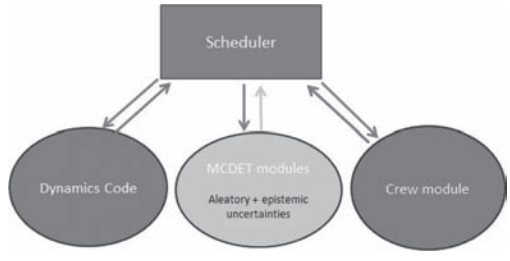


Figure 1. A scheduler program arranges the calculations of the MCDET modules, the crew module and a dynamic code.

The MCDET module system was supplemented by an extra crew module which enables calculating the dynamics of operator actions depending and acting on the plant dynamics as modeled in a deterministic code and on stochastic influences as considered in the MCDET modules. The crew module allows for running situation-dependent sequences of human actions as they are expected for a dominant mental state and cognitive behavior.

The combination of the MCDET and crew modules with an appropriate deterministic code allows for evaluating complex accident scenarios where human actions, technical installations, the physical-chemical process and stochastic influences are the main interacting parts in the course of time. A scheduler program arranges the corresponding calculations (Fig. 1).

The capacity of the MCDET and crew modules has been demonstrated by several applications. Two large scale applications are described in the paper. An overview on the MCDET method and the implemented modules is given as well.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Development of a simulator independent cognitive human reliability model for nuclear accident conditions

R. Sundaramurthi & C. Smidts
The Ohio State University, Columbus, OH, US

ABSTRACT

This paper describes a simulator independent human reliability model that can be applied to the probabilistic assessment of any nuclear power plant accident. Unlike mechanical systems where reliability has been quantified and the systems designed to high reliability standards, it is difficult to measure the degree of reliability of an operator. It has been documented that Human Error Probability (HEP) can be as high as 0.5 for certain tasks (Swain, 1983) and that uncertainty margins are significant. As such, human behavior is one of the primary contributors to uncertainty in risk assessment and requires high fidelity modeling. High fidelity modeling is obtained by carefully replicating the operating conditions as they unfold, as well as by modeling the various internal decision making and situation assessment processes that take place during an accident. This can only be achieved by the combination of a dynamic reliability modeling environment, powerful and high fidelity process simulation and cognitive operator models. The model discussed in this paper is a derivative of IDA (Smidts, Shen & Mosleh 1996), which models the operator behavior by considering its cognitive aspect through the three modules of information, decision making and action. Four models/modules are designed which along with the interface facilitating the interactions between them constitute the HRA model (IDA-SI) (Fig. 1). The components are: 1) Problem Solving and Decision Making module (PS/DM) 2) Performance Shaping Factors module (PSF) 3) Mental model module 4) Memory module. The operator diagnostics and decisions are guided by goals and are reached through strategies influenced by Performance Shaping Factors (such as stress level, timing constraints, etc). As an extension to IDA, the model portrays the relationship between these PSFs in the form of a causal diagram. Possible strategies adopted by the operator are modeled and the influence of the PSFs causing switch between the strategies is depicted. Every operator has a mental model of the evolution of scenarios in a plant, developed through knowledge and experience, and he/she constantly updates it based on the feedback that he/she receives from the plant (Laird, 1983). Mental models have not been a focus of human reliability research within the context of nuclear power plant operation. In this paper a foundation is laid to depict the dynamic updating of the operator's mental model and possible development of flaws in the same. These in turn translate into incorrect decisions/actions that culminate into accidents. This proposed human reliability model should be an asset to train operators by making them aware of their responses in unfamiliar scenarios and enable discovery of pre-existing flaws for timely corrective action.

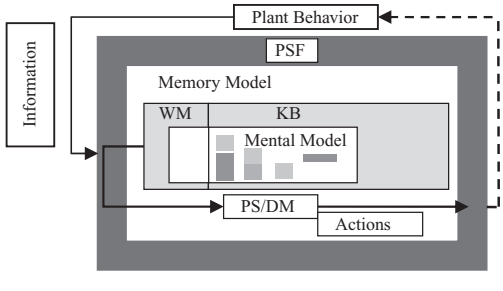


Figure 1. IDA-SI Overview of Modules and their interactions.

REFERENCES

Laird, P.N. 1983. Mental Models – *Towards a cognitive science of language, inference and consciousness*. Cambridge, Massachusetts: Harvard University Press.

Smidts, C. Shen, S.H. & Mosleh, A. 1996. The IDA cognitive model for the analysis of nuclear power plant operator response under accident conditions—Part 1: problem solving and decision making model. *Rel. Eng. and Syst. Safety*. 51–71.

Swain, A.D. et al. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Application*. NUREG/CR–1278. Washington, D.C: US NRC.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Dynamic reliability and uncertainty analysis of severe accident with randomly delayed events

R. Alzbutas
Lietuvos energetikos institutas, Lithuania
Kauno technologijos universitetas, Lithuania

P.E. Labeau
Université Libre de Bruxelles, Belgium

ABSTRACT

The Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD) and its simplified version the Theory of Stimulated Dynamics (TSD) have been introduced for the analytical modeling and the simulation of hybrid (continuous-discrete) systems as well as for dynamic reliability considerations. The main reason for TSD was to keep alive the concept of countable sequences that is at the heart of the classical safety assessment approach, keeping at the same time the level of SDTPD complexity tractable. The described theory deals with the concepts of stimulus and delay in event sequence delineation, and their implementation.

In addition, the focus is set on the simulation and analysis of systems with delayed events. Because stimuli activation and random delays condition the event occurrences, the history of stimuli activations during the accident transients does matter in calculating the frequencies of events. Thus, an extension of the Markovian process accounting for these features is considered.

An approach of non-Markovian simulation and uncertainty analysis is discussed in order to simulate complex dynamic systems and to adapt SDTPD for practical applications, mostly in the context of dynamic reliability analysis. This developed approach and related methods for uncertainty analysis have been used as a basis for test case simulation in the perspective of its applications for severe accident scenario analysis.

Various formal definitions and a methodology of how to assess uncertain parameters' influence on the estimation of results are considered before the test case. For the analysis of the dynamic results' sensitivity to the uncertain model parameters, the uncertainty analysis is integrated within TSD. It is also introduced as a possible way for analysis of TSD-based simulation results and demonstration of timing importance.

Finally, it is concluded that modeling of stimulated dynamics as well as uncertainty and sensitivity analysis allows the detailed simulation of system characteristics and representation of their uncertainty. The developed approach of analysis for hybrid systems with delayed events can be efficiently used to estimate the reliability of complex systems and at the same time to analyze the uncertainty of this estimate.

REFERENCES

Alzbutas, R., Izquierdo, J.M. & Labeau, P.E. Application of stimulated dynamics to probabilistic safety assessment, Proceedings of ESREL (2), pp. 1027–1034 (2007).

Alzbutas, R. & Janilionis, V. Aggregate simulation of stimulated dynamics for reliability analysis, Proceedings of ESREL 2007 (2), pp. 1035–1041 (2007).

Alzbutas, R. & Janilionis, V. Determination and Simulation of Stimulated Dy-namics. Science Works of Lithuanian Mathematicians Association 46, pp. 321–327 (2006).

Chaumont, B. Overview of SARNET Progress on PSA2 Topic, First European Review Meeting on Severe Accident Research (ERMSAR), Aix-en-Provence (2005).

Devooght, J. & Smidts, C. Probabilistic Dynamics as a Tool for Dynamic PSA, Reliability Engineering and System Safety 52 (3), pp. 185–196 (1996).

Hofer, E. Sensitivity analysis in the context of uncertainty analysis for computationally intensive models, Computer Physics Communications 117, pp. 21–34 (1999).

Izquierdo, J.M. et al. Relationship Between Probabilistic Dynamics and Event Trees, Reliability Engineering and System Safety 52, pp. 197–209 (1996).

Izquierdo, J.M. & Labeau, P.E. The stimulus-driven theory of probabilistic dy-namics as framework for probabilistic safety assessment. Proc. of interna-tional conference PSAM 7 – ESREL'04 (2), pp. 687–693 (2004).

Krzykacz, B., et al. A software System for Uncertainty and Sensitivity Analysis of Results from Computer Models, Proc. Int. Conf. PSAM-II (2), pp. 20–25 (1994).

Labeau, P.E. et al. Dynamic Reliability: Towards an Integrated Platform for Probabilistic Risk Assessment, Reliability Engineering and System Safety 68, pp. 219–254 (2000).

Labeau, P.E. & Izquierdo, J.M. Modeling PSA Problems-I: The Stimulus-Driven Theory of Probabilistic Dynamics, Nuclear Science and Engineering 150, pp. 1–25 (2005).

Raimond, E. & Durin, T. Comparison between classical and dynamic reliability approaches. Specification and results of a benchmark exercise, European Review Meeting on Severe Accident Research (ERMSAR), Forschungszen-trum Karlsruhe GmbH (2007).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Lazy forward-chaining methods for probabilistic model-checking

Florent Teichteil-Königsbuch, Guillaume Infantes & Christel Seguin
ONERA—The French Aerospace Lab—Toulouse, France

Model-checking of probabilistic discrete-event systems is a thriving research area with still important theoretical issues and a growing interest from industries. Exact methods used in state-of-the-art model-checkers like PRISM or MRMC do not scale very well and are still not relevant for large industrial systems. On the other hand, simulation-based methods like stochastic comparison or the APMC model-checker scale better, but only provide statistical and approximate results, that are not well-suited to critical systems where quantitative properties must be proved without approximation. This paper targets a new algorithmic framework inspired by recent advances in probabilistic automated decision-making, that allows to validate without numeric approximation quantitative properties of large discrete-time systems defined in formal languages such as PRISM and AltaRica.

Our algorithm constructs an incremental graph of reachable states from a known initial state. Since PCTL properties boil down to validate *until* formulas $f_1 u^{t\leq T}_{p\geq\alpha} f_2$ (f_1 is true until f_2 is true within T time steps, with probability higher than α), we stop the construction of a path in the graph when either f_1 becomes false, or t becomes equal to zero, or f_2 becomes true. The transitions of the graph are generated on-the-fly when necessary from the high-level language description. An important feature of our algorithm is the lazy discovery of reachable *strongly connected components* (SCCs) of the graph, i.e. the sets of states that are bilaterally connected, using the framework of Tarjan's depth-first search algorithm for any oriented graph. Starting from a given initial state, this algorithm explores the graph of reachable states by expanding paths until absorbing states or loops are reached, then it goes up these paths to identify on-the-fly each SCC once. The main advantage of identifying SCCs is that the probability of the formula $f_1 u^{t\leq T} f_2$ can be computed locally inside each SCC. Moreover, as SCCs are discovered one after the other in a backward manner when going up paths, the latter formulas are computed only once and guaranteed to be exact. The local computation of until formulas can be performed with state-of-the-art computation schemes used in PRISM or MRMC (in these model-checkers, validation of quantitative properties relies on sparse data structures defined over all states of the model, but not over local states).

In this paper, we present our algorithm for exactly validating PTCTL formula using on-the-fly SCCs discovery and local computations. We highlight the key ideas of this algorithm on examples from embedded aeronautical avionics systems, modeled in PRISM and AltaRica. We also show preliminary results compared with other state-of-the-art probabilistic model-checkers such as PRISM and MRMC.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability assessment for complex systems operating in dynamic environment

G. Babykina, N. Brinzei & J.-F. Aubry
CRAN, UMR 7039, Nancy-Université, CNRS. Vandoeuvre-les-Nancy, France

G.A. Pérez Castañeda
Instituto Tecnológico de Tehuacán. Tehuacán, Puebla, Mexico

ABSTRACT

The paper aims to study a complex repairable system, operating in a dynamic environment. The reliability of the system is assessed by means of statistical modeling. We consider a system with several redundant components. The system operates in different modes defined on one hand by discrete states of its components (active/passive, failure/normal operation) and on the other hand by the operational environment conditions. These conditions are defined by continuous physical phenomena. The system's failure is conditioned by a certain combination of its components failures. The dynamic operational environment, the different discrete modes of system's operation and the deterministic and/or stochastic transitions between these modes are simultaneously accounted for by means of the Stochastic Hybrid Automaton (SHA). The SHA model contains the possible states of the system and the events which govern the transitions between these states. Some transitions occur when the components fail according to a random failure rate (stochastic transitions). Other transitions can be governed by the deterministic behavior of the physical phenomenon defining the operational environment of the system. The objective in this context is to estimate the global system's failure rate. Monte Carlo simulations are carried out to generate a long trajectory followed by the system. The system's failure behavior is then modeled using the counting process framework applied to the simulated data. Precisely, failures are assumed to be driven by a Non Homogeneous Poisson Process (NHPP). The NHPP parameter estimates are used to assess the reliability of the complete system.

The proposed approach is applied to an electrically powered furnace containing two redundant components: two temperature control loops. The temperature evolution is deterministic. The components' failure rates are allowed to be constant or time-dependent. The failure of the system occurs when both control loops fail or the furnace itself fails.

The results show the relevance of statistical methods for global system's failure rate assessment in dynamic environment.

REFERENCES

Andersen, P., Borgan, Ø., Gill, R. & Keiding, N. (1993). *Statistical models based on counting process*. Springer-Verlag, New York.

Labeau, P., Smidts, C. & Swaminathan, S. (2000). Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering & System Safety 68(3)*, 219–254.

Pérez Castañeda, G., Aubry, J.-F. & Brinzei, N. (2011). Stochastic hybrid automata model for dynamic reliability assessment. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 225(1)*, 28–41.

Rigdon, S. & Basu, A. (2000). *Statistical methods for the reliability of repairable systems*. Wiley.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Using dynamic Bayesian networks to solve a dynamic reliability problem

Perrine Broy
Université de technologie de Troyes & CNRS, Troyes, France
EDF R&D, Département Management des Risques Industriels, Clamart, France

Hassane Chraibi & Roland Donat
EDF R&D, Département Management des Risques Industriels, Clamart, France

ABSTRACT

In probability risk assessment, evaluation of system reliability tries to be more and more precise. To that end, physical phenomena affecting the systems should be taken into account. Such systems are called hybrid systems and are often referenced in the literature as a part of the dynamic reliability framework.

The evolution of hybrid systems is a combination between discrete stochastic events on the one hand and continuous or transitional deterministic phenomena on the other hand.

Mathematically, hybrid systems are generally represented by Piecewise Deterministic Markov Processes (PDMP). A PDMP (Davis 1984) is a pair consisting of a random vector in a finite state space and a deterministic vector in a continuous state space. The random vector describes the configuration of the system and the deterministic vector characterizes some environmental variables. The evolution of these variables is governed by differential equations that depend on the configuration in which the system stands.

There are some methods which are supplied with tools dedicated to describe and quantify PDMP. Each method has its advantages and disadvantages, depending on the criteria such as readability, flexibility or time of calculation.

In an industrial context, it is essential to get a representation of the system both readable and trusty. Furthermore, an elaborated mathematical background and existing software tools should lead to limit simplifying assumptions and decrease the computation time. Thus a challenge is to judiciously select both description and quantification methods regarding the characteristics of systems, the expected indicators and the level of accuracy required for the probability risk assessment.

This paper aims to introduce a methodology to describe and quantify hybrid systems based on the use of the formalism of Dynamic Bayesian Networks (DBN) (Murphy 2002). We show that this approach turns out to be relevant to perform reliability analyses of simple hybrid systems.

This article briefly presents the DBN formalism along with a compatible quantification method, namely the bucket elimination. Finally, we illustrate this approach by applying our methodology to a simple system from a popular benchmark known as the heated tank system in the literature. Our results are compared to those from the literature (Zhang et al., 2008).

REFERENCES

Davis, M. (1984). Piecewise-deterministic Markov processes: A general class of non-diffusion stochastic models. *Journal of the Royal Statistical Society. Series B (Methodological) 46*(3), 353–388.

Murphy, K.P. (2002). *Dynamic Bayesian Networks: Representation, Inference and Learning*. Ph. D. thesis, University of California.

Zhang, H., Dufour, F., Dutuit, Y. & Gonzalez, K. (2008). Piecewise deterministic Markov processes and dynamic reliability. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 222*(4), 545–551.

This page intentionally left blank

Fault diagnosis, prognosis and system health management

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A comparison of distribution estimators used to determine a degradation decision threshold for very low first order error

O. Hmad & A. Mathevet
Safran Engineering Services, Etablissement de Villaroche, France

P. Beauseroy & E. Grall-Maës
Institut Charles Delaunay UMR STMR (6279), Université de Technologie de Troyes, France

J.R. Masse
Safran Snecma, Etablissement de Villaroche, France

ABSTRACT

Before introducing a monitoring algorithm in an operational system, it is important to assess very carefully its performances. The performance estimation of the algorithm requires the tuning of a decision threshold based on its abnormality decision criterion for very low first order error. In this paper a detection process for deciding between correct and incorrect behavior of the start system is considered. The first order error (Pfa) of the detector required by the companies is about 10E-9, which is very low. Thus the decision threshold has to be properly determined in order to satisfy this requirement. The value of this threshold depends only on the distribution of the abnormality decision criterion Y under the hypothesis of no degradation. The distribution law of Y is not known and the searched threshold has to be determined using some limited data set.

The approach we use consists in determining the threshold using an estimation of the abnormality decision criterion distribution. Three methods to estimate this distribution are compared. Firstly, a Gamma distribution model has been considered because the distribution of Y should be approximately a Gamma distribution. Secondly non parametric probability density estimator has been considered. A Parzen window estimator has been used. Thirdly we considered the Johnson transformation which is used to convert non normal random variable to obtain a new one which distribution is normal.

This communication presents a comparison of these three methods according to threshold estimation for very low first order error and concludes about the robustness of Johnson transformation for this problem. Two cases were studied: one when the abnormality decision criterion follows a Gamma distribution and one when it is not a Gamma distribution. We studied the influence of the parameter distribution values, of the data set size and of the targeted first order error value.

As a conclusion, results show that the average estimated threshold using the Johnson transformation is by far too pessimist in all cases. Using the obtained threshold would lead to reduce the power of the decision rule which may not be acceptable. In addition, the variance of the estimated threshold is very large leading to highly unreliable results. Note also that the Johnson transformation does not always succeed to produce a normal random variable while it is designed for that. The number of unsuccessful transformations is shown to increase with the size of the used data set. Fitting a Gamma distribution when data are not Gamma gives more pessimist estimates than using Johnson transformation but with a much lower variance. Finally non-parametric estimator is shown to give the best performances among the three tested estimators. These performances should be improved by optimizing the non-parametric estimator.

REFERENCES

Anderson, T.W. & Darling, D.A. (1952). "Asymptotic theory of certain "goodness-of-fit" criteria based on stochastic processes". Annals of Mathematical Statistics 23, 193–212.

Ausloos, A., Grall, E., Beauseroy, P., Grall, A. & Masse, J.R. (2009). Estimation of Monitoring Indicators Using Regression Methods - Application to Turbofan Starting Phase. ESREL conference.

Bowman, A.W. & Azzalini, A. (1997). "Applied Smoothing Techniques for Data Analysis". Oxford University Press.

Chou, Y., Polansky, A.M. & Mason, R.L. (1998). "Transforming nonnormal data to normality in Statistical Process Control". Journal of Quality Technology 30, 133–141.

Johnson, N.L. (1949). “Systems of frequency curves generated by methods of translation”. Biometrika 36, 149–176.
Parzen, E. (1962). “On estimation of a probability density function and mode”. Annals of Mathematical Statistics 33, 1065–1076.
Shapiro, S.S. & Wilk, M.B. (1965). “An analysis of variance test for normality”. Technometrics 14, 355–370.
Silverman, B.W. (1986). “Density Estimation for Statistics and Data Analysis”. Chapman and Hall: London.
Slifkerm J.F. & Shapiro, S.S. (1980). “The Johnson System: Selection and Parameter Estimation”. Technometrics 22(2), 239–246.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A first step toward a model driven diagnosis algorithm design methodology

J.-M. Flaus, O. Adrot & Q.D. Ngo
Laboratory G-Scop, Grenoble, France

ABSTRACT

Large-scale complex process plants are safety critical systems where the real-time diagnosis is of great importance. In a model based systems engineering approach, the structured development process from the concept to the production to the operation phase is organized around a coherent model of the system. This model contains in particular mathematical relations about the behaviour of the system that could have been used for simulation in the design phase.

The objective of this work is to use this information to design automatically an online diagnosis algorithm.

In order to detect abnormal behaviour, model based algorithm compares the observed behaviour to the expected behaviour. To do this, Analytical Redundancy Relation (ARR), must be build. An Analytical Redundancy Relation (ARR) is a constraint deduced from the system model which contains only observed variables, and which can therefore be evaluated from any observations set to check if observed and expected behaviours are consistent.

The approach allows:

- To extract the valid relations about behaviour for a working mode of the system.
- To build, using symbolic analysis graph path search, analytical redundancy relation for the various system configurations.
- To evaluate this ARR in using set valued computations (interval arithmetic) to take into account model and measurements uncertainties.

The model of the system is given as a set of model blocks, which define variables, relation between these variables, input/ouput visibility of these variables and connections between variables of different blocks. Such a model definition is used with some syntax variations in numerous simulation tools such as Modelica, Matlab, SysML or Yasma.

An activity model describing the part of the system that are active is also required to identify the valid blocks at a given time. This activity model is often described with a discrete event model. In this work, we use an activity model as describe in the UML specification.

Using this information our algorithm selects the valid relation for a given configuration. This set of relations allows building a bipartite graph with nodes representing variables and nodes representing constraints. Some of variables are measured on line. A path graph search allows building the set of all the structural elementary ARR.

Each ARR is defined with a set of relations which can be structurally evaluated from measurements. However, as it could be difficult or even impossible to solve analytically these relations, we solve them as a system of constraints to be satisfied (CSP). An empty solution set reveals an abnormal behaviour.

Of course, measurements are not perfect and the system evolution is not exactly as the relations model it. In order to take this into account, intervals ARR are considered and checked using interval arithmetic.

The proposed algorithm has been developed in JAVA and its capabilities are demonstrated on a basic illustrative example.

REFERENCES

Adrot, O. & Flaus, J. (2010). Guaranteed fault detection based on interval constraint satisfaction problem. In *Control and Fault-Tolerant System (Systol), 2010 Conference on, pp. 708–713.*

Adrot, O. & Ploix, S. (2006, August). Fault detection based on set-membership inversion.

Flaus, J.-M. (2008). A model-based approach for systematic risk analysis. *Proceedings of the institution of Mechanical Engineers, Part O: Journal of Risk and Reliability Volume 222, Number* 1/, 79–83.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A generic adaptive prognostic function for heterogeneous multi-component systems: Application to helicopters

P. Ribot & E. Bensana
Onera—The French Aerospace Lab, Toulouse, France

ABSTRACT

Maintenance efficiency of industrial systems is an important economical and business issue. It is a way to improve reliability and safety while reducing the final cost of systems. The Helimaintenance project aims at optimizing the maintenance of civil helicopters. The objective is to develop an integrated logistics system in order to support the scheduling of maintenance actions and reduce the unavailability of helicopters. Maintenance actions must be decided on an efficient and complete analysis of the health of the system when it is operating. An embedded supervision system is in charge of monitoring the helicopter and detecting problems and misbehaviors which require maintenance actions. The supervision system integrates a diagnostic function to accurately determine which components may cause a system failure and have to be replaced by a maintenance action. In order to optimize the maintenance cost, it is also necessary to perform preventive maintenance by deciding to perform actions on the system before the problems actually occur. To reach this objective, a prognostic reasoning must be performed over the system to establish whether a preventive action is pertinent at a given time. A data processing system integrating a prognostic function receives information from the supervision system (embedded sensors, pilot observations, diagnostic result) and suggests component replacements before they fail. For this purpose, the prognostic function has to compute a fault probability for each component and evaluate their Remaining Useful Life (RUL for short). Classical reliability methods can be used to compute the RUL of components but they do not take into account the real stress of the supervised system when it is operating. A stress can result from a fault within the system or an abnormal solicitation (like mechanical vibrations, thermal impacts, pressure, etc.) that may affect the system RUL. An adaptive prognostic function is then required to take into account the current condition of the system that is evaluated by the diagnostic function and by monitoring environmental conditions.

Aeronautical systems, like helicopters, are complex systems built from an assemblage of heterogeneous components (mechanical, hydraulic, electric or software, etc.). In this paper, a formal generic modeling framework is presented for a heterogeneous multi-component system. Available knowledge about each component is represented in an abstracted but homogeneous way with a set of parameters, a set of ranges for parameters and a set of relations describing the component behaviors. The component description is refined by introducing a structural model and a functional model. Some operational modes are then defined for components according to the functional state of the system.

In order to evaluate the RUL of components, the prognostic function has to predict the occurrence of each possible fault that may occur on the system components. The proposed prognostic methodology uses reliability analyses and physics-based models in order to compute fault probabilities of components. Due to its flexibility, the parametrized Weibull model is used to represent a fault probability density function. The Weibull characteristics depends on component solicitations that are modeled as component parameters. The parameter values are either monitored by sensors or estimated from current diagnosis and allow to model the component degradation. The first component that is predicted to fail may cause some abnormal solicitations on components it interacts with. The prognostic function has to take the fault propagation in the system into account by predicting abnormal solicitations caused by future faults that may accelerate the component degradation. These fault probabilities of components have to be updated according to new parameters values resulting from sensors or estimated from on-line diagnosis. For illustration, the proposed prognostic function is finally applied to an example of a helicopter transmission system.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Advanced text mining algorithms for aerospace anomaly identification

Z. Bluvband & S. Porotsky
A.L.D, Tel-Aviv, Israel

ABSTRACT

The paper describes an advanced text categorization procedure developed and successfully used in aerospace industry, especially for safety assessment, analysis and improvement. Typically, failure reports are human-written records, usually just free text written by professional people. Therefore understanding and treatment of this statistical documentation is vital for Safety and Reliability measurement and improvement. The purpose of presented paper is the computerized analysis and interpretation of human reported free-text aviation safety records, in order to automatically "read", discover and treat anomalies occurred in the field. The methodology and algorithms were verified on actual, significant and appropriate Safety and Reliability data bases including the ASRS (Aviation Safety Reporting System) data base (http://asrs.arc.nasa.gov/index.html) containing millions of unprocessed safety events reports. One of the most important applications and goals of the research is to assign new in-coming reports to one or more from the several of predefined categories on the basis of their textual content.

Examples of anomalies, extracted from ASRS (Aviation Safety Reporting System) data base (http://asrs.arc.nasa.gov/index.html), are "817: Ground Incursion—Landing without Clearance" (occurs in 2% of the reports), "856: In-flight Encounter—Turbulence" (occurs in 3% of the reports), "860: In-flight Encounter—VFR in IMC" (occurs in 1% of the reports), etc.

Optimal categorization functions can be constructed from labeled training examples (i.e., after human expertise) by means of supervised learning algorithm and cross-validation. Numerous methods for text categorization have been developed lately: Neural Networks, Naive Bayes, AdaBoost, Linear Discriminant Analysis, Logistic Regression, Support Vector Machines (SVM), etc. SVM has become a popular learning algorithm, used in particular for large, high-dimensional classification problems; it has been shown to give most accurate classification results in a variety of applications. However the Direct application of these methods to Aerospace Anomaly Discovery is restricted for the following reasons:

a. fully automatic procedure can support only middle values of output parameters Recall and Precision, 50–75%;
b. safety report statistical parameters are absent, i.e., the frequency of words in a report has been changing on a "year to year" basis.

The method suggested in the paper is based on SVM binary classification approach intended to perform a multi-label categorization, but practically performing several times the binary one of type One-Versus-Rest (according to the amount of anomalies). In the standard SVM method, the optimal separating function is reduced to a linear combination of kernels on the training data with training feature vectors $\mathbf{X}$ and corresponding labels y. If $y(\mathbf{X}) \geq 0$, the non-marked document $\mathbf{X}$ is recognized as "Positive" for current category (anomaly), otherwise as "Negative".

To support high values of output criteria (e.g., both Recall and Precision have to be simultaneously more than 90 … 95%) and non-stability of the report statistics, we propose the mixed, partially automated approach for the selection of most of anomalies automatically, by means of text categorization algorithm, with occasional usage of human expertise. The following additional meta-parameters are introduced:

- G_{low}—Low boundary for separating function;
- G_{high}—High boundary for separating function.

The proposed Text Categorization algorithm is performed as following:

If $y(\mathbf{X}) \geq G_{high}$, the non-marked document $\mathbf{X}$ is recognized as "current category" and expert should not verify this solution;

If $y(\mathbf{X}) \leq G_{low}$, the non-marked document $\mathbf{X}$ isn't recognized as "current category" and expert should not verify this solution;

If $Glow < y(\mathbf{X}) < G_{high}$, the expert should manually verify this document for current category.

Some numerical results, based on ASRS On-Line Data Base, are considered. In order to support values of Recall = 0.9 and Precision = 0.95 for anomaly "860: In-flight Encounter—VFR in IMC" it is necessary to perform an expert verification of 910 reports from the total amount of 10,000. Thus we are able to achieve significant acceleration of expert work (reduction of report amount, verified by expert after automatic text categorization)—11 times less reports to review.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

ANN based Bayesian hierarchical model for crack detection and localization over helicopter fuselage panels

C. Sbarufatti, A. Manes & M. Giglio
Politecnico di Milano, Milano, Italy

ABSTRACT

If from one hand the aerospace industry is trying to extend the duration of life-limited components, from the other hand a deep control is necessary over the structures to guarantee both the machine availability and reliability. In effect, thanks to the advance in the evaluation of the actual structural health by means of a Structural Health Monitoring (SHM) system, it could be possible to set a Condition Based Maintenance (CBM). Inside this frame, the key factor is the disposal of detection and monitoring systems as reliable as possible in order to conjugate safety with economics objective. The first step for developing such advanced technology would be the disposal of a robust damage detection system, able to recognise, locate and quantify the damage in a certain component.

The work described hereafter is a simulation of crack detection and localization problem over a typical aerospace structure, consisting of a riveted aluminium skin, stiffened with some reinforcing elements, as the one experimentally tested by Giglio (2008) for damage tolerant material characterization purposes. The combined use of Bayesian Hierarchical Models (BHM) and Artificial Neural Networks (ANN) is proposed. As a matter of fact, the enormous resemblance between hierarchical models and distributed detection problems makes the former applicable to problems where parameters and/or observations interact (in the form of conditional probability) through a certain hierarchical structure. In addition, Finite Element (FE) numerical Models for damage inside the structure (Figure 1) could be used to train algorithms, as reported in detail by Katsikeros (2009). Basic system knowledge would result, upon which to introduce the variability by means of real sensor network data, coming from similar structures studied by Sbarufatti (2010), in order to consider the problem from a statistical point of view. The ANN could then be used as a level of the BHM presented by Chen (2002), thus reformulating the decision problem using hierarchical models and performing Bayesian inference to calculate posterior probability-based fusion. Finally, a proposal for the sensor network characterization in terms of Probability of Detection (PoD) and False Alarm (PFA) is also reported. The algorithm proved to perform quite well, though some improvements in decision fusion are still under development by the authors, foreseeing further advances in the methodology.

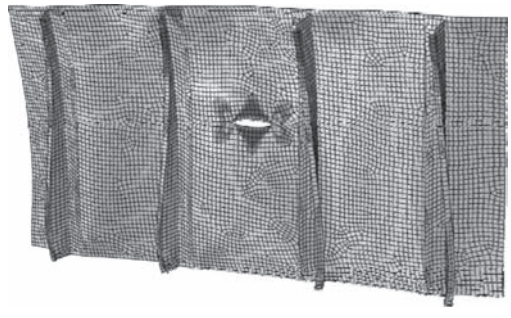


Figure 1. Example of a skin crack damage over the monitored structure. FE models are used to extract information (strain field modification inside this framework) to be used to train algorithms.

REFERENCES

Chen, B. & Varshney, P.K. 2002. *A Bayesian Sampling Approach to Decision Fusion Using Hierarchical Models*, IEEE transactions on signal processing, Vol. 50, Nr. 8.

Giglio, M. & Manes, A. 2008. *Crack propagation on helicopter panel: experimental test and analysis.* Engineering fracture mechanics, Vol. 75, pp. 866–879.

Katsikeros, C.E. & Labeas, G.N. 2009. *Development and validation of a strain-based Structural Health Monitoring system*. Mechanical Systems and Signal Processing, Vol. 23/ 2.

Sbarufatti, C., Manes, A. & Giglio, M. 2010. *Probability of detection and false alarms for metallic aerospace panel health monitoring*. Proc. 7th Int. Conf. on CM & MFPT, BINDT.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Contribution to specific determination of system state and condition

D. Valis
University of Defence, Brno, Czech Republic

L. Zak
Brno University of Technology, Brno, Czech Republic

ABSTRACT

Nowadays system requirements are set up and evaluated in various manners. When determining an item technical state, there are many options available. However, in order to specify the state and the condition of a system, we choose one off-line approach. The paper deals with mathematical processing, monitoring and analysing oil field data. Such data comes from the laser spectrography within tribodiagnostic oil tests. When analysing oil data, we apply mathematical methods based on the analyses and calculations of time series. It is expected to get the results which will help to improve maintenance policy, life cycle costing and operations. Due to the fact that the data sample has been classified as fuzzy and uncertain, the FIS (Fuzzy Inference System) is used.

The growing dependability and operation safety requirements of modern equipment along with the increasing complexity and the continuous reduction of the expenses of operation and maintenance might be satisfied among others by the consistent use of modern diagnostic systems. Present systems can be equipped with signal processors related to board computers and intelligent sensors which are the source of the primary information on a technical state in real time. The main task of object technical state diagnostics is to find out incurred failures, and also prevent from failure occurrence while detecting and localizing changes in an object structure.

The paper is going to deal mainly with the analysis of tribotechnical system outcomes (TTS—friction in it, wear and lubrication). Regarding the tribotechnical system, the basic information on tribological process, operating and loss variables is provided. Tribology is the science and the technologies of interacting surfaces in a relative motion. The function of a tribotechnical system is to use the system structure for converting input variables (e.g., input torque, input speed, input type of motion, and sequence of motions) into technically utilizable output variables (e.g., output torque, output speed, output motion) (GfT, Moers 2002, Czichos & Habig 2003).

The primary type of interaction depends greatly on a friction state. Consequently, when a lubricant is present, the atomic/molecular interaction might not occur, while the mechanical interaction can. Friction and wear in a given TTS ultimately depend on the interactions between elements. The friction state, the effective mechanisms of friction and wear, and the contact state can be used to describe the interactions. The tribological loads occurring in the real contact areas produce tribological processes. These tribological loads include the dynamic physical and chemical mechanisms of friction, wear and boundary-layer processes.

Due to the TTS there are a lot of oil diagnostic data available. The data were also obtained thanks to the maintenance monitoring program in the Czech Armed Forces. These data are considered to be the final outcome of tribodiagnostic, but they are not when it comes to assess system health and condition. These data can tell us a lot about lubricants/life fluids quality itself and a system condition. In terms of reliability, maintainability and safety we consider such data to be very valuable. There are methods analysing oil/life fluids samples. Some of these methods have been used in this paper in order to determine the physical quality of a sample and to get the picture of it, e.g. age, condition, etc. Since the system operation, the taking of oil samples and the outcomes themselves are very fuzzy, we adapted some approaches from the fuzzy logic theory. This function was later supported by the approaches of fuzzy logic.

REFERENCE

Czichos, H. & Habig, K.-H. 2003. *Tribologie-Handbuch; Reibung und Verschleiß*, 2nd edition. Weisbaden: Vieweg. In German.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Decision support with a markovian approach for maintenance context activities

P. Vrignat, M. Avila, F. Duculty & B. Robles
University of Orléans, PRISME Laboratory, MCDS Team, IUT de l'Indre, Châteauroux, France

F. Kratz
ENSI, PRISME Laboratory, MCDS Team, Bourges, France

ABSTRACT

Industrial processes need to be maintained to prevent breakdown. Some years ago, maintenance activities were only deployed to repair process after the problem occurs.

As in these studies, we show that a degradation level of a process can be proposed to the expert, from series of "field" events. In this study, we try to learn, without "a priori", this default signature. The originality of our work, is to use maintenance activities as an indicator (Figure 1). Works, presented in this paper, take part of condition monitoring systems. Using observations provided on the process, we try to generate an availability indicator which can be used by maintenance manager to plan actions dynamically (Figure 1). According to system availability, preventive maintenance could be scheduled to prevent uncontrolled stops of system.

The replacement of components for which failure is thought to be imminent, can be performed when the component is strongly damaged according to different use criteria, or when it has reached a critical condition. The success of this approach depends on the ability to predict remaining life of the component and when to perform the replacement.

Hidden Markov Models (HMM) have been used, with success, to model sequences of events like, for example, in speech recognition. To improve results of these methods, model parameters should be adjusted to match event characteristics (states, topology …). In this study, we use the same strategy to learn events which can be observed on an industrial process. Model topology is configured to provide an availability explanation to our model. When system is started, model will indicate a high level of availability. When system is stopped by defaults, model will be in the "off" state (red state: it is too late to prevent default). Our new estimator is compared with "classical" degradation laws. These degradation laws are used as references.

In this paper, we introduce maintenance strategies and our works are located in this context. We recall some "classical" reliabilities laws. We give more details for Kaplan-Meier law and Cox model, which have been implemented. Our strategy to use HMM for availability indicator implementation is presented. In conclusion, we compare results of "classical" degradation laws with our HMM availability indicator on a synthesis model.

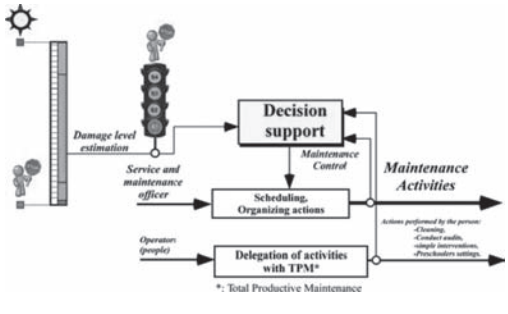


Figure 1. Works goals.

REFERENCES

Aupetit, S., Monmarché, N. & Slimane, M. 2008. Hidden Markov models training using population based metaheuristics, in Advances in Metaheuristics for Hard Optimization, Natural Computing Series, Siarry P. and Michalewicz Z., Springer-Verlag, 415–438.

Ben Salem, A., Muller, A. & Weber, P. 2006. Bayesian networks in system reliability analysis, Proceedings of 6th IFAC Symposium on Fault Detection, Supervision and Safety of technical process, Beijing, P.R. China.

Bérenguer, C. 2008. On the mathematical condition-based maintenance modelling for continuously deteriorating systems, International Journal of Materials & Structural Reliability, 6(2): 133–151.

Bitouzé, D., Laurent, B. & Massart, P. 1999. A Dvoretzky-Kiefer-Wolfowitz type inequality for the Kaplan-Meier estimator, Annales de l'Institut Henri Poincaré, 35, 735–763.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Diagnostic of discrete event systems using timed automata in MATLAB SIMULINK

Z. Simeu-Abazi
G-SCOP laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

E. Gascard
TIMA laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

F. Chalagiraud
Polytech'Grenoble, Université Joseph Fourier, Grenoble, France

ABSTRACT

In the field of dependability, diagnostic plays a most important role in the improvement of the operational availability of equipments. In the industrial field, a significant part is devoted to the maintenance, the tests and the diagnostics of systems (Blanke et al., 2003). Generally, diagnostic involves two interrelated phases: the detection and the localization of failures. The approach proposed in this paper is based on operating time and is applicable to any system whose dynamical evolution depends not only on the order of discrete events but also on their durations as in industrial processes.

Diagnosis of faults is achieved through the implementation of a model observer based on timed automata. This observer called diagnoser makes it possible to detect and locate possible process failures in real time. A failure is detected when an event is not reaching the desired date, or if it lasts too long compared to its ongoing operations. Temporal knowledge of the process to be monitored is therefore essential (Lunze et al., 2001, Simeu-Abazi et al., 2010).

The proposed diagnoser is a monitoring tool that can detect, isolate and locate a fault in a system. The used methodology is based on the timed automata.

The presence of an error corresponds to the execution of a state defined as the defective controller. For the detection phase, parameter detectability is the ability to detect a fault in the system. For the localization phase, the isolation is a property that corresponds to the ability to isolate (locate) a fault.

The diagnostic performance is quantified through two parameters:

- A detection parameter that represents the delay of detection which is the time elapsed between the occurrence of a fault and the detection thereof.
- An isolation parameter that represents the time elapsed between the occurrence of a failure, and the location.

In the complete paper, the methodology is detailed with its implementation in MATLAB-SIMULINK. All developments are illustrated on an example of a system: tank filling system. A fault will be randomly injected into the system and the monitoring module will detect it and locate it as quickly as possible.

REFERENCES

Blanke, M., Kinnaert, M., Lunze, J. & Staroswiecki, M. 2003. *Diagnosis and Fault-tolerant Control*. Berlin: Springer Verlag.

Lunze, J. & Supavatanakul, P. 2002. Diagnosis of discrete-event system described by timed automata. *Proceedings of IFAC 15th World Congress*. Vol J Fault Detection and Supervision, pp. 77–82.

Simeu-Abazi, Z., Di Mascolo, M. & Knotek, M. 2010. Fault Diagnosis for discrete event systems: Modelling and verification, *Reliability Engineering & System Safety*, Vol 95, pp. 369–378.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Differential evolution for optimal grouping of condition monitoring signals of nuclear components

P. Baraldi, E. Zio, F. Di Maio & L. Pappaglione
A. Politecnico di Milano, Milano, Italy

R. Chevalier & R. Seraoui
Electricité de France—R&D, France

ABSTRACT

It is well known that grouping measured signals and then building a specialized model for each group allows to remarkably increase the condition monitoring performance (Roverso, D. et al., 2007). In this paper we propose an approach for optimally grouping a large number of signals measured, for utilization in models for reconstructing the equipment behavior in normal conditions. The algorithm considered in this work is based on the Auto-Associative Kernel Regression method (AAKR), an empirical modeling technique that uses historical observations of the signals taken during normal plant operation (Hines, J.W. & Garvey D.R. 2006). We use a Differential Evolution (DE) algorithm for the optimal identification of the groups (Storn, R. & Price, K. 1997); the decision variables of the optimization problem relate to the composition of the groups (i.e. which signals they contain) and the objective function (fitness) driving the search for the optimal grouping is constructed in terms of quantitative indicators of the performances of the condition monitoring models themselves: in this sense, the DE search engine functions as a wrapper around the condition monitoring models (Fig. 1). A real case study is considered, concerning the condition monitoring of the Reactor Coolant Pump (RCP) of a nuclear Pressurized Water Reactor (PWR). The results of the grouping are evaluated with respect to the accuracy, i.e. the ability of the overall model to correctly and accurately reconstruct the signal values when the plant is in normal operation and robustness, i.e. the overall model ability to reconstruct the signal values in case of abnormal operation and consequent anomalous behavior of some monitored signals of the estimates of the monitored signals by the condition monitoring model developed on the optimal groups, and compared with those achieved with groups obtained using Genetic Algorithm wrapper approach.

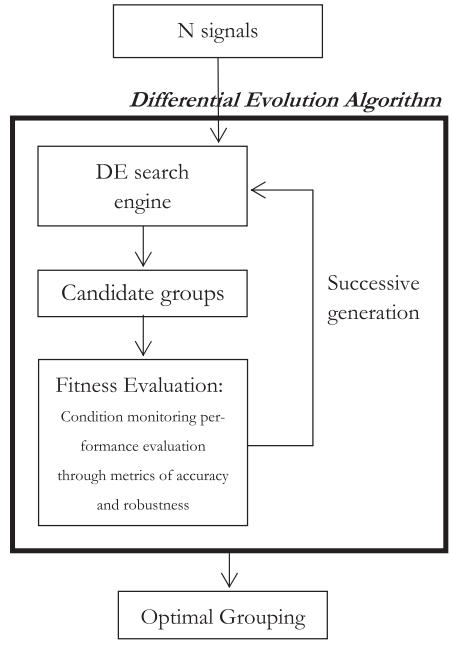


Figure 1. Wrapper approach for optimal signals grouping based on Differential Evolution optimization algorithm.

REFERENCES

Hines, J.W. & Garvey, D.R. 2006. Development and Application of Fault Detectability Performance Metrics for Instrument Calibration Verification and Anomaly Detection. *Pattern Recognition Research* 1: 2–15.

Roverso, D., Hoffmann, M., Zio, E., Baraldi, P. & Gola, G. 2007. Solutions for plant-wide on-line calibration monitoring. *ESREL* 1: 827–832, Stavanger: Norway.

Storn, R. & Price, K. 1997. Differential evolution - A simple and efficient heuristic for global optimization over continuous spaces. *Global Optimization* 11: 341–359.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Ensemble of unsupervised fuzzy C-Means classifiers for clustering health status of oil sand pumps

F. Di Maio
Energy Department, Polytechnic of Milan, Milan, Italy

E. Zio
Energy Department, Polytechnic of Milan, Milan, Italy
Ecole Centrale de Paris and Supelec, Grande Voie des Vignes, Chatenay-Malabry Cedex, France

M. Pecht, P. Tse & K. Tsui
Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Hong Kong

ABSTRACT

Detection of anomalies and faults in slurry pumps is an important task with implications for their safe, economical, and efficient operation. Wear, caused by abrasive and erosive solid particles, is one of the main causes of failure. Condition monitoring and on-line assessment of the wear status of wetted components in slurry pumps are expected to improve maintenance management and generate significant cost savings for pump operators.

In this context, the objective of the present work is to present a framework for the assessment and measurement of the wear status of slurry pumps when available data is extremely limited.

Figure 1 shows the flowchart of the method: the first step entails the collection into a dataset of raw data, e.g., vibration data; feature extraction consists in the evaluation of the most common summary statistics, e.g. mean, standard deviation, in order to summarize the characteristics of the available data; the aim of feature selection is then to obtain the features which are essential for class separation which is the goal of the last step, i.e., classification.

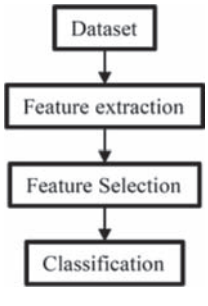


Figure 1. Pattern recognition flowchart.

Experimental data were collected from a number of slurry pumps that are used to deliver a mixture of bitumen, sand, and small pieces of rock from one site to another. For each pump, vibration is monitored as a symptom of system health. Vibration signals have been collected at the inlet and outlet of slurry pumps operating in an oil sand mine.

The main idea is to combine the predictions of multiple unsupervised classifiers, based on fuzzy C-means clustering (FCM), to reduce the variance of the results so that they are less dependent on the specifics of a single classifier. This also reduces the variance of the bias, because a combination of multiple classifiers may learn a more expressive concept class than a single classifier.

The method relies on an unsupervised clustering ensemble methods, based on FCM for classifying the available data. In particular, the adopted unsupervised FCM approach exploits the advantages of the automated generation of fuzzy rules, low computational burden, and the high-level, humanlike thinking and reasoning of fuzzy systems, which offer an appealingly powerful framework for tackling practical classification problems. Fault detection based on FCM allows building clusters with uncertain boundaries accommodating for different pump locations and different pump types and sizes. Moreover, the cluster centers identified by the FCM can turn out useful during on-line fault detection for classifying a new developing degradation pattern into healthy/failed clusters according to the distances of the feature values from the centers. The application of

the framework (data collection, feature extraction, feature selection and classification) can be useful for industries to monitor the health of a machine prone to degradation and sporadic catastrophic breakdowns and dynamically plan equipment maintenance. However, further verification with additional real data is required for the framework to be of practical use in real industrial applications.

REFERENCES

Bezdek, J.C. 1981. *Pattern Recognition with Fuzzy Objective Function Algorithms*, Plenum, New York.

Hancock, K.M. & Zhang, Q. 2006. A Hybrid Approach to Hydraulic Vane Pump Condition Monitoring and Fault Detection, *Transactions of the American Society of Agricultural and Biological Engineers*, Vol. 49(4), pp. 1203–1211.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Evaluation of relevance of stochastic parameters on Hidden Markov Models

B. Roblès, M. Avila, F. Duculty & P. Vrignat
PRISME Laboratory, MCDS team University of Orleans, France

F. Kratz
PRISME Laboratory, MCDS team ENSI, Bourges, France

ABSTRACT

Prediction of physical particular phenomenon is based on knowledge of the phenomenon. This knowledge helps us to conceptualize this phenomenon around different models. Hidden Markov Models (HMM) can be used for modeling complex processes. This kind of models is used as tool for fault diagnosis systems. Nowadays, industrial robots living in stochastic environment need faults detection to prevent any breakdown. In this paper, we wish to evaluate relevance of Hidden Markov Models parameters, without a priori knowledges. After a brief introduction of Hidden Markov Model, we present the most used selection criteria of models in current literature and some methods to evaluate relevance of stochastic events resulting from Hidden Markov Models. We support our study by an example of simulated industrial process by using synthetic model. Therefore, we evaluate output parameters of the various tested models on this process, for finally come up with the most relevant model.

Data used for evaluation: We use synthetic model to produce about 1000 data events. These simulated symbols, according to real industrial process, are obtained by using uniform and normal distribution. Correlatively, we produce states for others models by using same process. Then, these states are used to compare models whose states are obtained by differents learning and decoding algorithms:

- Baum-Welch learning, decoding by Forward,
- Segmental K-means learning, decoding by Viterbi.

Criteria used for evaluation: We try to evaluate the best Hidden Markov Model, by using Shannon's entropy, especially maximum entropy principle. Calculation is made with states and observations (symbols production of HMMs). To emphasize our analysis, we also use some criteria which penalize likelihood value, in order to overcome over-parameterization models, like Akaike and *BIC* criteria.

Some results: We have successfully applied this method to three different models. The first one, uses Shannon's entropy and entropic filter. Given set of observations sequences simulated by our synthetic model, we verify that the most relevant model obtains a good "entropic" score. That corroborates results which show that model 2 is the one which comes closest to real industrial process. This criterion also shows that Baum–Welch learning algorithm with Forward variable decoding gives best results. Second and third criterion (Maximum likelihood and *BIC*) emphasis that HMM 2 is the best model, whatever distribution of symbols. Unfortunately, these criteria are too near each other to make conclusions about learning algorithm.

REFERENCES

[1] Akaike, H. 1973. Information theory and an extension of the maximum likelihood principle. 2nd inter. symp. on information theory, 267–281.
[2] Schwarz, G. 1978. Estimating the dimension of a model. The Annals of Statistics 6, 461–464.
[3] Rabiner, L.R. 1989. A tutorial on Hidden Markov Models and selected applications in speech recognition. Proceeding of the IEEE, 77(2) SIAM interdisciplinary journal, 257–286.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Exploitation of built in test for diagnosis by using Dynamic Fault Trees: Implementation in Matlab Simulink

Eric Gascard
TIMA laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

Zineb Simeu-Abazi
G-SCOP laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

Joseph Younes
Polytech'Grenoble, Université Joseph Fourier, Grenoble, France

ABSTRACT

Fault tree (FT) (Vesely, Goldberg, Roberts & Haasl 1981) is a tool commonly used to assess the causes of industrial system failures. It is particularly used in order to guarantee safety levels of complex systems, and to avoid excessive financial losses. As an example, in the aeronautical field, the diagnostic of all the electronic devices of an aircraft is based on the alarm messages recorded during a flight. In order to establish a diagnostic FT can be used to correlate these alarms between each the others according to specific rules. However, some of these warnings can be false alarms and the localization of the system failures can be ambiguous. Furthermore, FT are limited because they are built with traditional logic gates (OR, AND) which do not consider the dynamic aspects such as the time and the dependencies in an automated system. Consequently, a new type of logic gates has been created to extend the FT into a new version called Dynamic Fault Tree (DFT) (Dugan et al., 1990, Dugan et al., 1992) which uses both the traditional and the dynamic logic gates in order to consider all the functioning aspects of discrete event systems. It will make it possible to improve the efficiency of the diagnostic resulting in lower maintenance costs and better safety levels of automata.

This paper presents the purpose of Dynamic Fault Tree in order to diagnose discrete event systems. The aim is to filter built in test false alarms (Rosenthal & Wadell 1990, Westervelt 2004) in automated systems that feature dependencies. This work consist in programming the logic gates using the StateFlow library of Matlab Simulink and add them to a Matlab toolbox created especially to provide the event blocks that make it possible to build and to simulate DFT models in Matlab Simulink. Consequently a research is on the description of all functioning cases of each gate and to represent them into digital timing diagram. Then, in order to provide an easy way to built DFT and analyse automated system faults, traditional and dynamic gates have been programmed using the StateFlow library of Matlab Simulink and added to a new toolbox created especially in Simulink for the construction and the simulation of DFT.

In the complete article, we will present the whole of the development in three parts. The first one presents the DFT, then the second one explain the principle used to program the logic gates and their inclusion into a new toolbox, and the last one shows an example of application on alarm filtering with DFT in Matlab Simulink.

REFERENCES

Dugan, J., Bavuso, S. & Boyd, M. (1990). Fault trees and sequence dependencies. In *Proceedings of the Annual Reliability and Maintainability Symposium, RAMS'90*.

Dugan, J.B., Bavuso, S.J. & Boyd, M.A. (1992). Dynamic fault tree models for fault tolerant computer systems. *IEEE Trans. Reliability 41*(3), 363–377.

Rosenthal, D. & Wadell, B. (1990). Predicting and eliminating built-in test false alarms. *Reliability, IEEE Transactions on 39*(4), 500–505.

Vesely, W., Goldberg, F. Roberts, N. & Haasl, D. (1981). *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission.

Westervelt, K. (2004). Root cause analysis of bit false alarms. In *IEEE Aerospace Conference*, Volume 6, pp. 3782–3790.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Fault detection through physical modelling in an axial flow compressor of a combined-cycle power plant

J.A. García-Matos, M.A. Sanz-Bobi & A. Muñoz
Institute for Research in Technology (IIT)—ICAI School of Engineering—Comillas Pontifical University, Madrid, Spain

A. Sola
Iberdrola Generación S.A

ABSTRACT

Technological development in recent decades has resulted in a steady growth in power demand, which has required an increase of electrical power generation resources. All these new generating resources require significant investments and maintenance, which involve high costs for companies and lead to higher energy costs. In this context, it is very important to implement an appropriate system able to monitor the health of the assets and, in particular, to detect and diagnose faults in advance.

An important part of these new generation resources are combined-cycle power plants. In these facilities, the axial flow compressor within gas turbines is a critical component. Its malfunction could cause important repair costs, important non-production losses and even power plant shutdowns (Carazas & de Souza 2010). For this reason, early fault detection and diagnosis in these equipments are extremely valuable in order to prevent undesired unavailabilities and to ensure the reliability of the service.

One of the best options to perform evaluation of the health condition of an asset is its continuous monitoring based on multiple sensors acquiring data from the most critical variables of the system (Garcia et al., 2006). Traditional fault detection and diagnosis methods use these data to perform their tasks. It ought to be taken into account that in many cases not all relevant variables can be continuously monitored. This might be due to costs constraints or to the technical difficulty for measuring certain physical variables. However, some of these non measurable variables can precisely describe the system behaviour because they have a clear physical meaning. Some changes in their typical values that could alert about any anomaly or change in the current condition of an industrial component.

This paper proposes a new method for fault detection and diagnosis using real-time information about non-measurable important variables. In order to reach this objective, a physical model will provide the continuous estimation of variables such as enthalpy, taking advantage of the available knowledge of the system. The main goal of the new method is to achieve the capability to explain incipient fault, detected using a physical interpretation.

In order to prove the methodology, it has been applied to a real case, in particular an axial flow compressor of a combined cycle power plant. To this end a detailed physical model of an axial flow compressor has been developed using empirical off-design correlations (Aungier 2003) and turbo machine fundamentals to determine flow conditions at the mid-span of each blade.

Real faulty data of a compressor were used and a fault was successfully detected observing the enthalpy at the outlet of the first rotor cascade. These results suggest the possible improvements that the application of this methodology could bring.

Despite the physical model development drawbacks, a physical explanation can be derived from a detected fault, while other fault detection techniques, such as MLP, cannot provide any explanation about the cause of the failure. Implementing all the methodology steps, despite the challenges they represent, encourage considering fault evolution forecasting as a plausible goal.

REFERENCES

Aungier, R.H. (ed) 2003. Axial-flow compressors: a strategy for aerodynamic design and analysis. ASME Press: New York, NY, USA.

Carazas, F.J.G. & de Souza, G.F.M. 2010. Availability Analysis of Gas Turbines Used in Power Plants. International Journal of Thermodynamics 12(1): 28–37.

Garcia, M.C., Sanz-Bobi, M. & del Pico, J. 2006. SIMAP: Intelligent System for Predictive Maintenance: Application to the health condition monitoring of a windturbine gearbox. Computers in Industry 57(6): 552–568.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fault propagation in systems operating phased missions

R. Remenyte-Prescott & J.D. Andrews
University of Nottingham, UK

ABSTRACT

Locating causes of faults and reducing system maintenance downtime can have substantial benefit to complex engineering systems. Fault diagnostic systems use sensor information in order to determine the causality of loss of functionality in terms of component failures. In practice a limited number of sensors can be installed, therefore, a strategy is needed on how to select the sensors. For example, the sensors can be chosen according to the value of the information that they produce to the fault diagnostic process. The value of each sensor can be described by the effect on the variable which it measures, when component failures occur and the disturbances are propagated through the system. In order to identify the symptoms of component failures a fault propagation technique is needed, which can monitor the deviations in the system process variables, produced when single or multiple component failure events occur.

A fault propagation process can aid in the design of the fault diagnostic system, but it also has a use in its own right. Such modeling approach can be used to confirm or reject the occurrence of reported faults. This situation can occur during the system start-up phase when false faults are reported due to high levels of vibration or due to independently designed interfaces of subsystems. This can result in unnecessary system shutdowns. Using the fault propagation modeling to establish whether the reported faults exist can help to avoid such situations.

Traditional techniques to model fault propagation, such as digraphs (Lapp & Powers 1977), decision tables (Kumamoto & Henley 1979) and mini-fault trees (Kelly & Lees 1986), are limited in their capability to model dynamic system behavior. Therefore, this paper considers Petri nets due to their suitability to model system complexities, such as multiple failure modes, multiple component failures, phased mission systems and dynamic effects of component failures. The novelty of the approach is to use PNs to model fault propagation process, when tokens are passed through the net once single or multiple component failures are introduced. Information about the effects of component failures on the system is then used to determine sensor locations for the fault diagnostics process.

There are three types of PNs used in the model. The component PN describes the state of the component, controls its operating mode and models component failure. Information from component PNs is passed to sub-system and phase PNs. Finally, the master PN is used to model phase progression and pass relevant control signals for each phase. Phase and master PNs are built using FTs, which express failure conditions in each phase. Sub-system PNs can be built directly from the system diagram or converting sub-system FTs to PNs. The methodology is illustrated using a tank level control system.

Knowledge of how system variables deviate due to failures can be used to choose the most valuable sensors. The importance of the sensor will depend on the information it produces to the desired fault diagnostics system, for instance, how suitable it is for quick detection and isolation of failures or multiple fault identification. A sensor information index for each sensor could be defined which describes the amount of information that the sensor gives and best sensors could be selected according to their indexes.

REFERENCES

Lapp, S.A. & Powers, J.G. 1977. Computer-aided Synthesis of Fault Trees, *IEEE Transactions on Reliability* 26(1): 2–13.

Kumamoto, H. & Henley, E.J. 1979. Safety and Reliability Synthesis of Systems with Control Loops, *American Institute of Chemical Engineering Journal* 200(2): 108–113.

Kelly, B.E. & Lees, F.P. 1986. The Propagation of Faults in Process Plants: 1. Modeling of Fault Propagation, *Reliability Engineering* 16(1): 3–38.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Guaranteeing high availability of wind turbines

G. Haddad, P.A. Sandborn, T. Jazouli & M.G. Pecht
CALCE, University of Maryland, College park, MD, US

B. Foucher & V. Rouet
EADS Innovation Works, Suresnes, France

ABSTRACT

Alternative energy sources have increasingly gained the interest of governments, research institutes, academia, and industry in order to advance the penetration of sustainable energy to reduce the dependency on and environmental hazards posed by traditional energy sources such as coal and oil. Wind energy stands at the forefront of these energy sources; the United States Department of Energy (DoE) and the National Renewable Energy Lab (NREL) for instance, under the '20% Wind Energy by 2030' plan, announced that the US could feasibly increase the wind energy's contribution to 20% of the total electricity consumption in the United States by 2030 (U.S. DoE, 2008).

Wind energy sources face numerous challenges that obstruct them from competing with traditional sources, and capturing a significant market share. Wind energy has not been proven out over a sufficient amount of time to assess their long term viability. Furthermore, the reliability of wind turbines turned out to be different from what was originally predicted.

This paper presents the major challenges with guaranteeing high availability of wind turbines; reliability and maintainability, and availability- a function of both. The paper then discusses Prognostic and Health Management (PHM) methods as potential solutions for guaranteeing high availability of wind turbines. PHM consists of methods and technologies to assess the reliability of systems in the actual life cycle and mitigate system risks. PHM is an enabler of Conditional-Based Maintenance (CBM), which can potentially reduce the operation and maintenance cost of wind farms.

The paper then discusses the efforts of prognostic and health management or condition monitoring that have been performed on wind turbines. They are mainly focused on the gearbox, generators, blades, oil, electronics, and overall performance.

We then propose a solution for the health monitoring of the blades and gearboxes of turbines; TRIADE, and we give the specifications of the sensor system that are relevant to the application.

Finally we perform a return on investment analysis to justify the implementation of PHM on wind turbines. We consider TRIADE with data for offshore wind farms from the literature. Results include optimal prognostic distance, life cycle costs with and without PHM, and a distribution of the return on investment.

This work sheds the light on the importance of PHM to the wind energy industry and demonstrates the economic viability of implementing PHM using an already developed sensor system.

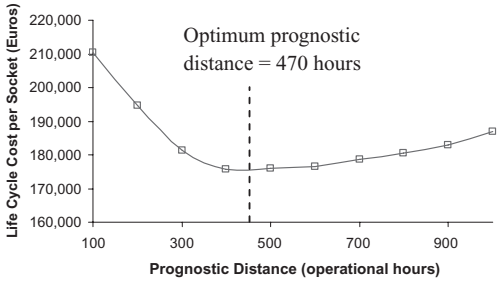


Figure 1. Variation of mean life cycle cost with a fixed maintenance interval (1000-socket population).

REFERENCE

U.S. Department of Energy-Energy Efficiency and Renewable Energy, 2008, 20% Wind Energy by 2030, Increasing Wind Energy's Contribution to U.S. Electricity Supply.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Method of fault detection and isolation in nonlinear electrical circuits

A. Zhirabok & D. Tkachev
Far Eastern Federal University, Vladivostok, Russia

ABSTRACT

Electrical circuits are a convenient tool for modeling different technical objects such as transformers, synchronous and asynchronous electrical machines, drives, and so on. For this reason, electrical circuits are the subject of investigation for fault diagnosis. In the past decades several approaches to the diagnosis of circuits have been developed (Liu 1991). The majority of papers considering the problem of fault diagnosis in electrical circuits use methods of identification (Kinsht et al., 1983, Benlder & Salama 1985, Simani et al., 2002). These methods allow providing an exhaustive analysis (in particular, determining values of parameters) but demand comprehensive information about the circuit operation and are of high computational complexity. At the same time, in practice, one need only to know that parameters of some elements have been changed.

In this paper, the method of fault detection and isolation in electrical circuits described by linear and nonlinear equations is suggested. It does not use methods of identification and allows finding out an element whose parameter has been changed, i.e., has been deviated from its nominal value. The suggested method is based on methods used for diagnosis in dynamic systems (Zhirabok & Usoltsev 2002). This method uses simple matrix methods and can be applied for diagnosis in nonlinear electrical circuits containing non-differentiable nonlinearities such as saturation and hysteresis.

To solve the problem under consideration, so-called logic-dynamic approach developed in (Zhirabok & Usoltsev 2002) is suggested. This approach includes the following three steps.

Step 1. Replacing the initial nonlinear model describing the circuit by certain linear model.

Step 2. Solving the fault detection and isolation problem for this linear model with certain additional restrictions by known methods. The step results in a set of linear diagnostic observers.

Step 3. Transforming the obtained linear observers into the nonlinear ones by adding nonlinear terms. The step results in a set of nonlinear diagnostic observers.

The logic-dynamic approach allows solving nonlinear problem by linear methods without degradation of the solution quality except perhaps dimension of diagnostic observers.

It is assumed that the circuit contains resistors, capacitors, inductances, sources and may operate in no stationary regime. The suggested method is based on the state-space description of the circuit which in the linear case has a form

$$\dot{x}(t) = Fx(t) + Gu(t), \quad y(t) = Hx(t) + Bu(t),$$

where $x(t)$ is the state vector whose components are voltages across the capacitors and currents through the resistors and inductances, $u(t)$ is the vector whose components are values of the sources, $y(t)$ represents measured components of the state vector; F and G are constant matrices describing a structure of the circuit and values of the resistors, capacitors, and inductances, H and B are constant matrices describing measurements. This description can be obtained on the basis of the equations

$$C\dot{U}(t) = I(t), \quad L\dot{I}(t) = U(t)$$

and Kirchhoff's laws.

REFERENCES

Benlder, J. & Salama, A. 1985. Fault diagnosis in analog circuits, *Proc. IEEE*, 73: 1279–1325.

Kinsht, N., Gerasimova, G. & Kats, M. 1983. *Diagnosis of electrical circuits*. Moscow: Energoatomizdat (in Russian).

Liu, R.-W. 1991. *Testing and diagnosis of analogs circuits and systems*. New York: Van Nostrand Reinhold.

Simani, S., Fantuzzi, C. & Patton, R. 2002. *Model-based fault diagnosis in dynamic systems using identification techniques*, New York: Springer-Verlag.

Zhirabok, A. & Usoltsev, S. 2002. Fault diagnosis for nonlinear dynamic systems via linear methods, *CD ROM Proc. 15th World Congress IFAC*, Barcelona, 2002. Spain.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Modeling and fleet effect for the diagnosis of a system behavior

F. Ankoud, G. Mourot & J. Ragot
Centre de Recherche en Automatique de Nancy, CNRS, UMR 7039, Nancy-Université, Nancy, France

R. Chevalier & N. Paul
EDF R&D, Département STEP, Chatou, France

ABSTRACT

In many industrial sectors, a group of identical machines can be exploited by the same process (nuclear power plants, wind farms, etc.). These machines may, however, work under different conditions. Such a set of machines is called a "fleet of machines". In this paper, the problem of modeling the normal behavior of those machines, in the aim of their diagnosis, is considered. Under linearity hypothesis, models describing the normal behavior of identical machines of a fleet may share some common parts (with the same explanatory variables and coefficients) depending on the environmental conditions under which the machines are operating. Identifying these models under the consideration that they may share some common parts is an unsolved problem in the literature. In [2], a method is presented in order to identify, based on the data collected on several identical machines, both the structure and the coefficients of the linear models using a generalization of the LASSO method [4]. However, this approach supposes that all the models have the same structure and approximately the same coefficients. In [3], a method for estimating the coefficients of the models sharing some a priori known common part is proposed. A method for identifying the models of different machines of the same fleet taking into account an identified common part shared by all the models was presented in a previous work [1].

All existing work on the identification of multiple linear models does not take into account that, in addition to the part shared by all the models, some features can be common to a subset of models. In this paper, an approach to identify the parts shared by any subset of models and to estimate the coefficients of these models considering the common parts is suggested. The proposed method consists in minimizing a criterion that takes into account, in addition to the quadratic residual error, the proximity of the coefficients of each couple of models. Starting from some initial values of the different parameters, the method alternates two steps in order to estimate the coefficients of the models and some weights which are indicators of the proximity between the coefficients until convergence. The method is successfully applied on real data collected on a set of reactor coolant pumps of different nuclear power plants.

REFERENCES

[1] Ankoud, F., Mourot, G., Chevalier, R., Paul, N. and Ragot, J. 2011. Estimation of a generic model for a fleet of machines. International Conference on Communications, Computing and Control Applications, IEEE CCCA'11, Hammamet, Tunisia.

[2] Argyriou, A., Evgeniou, T. and Pontil, M. 2007. Multi-task feature learning. Advances in Neural Information Processing Systems 19, Van-couver, Canada. MIT Press.

[3] Liu, A. (1996). Estimation of the parameters in two linear models with only some of the parameter vectors identical. Statistics & Probability Letters, 29(4), 369–375.

[4] Tibshirani, R. (1996). Regression shrinkage and selection via the LASSO. Journal of the Royal Statistical Society Series B, 58(1), 267–288.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

One-class SVM in multi-task learning

Xiyan He, Gilles Mourot, Didier Maquin & José Ragot
Centre de Recherche en Automatique de Nancy, CNRS UMR 7039, Nancy-Université, Nancy, France

Pierre Beauseroy, André Smolarz & Edith Grall-Maës
Institut Charles Delaunay, STMR CNRS UMR 6279, Université de Technologie de Troyes, Troyes, France

ABSTRACT

Classical machine learning technologies have achieved much success in the learning of a single task at a time. However, in many practical applications we may need to learn a number of related tasks or to rebuild the model from new data, for example, in the problem of fault detection and diagnosis of a system that contains a set of equipments *a priori* identical but working under different conditions. Indeed, it is common to encounter in industrial problems a number of *a priori* identical plants, such as in the building or maintenance of a fleet of nuclear power plants or of a fleet of their components. In such cases, the learning of the behavior of each equipment can be considered as a single task, and it would be nice to transfer or leverage the useful information between related tasks. Therefore, Multi-Task Learning (MTL) has become an active research topic in recent years.

While most machine learning methods focus on the learning of tasks independently, multi-task learning aims to improve the generalization performance by training multiple related tasks simultaneously. The main idea is to share what is learned from different tasks (*e.g.*, a common representation space or some model parameters that are close to each other), while tasks are trained in parallel [1]. Previous works have shown empirically as well as theoretically that the multi-task learning framework can lead to more intelligent learning models with a better performance.

In this paper, we present a new approach to multitask learning based on one-class Support Vector Machines (one-class SVM). The one-class SVM proposed by Schlkopf et al. [2] is a typical method for the problem of novelty or outlier detection, also known as the one-class classification problem due to the fact that we do not have sufficient knowledge about the outlier class. For example, in the application of fault detection and diagnosis, it is very difficult to collect samples corresponding to all the abnormal behaviors of the system. In the literature, this type of problem can be treated as a two-class classification problem, where the first class is called target class whose samples are available and the second class is called outlier class whose samples are often difficult to obtain. The main advantage of one-class SVM over other one-class classification methods is that it focuses only on the estimation of a bounded area for samples from the target class rather than on the estimation of the probability density. The bounded area estimation is achieved by separating the target samples (in a higher-dimensional feature space for non-linearly separable cases) from the origin by a maximum-margin hyper-plane which is as far away from the origin as possible.

Inspired by the work of Evgeniou and Pontil [3], we introduce the one-class SVM method, a widely used tool for single task learning, into the framework of multi-task learning. In the proposed method, we first make the same assumption as in [3], that is, the model parameters of different tasks are close to a certain mean function. This assumption is reasonable due to the observation that when the tasks are similar to each other, usually their model parameters are close enough. Then, a number of one-class SVMs, one for each task, are learned simultaneously. Our multi-task approach is easy to implement since it only requires a simple modification of the optimization problem in the single one-class SVM. Experimental results demonstrate the effectiveness of the proposed approach.

REFERENCES

[1] Caruana, R. 1997. Multitask Learning. Machine Learning, 28(1), 41–75.
[2] Scholkopf, B., Platt, J.C., Shawe-Taylor, J., Smola, A.J. & Williamson, R.C. 2001. Estimating the support of a high-dimensional distribution. Neural Computation, 13(7), 1443–1471.
[3] Evgeniou, T. & Pontil, M. 2004. Regularized multi-task learning. Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Seattle, WA, USA, 109–117.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Periodical inspection frequency of safety related control systems in machinery—practical recommendations for the determination

M. Dzwiarek
Central Institute for Labour Protection—National Research Institute, Warsaw, Poland

O. Hryniewicz
Systems Research Institute Polish Academy of Sciences, Warsaw, Poland

ABSTRACT

The analyses of accidents happened in the course of machine operation presented in Dźwiarek (2004) showed that 36% of them were caused by improper functioning of the machine control systems. Additionally, in the group of accidents caused by improper functioning of machine control systems serious accidents happened much more frequently (41%) as compared to the group of accidents with no relation to the control system (7%). Those results proved that designers of the safety related control systems should improve their resistance to fault, which most frequently means the application reliable elements and redundant architecture of the systems. In preventing the accidents due to improper operation of the control system periodical inspection of their functioning is of crucial importance. Therefore, the control system designer should specify how often the system should undergo the periodical inspection. The paper presents some recommendations for the determination of periodical inspection frequency of safety related control systems in machinery. The recommendations are based on very simple and easy to use mathematical models which have been developed by adaptation and simplification of models used for the determination of maintenance policies of complex systems.

Let us consider the simplest case when the inspection allows immediate verification if a system is ready to perform its safety function or not. The assumption that the "probability of a dangerous failure per hour" remains constant over the whole life cycle of the machine accepted in standards ISO 13849-1 and IEC 62061 means that also the availability of the system should remain unchanged in every year of its exploitation. Taking into consideration the values of PFH_D for particular PL or SIL, we can determine the required availability of the system per year A_r (see Table 1). If we set the required value of the availability A_r we can find the inspection interval T by solving equation $A(T) = A_r$. Hence, the required inspection interval should be calculated from the following equation

Table 1. Required availability of the system per year for particular SIL and PL.

Performance level (PL)	A_r	Safety integrity (SIL) level
a	0,957	No correspondence
b	0,987	1
c	0,997	1
d	0,99956	2
e	0,999956	3

$$T_0 = \frac{3 - 6\sqrt{0{,}25 - (2/3)(1 - A_r)}}{2\lambda} \approx \frac{2(1 - A_r)}{\lambda}. \qquad (1)$$

When the safety related control system has parallel structure with two channels described by the exponentially distributed random variables characterised by failure rates λ_1 and λ_2, respectively, we can use a procedure proposed in the international standard ISO 13849-1, Annex D that allows to approximate this system with an equivalent one having two identical channels characterized by the failure rate calculated.

Practical implementation of the proposed recommendation is illustrated on some actual case studies. The frequency of inspection has been determined for: system monitoring the access door to the dangerous zone of a machine with low risk level, system monitoring the access door to a robot group with a high risk level and redundant control system of a light curtain that monitors the access to the dangerous zone of an assembly automatic machine.

REFERENCE

Dźwiarek, M. (2004). An analysis of Accident Caused by Improper Functioning of Machine Control Systems. International Journal of Occupational Safety and Ergonomics, Vol. 10, No. 2, 129–136.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Predictive maintenance policy for oil well equipment in case of scaling through support vector machines

M.C. Moura, I.D. Lins, R.J. Ferreira & E.L. Droguett
Center for Risk Analysis and Environmental Modeling, Department of Production Engineering, Federal University of Pernambuco, Recife, Brazil

C.M.C. Jacinto
Petrobras-CENPES, Rio de Janeiro, Brazil

ABSTRACT

In the context of oil industry, scale deposition (fouling caused by salt accumulation) may prevent equipment of properly actuating. This may represent the interruption of oil production as well as economical losses related to oil well unavailability.

Scaling build-up is a result of the combination of a set of independent (or interacting) variables, such as temperature and water composition, which define the subsea environment. These factors need to be tracked in order to predict the amount of scaling that would be deposited. Having the scaling estimate, it is possible to determine the time to next predictive maintenance which aims at removing scaling that might have accumulated on the equipment surface in an attempt of avoiding its failure.

In fact, predicting the scale formation rate involves determining its functional mapping with relation to the influencing variables. However, this dependence function is generally unknown, non-parametric and non-linear. Therefore, Support Vector Machines (SVM) is here used to model the dependence between environment variables and scaling deposition.

SVM is a learning method whose theory is based on statistical concepts. The main idea is to use a dataset to train an algorithm which is able to predict future outputs (scaling deposition) based on empirical inputs (set of influencing variables). In this context, SVM can be compared to Artificial Neural Networks (ANNs) that involve the Empirical Risk Minimization principle which accounts only for the errors in the training stage. On the contrary, the training phase of SVM entails a convex quadratic optimization problem which embodies the principle of Structural Risk Minimization that in turn minimizes the upper bound of the generalization error, with good performance even in cases of small training datasets. Additionally, the characteristics of the SVM training optimization problem enable the Karush-Kuhn-Tucker conditions to be necessary and sufficient to provide a global optimum, differently from ANNs that may be trapped on local minima.

This paper precisely proposes that, from a set of empirical data, SVM can be trained in order to provide a model able to predict scaling deposition behavior over time. Given this model, it is possible to establish appropriate maintenance strategies that aim at cleaning the equipment surface in order to prevent its unavailability. In this context, SVM works as a valuable tool to anticipate the knowledge about system failures. An example of application of this methodology is provided considering scaling data obtained from simulated real environmental conditions of deepwater oil wells.

For this example, after training stage, SVM was able to track scaling increase over time in order to foresee time when a scaling threshold is attained what is associated to a non-acceptable flow loss that would turn out the wellbore unprofitable. In order to do this, it was assumed a set $\mathbf{x}$ of variables is known for a given real environmental condition. These variables define the real scenario for which it is desired to find out how scaling goes during a finite window frame.

Provided the scenario of interest it has been possible to predict scaling values and, thus establish a maintenance strategy through SVM. We also evaluate the uncertainty on scale growth and, then on the time to next predictive maintenance.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Scope and potential of applying artificial neural networks in reliability prediction with a focus on railway rolling stock

Olga Fink & Ulrich Weidmann
Institute for Transport Planning and Systems, ETH Zurich, Switzerland

ABSTRACT

Railways have experienced a steady demand increase over the last years, and this is projected to persist. Due to increased service frequency and the interconnectedness of railway networks, the consequences of service disruptions can be very considerable. Maintaining and increasing a high level of availability and reliability by preventing or reducing malfunctions, failures, disruptions and delays is therefore essential for the efficiency and competitiveness of railway systems. This can be achieved by anticipating, planning, and managing malfunctions and disruptions, which requires an accurate prediction of malfunction conditions. A promising method for reliability prediction, which shows potential for further investigation, is artificial neural network (in the following referred to as "neural networks"). However, neural networks were applied in few studies of reliability prediction for railway rolling stock systems. Currently, there are few studies (Smith et al., 2010)of reliability predictions for railway applications with neural networks. Furthermore, the potential and the scope of applying neural networks in reliability prediction especially for railway rolling stock have not yet been investigated systematically. The scope and potential of applying neural networks in reliability prediction, with a special focus on railway rolling stock systems, are systematically derived in this paper.

Neural networks are applicable in reliability prediction for railway rolling stock systems in a supplementary way, especially in areas where other methods have limitations or achieve only a poor performance. In competing fields of application, the performance of neural networks for selected problems, depending on the quality of input data, is comparable or superior to state of the art methods. But they can also be applied complementarily to other methods, particularly to accelerate computations, improve performance, and to supplement or automate analyses or decisions.

The major applications for railway rolling stock areas are approximation, categorization and association. The subcategories of categorization are classification and clustering. Classification is e.g., applicable for condition based monitoring, where neural networks are trained to classify the different states of the system based on combination of different describing parameters. Clustering is mainly applicable for pattern recognition for failure and malfunction failures. Association is especially applied for memorization purposes. Neural regression can be subdivided into static and dynamic regression. Whereas static regression is the most wide spread application field, dynamic regression implies more complex computation and is also the field with the most promising results. In this field, recurrent neural networks compete with other methods only to a certain extent and therefore provide additional functionalities and a boras scope of application. Neural dynamic regression is the field where there are few studies for reliability prediction.

REFERENCE

Smith, A.E., Coit, D.W. & Yun-Chia, L. 2010. "Neural Network Models to Anticipate Failures of Airport Ground Transportation Vehicle Doors." *Automation Science and Engineering, IEEE Transactions on* 7(1): 183–188.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

State estimation for nonlinear system diagnosis using multiple models: Application to wastewater treatment plants

Anca Maria Kiss, Benoît Marx, Gilles Mourot & José Ragot
Centre de Recherche en Automatique de Nancy, UMR—Nancy-Université, Vandœuvre-lès-Nancy, France

ABSTRACT

This article deals with the observer synthesis for uncertain nonlinear systems affected by unknown inputs. In order to design such an observer, the nonlinear system is represented under the Multiple Model (MM) formulation with unmeasurable premise variables. A Proportional Integral Observer (PIO) is considered and used for fault diagnosis using banks of observer to generate structured residuals. The Lyapunov method, expressed through Linear Matrix Inequality (LMI) formulation, is used to describe the stability analysis and to the observer synthesis. An application to a model of Wastewater Treatment Plant (WWTP) is considered.

In the field of the observer/controller synthesis, the extension of linear methods to nonlinear systems is generally a difficult problem. The multiple model (Murray-Smith and Johansen 1997) has received a special attention in the last two decades, in order to overcome this difficulty. Then the MM approach is a mean to deal with nonlinear systems and to design observer for such systems and is a convex combination of linear submodels. The multiple model formulation is obtained by applying a method proposed in (Nagy, Mourot, Marx, Schutz, and Ragot 2010).

Most of the existing works, dedicated to MM in general and to observer design based on MM in particular, are established for MM with measurable premise variables (inputs/outputs), that represents a simplified situation. The MM under study in this paper is more general and involves unmeasurable premise variables depending on the state variables—requently met in practical situations—hat are not always accessible.

A proportional integral observer approach for uncertain nonlinear systems with unknown inputs presented under a MM form with unmeasurable premise variables is proposed in this paper. The state and unknown input estimation given by this observer is made simultaneously and the influence of the model uncertainties is minimized through a L_2 gain. The convergence conditions of the state and unknown input estimation errors are expressed through LMIs (Linear Matrix Inequalities) by using the Lyapunov method and the L_2 approach.

The variable estimation results are then used for fault diagnosis using banks of observer to generate structured residuals. Several techniques can be used to cope with the Fault Detection and Isolation (FDI) problem, among them observer-based techniques are largely recognized (Patton, Frank, and Clark 2000). Observers are employed in a FDI framework in order to provide an estimation of the interesting signals to be monitored e.g. the outputs, the faults, etc. This is realized through a comparison between system extracted signals and estimated signals. Actuator and sensor faults, simultaneous or not, are treated.

Using these theoretical results, the diagnosis is performed for a wastewater treatment process modeled by an ASM1 model (Weijers 2000). The measures used for simulation process are those of the european program benchmark Cost 624. The numerical simulation results for the proposed application show good state and unknown inputs estimation performances and allows the sensors and actuators fault detection.

REFERENCES

Murray-Smith, R. & Johansen, T.A. (1997). *Multiple model approaches to modeling and control*. Taylor & Francis, London.

Nagy, A.M., Mourot, G. Marx, B. Schutz, G. & Ragot, J. (2010). Systematic multi-modeling methodology applied to an activated sludge reactor model. *Industrial & Engineering Chemistry Research 49*(6), 2790–2799.

Patton, R.J., Frank, P. & Clark, N. (2000). *Issues of Fault Diagnosis for Dynamic systems*. Springer-Verlag.

Weijers, S.R. (2000). *Modelling, identification and control of activated sludge plants for nitrogen removal*. Ph.D. thesis, Technische Universiteit Eindhoven, Eindhoven.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Supervision of switching systems based on dynamical classification approach

A. Chammas, M. Traoré, E. Duviella & S. Lecoeuche
Univ Lille Nord de France, Lille, France
EMDouai, IA, Douai, France

ABSTRACT

In this article, we propose an architecture of supervision of a system who present switching dynamics. The knowledge of the system's model is limited *i.e.,* the physical laws or differential equations that describe its behavior are unknown. In addition, the system has different operating modes. It switches between those modes according to demand. The only knowledge we have on this system is data collected from sensors by measuring its variables. The general purpose that we are after is the predictive maintenance of this system. The predictive maintenance requires a supervision architecture powerful enough to allow taking into account the specificity of this system. In order to achieve an efficient supervision on the system, we use the pattern recognition technique. This technique allows to model through classes the operating modes of the system. The system will then be modeled in classes reflecting its state of operation. The second part of the predictive maintenance strategy is the prognosis which goal is to predict the future state of operation but it wasn't aboard it in this article. The first step was to treat the data collected from sensors. We did so by estimating functions which describe the different dynamics of the system on each range. The next step was to use a clustering algorithm, AUDyC, which makes it possible to treat those data in an auto-adaptive way, allowing the creation of classes and their online update. The observation of these classes showed the different dynamics in normal operating modes and, in presence of fault, these classes started drifting. At this point, it was necessary to differentiate between faults who affect all the dynamics of the system *i.e.,* global faults and faults who affect only some dynamics *i.e.,* local faults. Further on, indicators on the actual state of the system were computed. The calculation of these indicators is based on metrics between the evolving classes and their values reflected the presence of a failure. Finally, some perspectives were given on the elaboration of a control loop and its possible effects on the regulation of the system in failure. Another interesting proposition is to deepen the studies on the proposed supervision approach so that local and global faults can be monitored and diagnosed.

This page intentionally left blank

Fault tolerant control and systems

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Control allocation of k-out-of-n systems based on Bayesian Network reliability model: Application to a drinking water network

P. Weber, C. Simon & D. Theilliol
CRAN—Nancy Université—CNRS UMR 7039, Vandoeuvre-lès-Nancy, France

V. Puig
Automatic Control Department—Technical University of Catalonia, Terrassa, Spain

ABSTRACT

In order to respect the growing of economic demand for high plant availability and reliability, fault tolerant control is introduced. The aim of fault-tolerant control is to keep plant available by the ability to achieve the nominal objectives in the faulty case and/or to accept reduced performances when critical faults occur (Noura et al., 2009).

In most safety critical systems, redundant components concept is considered. Particular cases of k-out-of-n (*koon*) systems have been developed to model various engineering systems. All these systems are over-actuated systems based on redundancy of actuators to increase the system reliability. Nowadays, one of the major problems in the dependability field is addressing the system modeling in relation with the increase of its complexity. A growing interest focused on Bayesian Network in the recent literature is presented to model the reliability of complex industrial systems (Weber et al., 2010). This modeling method seems to be very relevant in the context of complex systems (Langseth 2008). Bayesian Network is particularly able to compute the reliability taking into account observations (evidences) about the state of some components. For instance, the reliability of the system can be estimated and all its components knowing that a part of them are out of order.

This paper presents a new approach of control allocation based on the reliability of redundant actuators when failures occur. The aim is to preserve the health of the actuators and the availability of the system both in the nominal situation and in the presence of some unavailable actuators. Based on the on-line estimation of actuators reliability, this paper proposes a solution to control an over-actuated system that is structured as a k-out-of-n system. The graphical representation of Bayesian Network is very interesting because it formalizes the model by coupling a model structure with simple parameter matrices and the inference computes the reliability of actuators according to on-line observations (evidences). It is applied on k-out-of-n system to estimate its reliability and provide the parameters to distribute the control efforts among the redundant set of actuators. The effectiveness and the performance of the developed method are illustrated on a subsystem of a Drinking Water Network (Barcelona, Spain).

REFERENCES

Langseth, H. (2008). *Bayesian Network in Reliability: The Good, the Bad and the Ugly. Advances in Mathematical Modeling for Reliability*.

Noura, H., Theilliol, D., Ponsart, J. & Chamssedine, A. (2009). *Fault tolerant control systems: Design and practical application.*

Weber, P., Medina-Oliva, G., Simon, C. & Iung, B. (2010). Overview on bayesian network applications for dependability, risk analysis and maintenance area. *Engineering Applications of Artificial Intelligence*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Design of fault tolerant control for nonlinear systems subject to time varying faults

T. Bouarar, B. Marx, D. Maquin & J. Ragot
Centre de Recherche en Automatique de Nancy, UMR 7039—Nancy Université, Nancy, France

ABSTRACT

Generally speaking, there exists two strategies for faulty systems control: the passive strategy and the active one. In the case of the passive strategy, also called robust control, the controller design problem has been widely studied in the literature and many approaches have been proposed for linear and nonlinear systems. The objective is to ensure simultaneously the stability of the system and the insensitivity to certain faults. Nevertheless, robust control methodology concerns a specific class of faults characterized by a bounded norm. The active control or Fault Tolerant Control (FTC) has been introduced to overcome the passive control drawbacks. Indeed, the FTC method allows improving the system performances for a large class of faults. The principal idea of this strategy is to reconfigure the control law according to the fault detection and estimation performed by an observer to allow the faulty system to accomplish its mission.

Since the introduction of FTC techniques, several works have been developed for linear and nonlinear systems. This paper concerns the case of discrete nonlinear systems represented by Takagi-Sugeno models.

In the last decades, Takagi-Sugeno nonlinear systems [1] have attracted a great deal attention, since they allow extending the linear systems theory to nonlinear ones. Thus, many problems dealing with stability, stabilization, observer design and diagnosis have been widely studied. Nevertheless, the FTC problem based on this kind of model is not largely treated. Some works have been introduced in recent years, for instance, trajectory tracking FTC design approach for Takagi-Sugeno systems subject to actuator faults has been developed by [2]. Note that this approach concern the Takagi-Sugeno systems with measurable premise variables (i.e. premise variables depending on the the input or the output).

In the other hand, when the premise variables are unmeasurable (depend on the states of the system), the FTC design problem has been studied by [3].

In the above studies, the considered faults affecting the system behavior are modeled by a constant function. However, in practice, the faults are often time variant.

Based on Lyapunov theory, two approaches dealing with FTC design for nonlinear systems represented by discrete Takagi-Sugeno systems with measurable premise variables are proposed. The objective is to ensure the tracking between a healthy reference nonlinear model and the eventually faulty nonlinear system. The proposed approaches are formulated in terms of Linear Matrix Inequalities (LMI) and they respectively concern the cases when fault dynamics is modelled by exponential function and first order polynomial. Moreover, the developed approaches does not require knowledge of the considered fault varying functions coefficients. To illustrate the applicability and the effectiveness of the proposed approaches, an academic example is considered.

REFERENCES

[1] Takagi, T. & Sugeno, M. 1985. Fuzzy identification of systems and its applications to modeling and control. IEEE Transactions on Systems, Man, and Cybernetics, 15(1), 116–132.

[2] Bouarar, T., Marx, B., Maquin, D. & Ragot, J. 2011. Trajectory tracking fault tolerant controller design for Takagi-Sugeno systems subject to actuator faults, In International Conference on Communications, Computing and Control Applications, Hammamet, Tunisia.

[3] Ichalal, D., Marx, B., Ragot, J. & Maquin, D. 2010. Observer based actuator fault tolerant control in nonlinear Takagi-Sugeno fuzzy systems: LMI approach. In 18th IEEE Mediterranean Conference on Control and Automation, Marrakech, Morocco.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fault-Tolerant system design in multiple operating modes using a structural model

B. Conrard, V. Cocquempot & S. Mili
LAGIS-FRE CNRS 3303, Lille1 University, Villeneuve d'Ascq, France

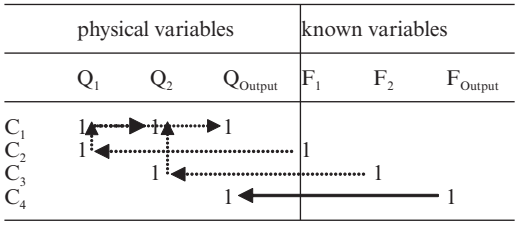
ABSTRACT

This paper deals with the design of fault-tolerant control system thanks to the use of a structural model. The objective of the developed method is to determine the instrumentation scheme (sensors and actuators) of the controlled system which guaranties to tolerate a given number of failures with the lowest cost. A structural model is used for that purpose and allows various potential solution of instrumentation to be deduced and to be expressed as a set of required instruments. The design problem is formalized as an optimization problem that consists in searching for a subset of instruments that provides the best reliable system with the lowest cost.

The novelty of that paper lies in taking into account different operating modes or discrete states of the process to be controlled, by introducing qualitative variables in the structural description.

STRUCTURAL MODEL AND ANALYSIS

A structural model describes the links between the physical quantities without the exact establishment of the physical equation. Despite the lack of information, the analysis of models represented by a bipartite graph or an incidence matrix, allows different paths that go from the known variables to the unknown variables to be deduced.



In this example, two ways allows Q_{Output} to be estimated, be summed up by the following relation:

$$Q_{Output} <= F_{Ouput} \vee (F_1 \wedge F_2)$$

This paper proposes to take into account operating modes with the introduction of variables with discrete states that define in which case the corresponding relations are valid.

DESIGN AND OPTIMIZATION PROCESS

Thanks to this analysis, for each variable (Γ) to be measured or controlled, a relation can be found about the required instruments (I) and can be expressed by a disjunctive normal form (DNF):

$$\Gamma <= (I_x \vee \dots I_y) \wedge \dots \wedge (I_x \vee \dots I_z)$$

According to the minimal number of faulty components (i.e. unusable constraints) that can be tolerated to reach each required variable, the previous relations can be transposed on constraints about the number of required instruments. Associated to a criterion of cost, the problem to solve takes the following form, which is a classical problem of optimization:

$$\begin{cases} \text{Min}\left(\sum C_i Nq_i\right) \\ \sum_{q_i \in E_1} Nq_i \geq n_1 \\ \dots \\ \sum_{q_i \in E_m} Nq_i \geq n_m \end{cases}$$

The final result of the optimization phase is a set of instrumentation schemes with the lowest cost and which all satisfy the dependability constraints imposed by the designer.

CONCLUSION

This paper presents a relatively easy-to-use control system design method. With few information on the system model, i.e. by using a structural description, potential instrumentation schemes for a control system are deduced according to a given fault tolerance level and with a cost criteria. Moreover, qualitative variables are used to represent various operating modes or process states, which lead to a more accurate model of the process.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Guaranteed localization using reliability of measurements in imperfect mobile sensor networks

F. Mourad & H. Snoussi
Institut Charles Delaunay (ICD), UMR STMR CNRS 6279, Université de Technologie de Troyes (UTT), France

F. Abdallah
Laboratoire HEUDIASYC, UMR CNRS 6599, Université de Technologie de Compiègne (UTC), France

C. Richard
Laboratoire Fizeau, UMR CNRS 6525, Université de Nice, Sophia-Antipolis, France

ABSTRACT

This paper deals with localization problems in mobile sensor networks. It thus proposes a robust localization technique that works efficiently under imperfect circumstances. The proposed method assumes that the reliability of exchanged messages is known. Having several collected measurements, the method uses both the Dempster-Shafer and the interval theories to combine all available information, and thus to make accurate decisions about sensors positions.

Mobile Sensor Networks (MSN) are networks composed of a large number of wireless devices, called intelligent sensors (Akyildiz, Su, Sankarasubramaniam & Cayirci 2002). These sensors have computation, communication and sensing capacities. Due to their wireless nature, sensors in MSN are able to move in an uncontrollable manner (Shorey 2006). In other words, sensors change positions in a passive manner due to an external force. In such situations, sensors need to be localized regularly.

In this paper, we propose an original algorithm for sensors localization in imperfect circumstances. The proposed method is an anchor-based method where two types of sensors are considered: anchors, equipped with GPS and thus having known positions, and non-anchor nodes, unaware of their locations, and thus they need to be localized. To do so, nodes collect distance information from neighboring anchors. Collected measurements mainly contain the anchors coordinates. The method assumes that the reliability of such measurements is given. In other words, in this paper, we do not propose a technique for computing measurements reliability. Collected information is then combined using the Dempster-Shafer (Smets & Kennes 1994) and the interval theories (Jaulin, Kieffer, Didrit & Walter 2001). If we consider a specific mobile node, the final solution would be composed of a set of boxes, each of which having a specific weight. Each weight represents the amount of confidence that could be given to the assumption that the corresponding box contains the position of the node. The punctual position estimate would be the center of the box having the highest weight at each time-step. Figure 1 illustrates the estimated trajectory of a node, using five anchors information, two of them at average being erroneous at each step. As shown in the plot, the solutions consist of two-dimensional boxes, whose barycenters define the estimated positions. Using this technique, one is able to compute accurate estimates of nodes positions, even when erroneous measurements may occur.

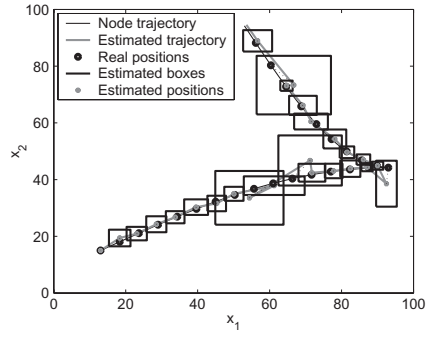


Figure 1. Estimation of a node trajectory using the proposed method.

REFERENCES

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks 38*, 393–422.

Jaulin, L., Kieffer, M., Didrit, O. & Walter, E. (2001). *Applied interval analysis*. Springer.

Shorey, R. (Ed.) (2006). *Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions*. John Wiley & Sons.

Smets, P. & Kennes, R. (1994). The transferable belief model. *Artificial Intelligence 66*, 191–234.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Leak detection in the lubrication system of an aircraft turbine engine

L. Rakoto & M. Kinnaert
Université Libre de Bruxelles, Brussels, Belgium

M. Strengnart & N. Raimarckers
Techspace Aero, Milmort, Belgium

ABSTRACT

This paper deals with a method for detecting leaks in the lubrication system of an aircraft turbine engine during flight. Leak detection in the lubrication system is usually performed by the monitoring of the oil level in the tank. However, the measurement of the oil level is affected by the oil consumption, the thermal expansion, the gulping and the attitude variation of the aircraft. The gulping represents the oil quantity which is not contained in the tank (i.e. oil hiding in the engine [pumps, pipes, sumps, etc.]).

In order to avoid the use of any additional sensor, a grey box model of the oil tank level variation is developed by exploiting experimental. Contrary to previous work [1], a single model is used for the entire operating range of the engine. Moreover, a systematic parameter estimation, using data recorded from the last flight, is developed to maintain the model accuracy despite the aging of the system. Measurements of the engine speeds, the oil tank temperature and the aircraft attitude are processed by a time-varying Kalman filter, which is designed based on the former model, to provide estimation of the level rate variation. The innovation sequences of the Kalman filter are monitored by several statistical change detection algorithms to detect the presence of a leak in the lubrication system. Validation has been performed using data from an aircraft during normal flight.

REFERENCE

[1] Diez, E., 2008. Diagnostic et pronostic de défaillances dans des composants d'un moteur d'avion. Masters thesis, Université Toulouse. III - Paul Sabatier.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Prognosis applied to an electromechanical system: A nonlinear approach based on sliding mode observer

D. Gucik-Derigny, R. Outbib & M. Ouladsine
Université Aix-Marseille, Domaine Universitaire de St Jerome, Marseille, France

ABSTRACT

In the last decades, diagnosis methodologies were developed in order to detect, to locate and to identify the faults. The proposed methodologies on diagnosis were concerned by fault detection. The main aim is the fault detection in the process. Hence, the methodologies of the diagnosis are adapted for situations after fault occurrence. Afterwards, results were established considering the problem of predictive diagnosis which are devoted to prediction of the fault before its occurrence and as soon as possible. This concept is interesting, however it can be inadequate concerning the economic challenges and for safety.

More recently, a new concept has emerged: the prognosis. The goal of this concept is to estimate the Remaining Useful Life (RUL) of systems and hence to forecast faults occurrence. This paper concerns model-based prognostic.

Throughout this work, it is assumed that the behavior of the considered technological process can be described using a multiple time scale model of the following form:

$$\begin{cases} \dot{x} &= f(x,\theta(\phi),u) \\ \dot{\phi} &= \in g(x,\phi) \\ y &= y(x,\phi,u) \end{cases} \quad (1)$$

where $x \in \mathbb{R}^n$ is the state of fast dynamic behavior. $\theta \in \mathbb{R}^r$ denotes a parameter vector assumed to be a function of $\phi \in \mathbb{R}^q$ the state of damage state. $u \in U \subset \mathbb{R}^m$ designates the input vector where U is a set of admissible controls. The ratio $\in$ is that $0 < \in \ll 1$. $y \in \mathbb{R}^p$ is the output vector. f, g, h are differentiable functions in adequate dimensions. f, h and the structure of g are assumed to be known.

System (1) is used to describe simultaneously the behavior of the process state and the evolution of the damage state. Moreover, the system expresses the interconnection of the two variables (i.e., process state and the damage) and it allows taking into account the time scale aspect induced by the difference of the dynamic behaviors. In fact, the process state is assumed to be with fast dynamic while the damage state is considered with slow dynamic.

Here, the subsystem (1a) describes the behavior of the state of the system and is assumed to be well defined. However, only the structure of the subsystem (1b) is supposed to be known a priori. Generally, in the literature the dynamics for the damage state is supposed to be polynomial function. A main objective is to identify parameters of damage state dynamic behavior (1b).

For that, the strategy consists in estimating unmeasured state for fast dynamic behavior subsystem based on the design of an unknown input observer. Hence, slow dynamic behavior state present in the fast dynamic behavior subsystem is led back to an unknown input. Unknown input sliding mode observer is designed to obtain accurate estimates for state, unknown input and dynamic of unknown input. Finally, parameters of slow dynamic behaviour are then identified.

The problem of unknown input observers synthesis has attracted the interest of several authors and many results were proposed.

In this work, a classical kind of finite time unknown input observer is applied to an electromechanical system for the problem of prognosis. From state estimate accuracy in finite time depends accuracy of parameter identification of slow dynamic behavior model and also the quality of the remaining useful life predictions. Here, our comparison is achieved on an electromechanical system.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

R^2wAC: Recursive redundancy with active comparison

J.G. de Chavarri, J. Mendizabal Samper, A. Villaro, S. Urcelayeta,
J.M. Blanco & A. Galarza
Ceit and Tecnun (University of Navarra), San Sebastian, Spain

ABSTRACT

A fault tolerant system is a system capable of fulfilling its operation without considerable performance degradation and without data corruption, in the presence of failure due to either internal or external causes. These systems are used in systems such as medical systems, aircraft and railway communications systems whose functionality is constrained in terms of Tolerable Hazard Rate (THR).

Safety standards set the maximum THR and define Safety Integrity Levels (SIL). SIL4 is the highest level according to IEC61508 and IEC50129. A SIL4 function implies that the THR of an error in the functionality is set between 10^{-8} and 10^{-9} f/h.

The origin of the errors that can affect the system is considered random. Among the different possibilities, there is one especially important for electronic devices that incorporate S-RAM technology: Single Event Upset (SEU). A SEU is a change of the state or transient induced in a device by an ionizing particle such as cosmic ray or proton (Stott et al., 1998).

Safety critical applications require fault tolerant architectures where computing components present very stringent failure rates. This paper presents a novel programmable logic voter design pattern. Active components are used in the architecture of this voter to improve reliability.

Many techniques can be used to develop fault tolerant systems, most of them based on redundancy. In this case, a hardware redundancy is needed because the component to be designed is a hardware voter.

An active fault tolerant voter system is designed combining the techniques N Modular Redundancy (NMR) (Kshirsagar and Patrikar 2009) and Duplication with Comparison (DwC) (Johnson 1989). The advantages of the previous mentioned techniques are exploited to improve the dependability of the voter and the disadvantages are avoided to offer the best solution in three clearly distinguishable system steps.

The components used in this design are based on modifications of the techniques that are shown in the state of the art: an NMR is used as active component whose performance is different depending on the feedback from the next step; and a DwC is used, that is also changed and controlled by the status signals of previous steps.

With this scheme, the system is able to mask errors, choose a final output signal and offer information of the status in real time. A warning signal is given when there is a component that is not working correctly but the system is able to mask that error. If the component can not mask those faults, it sends an error signal to the output to alert that the signal in the output is not the correct one.

To quantify the safety level of this architecture, a safety analysis is needed. An FTA could provide a quantitative value of the safety level of architecture. In this case, the most critical hazard is when a corrupted message is received as being correct, in which case it is then analyzed.

The safety analysis reveals that this architecture is not a good solution for most safety systems, but thanks to the inherent fault detection and masking capabilities and the reached dependability, it could be a suitable option in particular situations where the system requires a high safety level to work isolated and unmaintained for a long time.

REFERENCES

IEC50129 (2005). Railway applications - communication, signalling and processing systems - safety related electronic systems for signalling.

IEC61508 (2003). Functional safety of electrical/ electronic/ programmable electronic safety-related systems.

Johnson, B.W. (1989). Design and analysis of fault-tolerant digital systems. *Addison-Wesley. 218*, 1–17.

Kshirsagar, R. & Patrikar, R. (2009). Design of a novel fault-tolerant voter circuit for tmr implementation to improve reliability in digital circuits. *Phil. Trans. Roy. Soc. London. 249*, 235–297.

Stott, E., Sedcole, P. & Cheung, P. (1998). Fault tolerant methods for reliability in fpgas. *IEEE Field Programmable Logic and Applications. 415*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Sensor and actuator faults estimation for Takagi-Sugeno models using descriptor approach: Application to Fault Tolerant Control

M. Bouattour
Laboratory of Modeling, Information and Systems, University of Picardie Jules Verne, Amiens, France
Industrial Processes Control Unit, National Engineering School of Sfax, Sfax, Tunisie

M. Chadli & A. El Hajjaji
Laboratory of Modeling, Information and Systems, University of Picardie Jules, Amiens, France

M. Chaabane
Industrial Processes Control Unit, National Engineering School of Sfax, Sfax, Tunisia

ABSTRACT

This note proposes sensor and actuator faults estimation and Fault Tolerant Control (FTC) method for Takagi Sugeno (T-S) fuzzy system. Based on the descriptors systems technique, the idea consists in estimating the faults and then taking them account in the control. The method is based on the simultaneous estimation of state, sensor and actuator faults and then the stabilization by static output feedback. The control and the observer gains are determined by Linear Matrix Inequalities (LMI) conditions. An example is used to show the effectiveness of the proposed strategy.

Human factors and human reliability

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A model-based approach for the collection of human reliability data

S. Massaiu
OECD Halden Reactor Project, Halden, Norway

ABSTRACT

One of the major criticisms against Human Reliability Analysis (HRA) is the lack of empirical data to support its quantitative estimations. While there is increased confidence around the quantification of executions failure probabilities, there is still a great deal of uncertainty when it comes to less well-defined situations and higher-level activities, like diagnosis and decision errors: that is, the conditions that characterize the history of industrial accidents. New methods (second-generation HRA) have been developed to represent more realistically these conditions. Unfortunately, these methods strongly rely on expert judgment for quantification, and although their use strongly encourages event reviews and observation of simulated performance, the link between quantification and empirical evidence is not always transparent.

This paper presents an approach aimed at providing a traceable empirical base to quantification in second-generation HRA methods. The approach is potentially applicable to other aspects of the HRA process, such as scenario analysis and error identification.

The idea is to use a domain-specific modeling approach to convey empirical evidence into the expert-judgment processes of HRA. The model is the Guidance-Expertise Model (GEM) of crew cognitive control, which provides the classification system for collection and retrieval of domain-specific data. The GEM model recognizes and accounts for the dominant role of the emergency procedures during disturbances. In other words, explanation and prediction of operators' behavior under emergencies needs to describe how the procedures are used, since in these situations the operators control the plant largely, if not entirely, through the procedures. The GEM model follows a line of research in industrial settings that describe human performance in terms of distinctive cognitive categories. Consistently with Jens Rasmussen's Skill-Rule-Knowledge taxonomy, the GEM model postulates two control modes, or ways of acting, that the crews display in controlling emergencies with procedures.

In this paper we present a test of the ability of the model to identify regularities between environmental conditions (procedures), crew expertise (teamwork) and crew behaviors. The analysis is based on complex steam generators tube rupture events obtained from four Nuclear Power Plant (NPP) control room crews in the Halden Man Machine Laboratory research simulator.

The test shows that the approach is capable of retrospectively identifying crew behaviors of interest for HRA (e.g., unexpected progressions in the procedures set, responses to cues and extraneous events) and relating these to observable performance conditions. At present stage, the environmental conditions are the procedures and the crews' expertise as measured by the quality of teamwork. The behaviors are not necessarily errors or failures, but represent generic types of crew activity that typically impact the performance of tasks, and as such are part of possible failure stories of emergency systems. Eighteen such behaviors are identified.

The test also highlights environment-cognition-behavior regularities. These are obtained by calculating: 1) the frequency of occurrence of the outcome behaviors in the different control modes and by procedural guidance type; and 2) the frequency of occurrence of positive and negative teamwork dimensions in the different control modes. Given the small sample size, no discussion of these relationships is made, but the results are presented for illustration.

The main benefit of this approach is the possibility of collecting data on emergency operation behaviors and systematically relating them to observable features of the operational environment. These observed patterns could, in turn, constitute a source of empirical support for assumptions made in predictive analysis of scenario evolutions and of system failure that refer to the same environmental characteristics.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Accidents in the gas distribution industry: Some consequences of the introduction of new analysis criteria

G. Desmorat, P. Desideri & F. Loth
Pôle Maîtrise des risques, Gaz réseau Distribution Paris, France

F. Guarnieri & D. Besnard
Centre for Research on Risks and Crises, Mines ParisTech, France

ABSTRACT

The importance of the learning from past experience process is crucial for today's complex businesses. The difficulty of evaluating their degree of organizational resilience and the social and regulatory context imposes strict risk management policies, which drives the development of new safety management tools. Consequently, the development of efficient accident analysis tools is needed. The process of learning from past experience allows capitalization and exploitation of data from event analysis in order to develop prevention policies and barriers to protect the organization.

The design of such a process requires a choice of paradigm. The most common paradigm is based on dependability, which advocates a mechanistic view of accidents and makes the individual one failure factor among many in the system. However, several major catastrophes have driven experts to reevaluate the basic tenets of these methods. This re-evaluation led to the adoption of the Human and Organizational Factors paradigm.

This paradigm is characterized by the idea that an accident is no longer simply a technical phenomenon. Operators' performance is then explained by the influence of the socio-cultural context. Accident analysis framed by Human and Organizational Factors therefore aims to explain people's performance in terms of a context that is prone to failure.

GrDF (Gaz réseau Distribution France) is a company specialized in the distribution of natural gas. Its network is 190,000 km long. The notable feature of this network is the level of exposure to threats such as structural damage due to public works carried out by external contractors. Here, there is a great need for learning from experience which must respond to the high safety standards the company must meet.

To meet this requirement, GrDF initiated a project which led to the creation of an analysis grid based on some components of the CREAM method (Hollnagel, 1998). This will be discussed in detail in the presentation. The concept of Common Performance Conditions (CPC; Hollnagel, *op. cit.*) was used for the understanding of human and organizational factors. The work was carried out jointly with Mines ParisTech. This collaborative approach has allowed knowledge transfer to GrDF bodies responsible for safety management.

That operator's failure is due to the negative influence of the context on performance is an ideological departure for a company shaped by the earlier paradigm of human fallibility. The analysis grid developed by GrDF encourages operators and field managers to adopt this new way of understanding human performance.

This article will present the preliminary results of the grid. Two years of experience have identified several points of resistance and various factors leading to success. The first success factor lies in the interest of operators and local managers in the new tool. It can be taken as a sign that the break with the past has been fully accepted. However, the spirit of the method remains relatively misunderstood. This is illustrated by the persistence of practices influenced by the dependability paradigm.

Two lessons emerge. The first is the critical role of generational and demographic issues in the success of an approach that requires such a major break from past practices. It is easier for young people to make the necessary change in how they see their role, compared to operators with a longer history within the company. The second key point is the importance of internal communication, which has played an increasingly important role over time. These two elements form the main points which help to avoid a drift away from original course of action.

REFERENCE

Hollnagel, E. (1998). *Cognitive Reliability and Error Analysis Method.* Oxford: Elsevier Science.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An approach to predict human reliability in manual assembly

B. Günnel, M. Schlummer & A. Meyna
University of Wuppertal, Germany

M. Schick, F. Heumeni & M. Haueis
Daimler AG, Sindelfingen, Germany

ABSTRACT

As a result of the severe competition in the automotive industry and the continuously increasing customer requirements concerning quality and price, companies are interested in providing a maximum level of quality while keeping their costs as low as possible. Quality and price are significantly influenced by the production of the vehicle itself as the quality, later to be experienced by customers, is generated here. Furthermore, a large proportion of the production costs are caused in vehicle assembly.

Due to the fast-changing automotive market driven by continually changing versions of models, the assembly is carried out manually to a large extent in automotive production. The individual person who performs the assembly is very important since he or she directly affects the quality of the products. To ensure high quality the production system must be extremely reliable, which is determined by human reliability. Therefore it is very helpful to know which human actions or tendencies may reduce the quality of, or create a defect in, the finished product.

The aim of this study is to create an approach, which shall provide a quantitative prediction of human reliability in manual assembly. At present the known methods for predicting human reliability, which use for their assessment task-, time- or PSF- (Performance Shaping Factors) related quantification principles, are not practicable for vehicle production. Thus a new approach has to be generated that regards documents and failure data of the vehicle assembly. Using mathematical and reliability methods to analyze the collected information of the assembly it is finally possible to predict the expected failures in the assembly.

The assessment tool developed by this study is an operation-based model which uses available standardized documents from manual assembly, which allows an early application of the relevant calculations in the product development process. Thereby, a continuous and early adaptability of the created tool in the development process is guaranteed, so that preventive measures can be introduced to raise human reliability and therefore product quality by an optimized product and process design

The new method was adopted in a part of the manual vehicle assembly. The first results of the application show that it is possible to identify the relevant components with a high failure count without any information about the real facts of the assembly. Thereby, no failure data of an examined part of the assembly is required to predict the failures so that the estimation could be realized just before production start.

The results of the first implementation make it clear that further research is necessary to increase the precision of the model. Therefore, an expansion of the used production planning and quality data is being undertaken using statistical methods to optimize and validate the new model. If the model proves to be a practical and accurate approach, its applications in increasing quality and reducing costs in automotive assembly are obvious.

REFERENCES

Association of German Engineers e.V., VDI (ed.) 2003. *Human Reliability—Methods for quantitative assessment of human reliability*. Berlin: Beuth Verlag GmbH.

Bubb, H. 1992. *Menschliche Zuverlässigkeit*. Landsberg: Ecomed – Fachverlag.

Günnel, B. 2010. *Entwicklung eines prototypischen Werkzeuges zur quantitativen Prognose der menschlichen Handlungszuverlässigkeit in der manuellen Montage*. Master-Thesis, University of Wuppertal.

Swain, A.D. & Guttmann, H.E. 1983. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Final Report, NUREG/CR-1278: Washington DC.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Assessing the impact of domain-specific cognitive profiles on the reliability of human operators in the railway domain

M. Arenius & O. Sträter
Fachgebiet Arbeits—und Organisationspsychologie, University of Kassel, Kassel, Germany

M. Hammerl, M. Talg & K. Lemmer
Institute of Transportation Systems, German Aerospace Center, Braunschweig, Germany

H. Franzmeyer & B. Milius
Institute of Railway Engineering and Systems Safety, Technische Universität Braunschweig, Germany

ABSTRACT

Human cognition is tightly coupled to the context in which it operates (Hollnagel, 2004). Thus, any model aiming at capturing the features of cognition relevant for human reliability should consider the nature of the connection between the mind and the working environment affecting and shaping it if valid conclusions on human behavior are to be derived.

The Cognitive Couplings address the principal ways in which human cognition is bound to the working environment (Sträter & Bubb, 2003). They constitute a classification scheme for man-machine interaction in terms of types and levels of cognitive demand associated with a task.

By mapping a pattern of mental demands to the (often very technical) tasks at all levels, a cognitive profile with which the individual has to cope with is obtained, establishing a first link between working environment and its hypothesized effect on cognition.

In order to capture and ultimately quantify the actual effect on cognition and therefore performance, the human adaptive capacities towards these hypothesized configurations of cognitive demand have to be assessed by a model reflecting the coping strategies intrinsic to the cognition system operating upon the profiles (Sträter, 2005). This structured analysis of the domain-bound profiles and their associated impact on cognition has given valuable insights for different domains of work (Arenius, Athanassiou & Sträter, 2010; Günebak, Sträter & Allgaier, 2010).

Thus, the Cognitive Couplings and the associated cognitive profiles serve as a starting point for the reliability assessment of man-machine interaction. Results from the project SMSmod funded by the German Research Foundation (DFG) illustrates the logic for integrating the types and levels of cognitive demand associated with the Cognitive Couplings into a task analysis of train driving. Furthermore, the results are discussed in consideration of the existing barrier systems (Hollnagel, 2008) implemented in the domain of railway transportation.

REFERENCES

Arenius, M., Athanassiou, J. & Sträter, O. 2010. Getting the Feeling – "Human Error" in an educational ship handling simulator. In: GFA (Eds.): Neue Arbeits- und Lebenswelten gestalten. Dortmund: GFA Press.

Hollnagel, E. 2004. Barriers and Accident Prevention. Hamshire: Ashgate Publishing Limited.

Hollnagel, E. 2008. Risk + Barriers = Safety? Safety Science 46(2): 221–229.

Günebak, S., Sträter, O. & Allgaier, S. 2010. Systemgestaltung durch Kombination mentaler Belastungsanalyse und Blickbewegungsaufzeichnung In: GFA (Eds.): Neue Arbeits- und Lebenswelten gestalten. Dortmund: GFA Press.

Sträter, O. 2005. Cognition and Safety – An Integrated Approach to System Design and Assessment. Hampshire: Ashgate Publishing Limited.

Sträter, O. & Bubb, H. 2003. Design of systems in settings with remote access to cognitive performance. In: Hollnagel, E. (Ed.): Handbook of Cognitive Task Design. Hillsdale: Erlbaum.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Bayesian network modelling for fire safety assessment: Part I—a study of human reaction during the initial stages of a dwelling fire

D.B. Matellini, A.D. Wall, I.D. Jenkinson & J. Wang
Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, Liverpool, UK

R. Pritchard
Merseyside Fire and Rescue Authority, Liverpool, UK

ABSTRACT

Providing fire and rescue services is hugely complex due to the sheer number of different potential scenarios which must be covered. Not only are there variations between the types of locations, for example factories, vehicle tunnels, dwellings, etc., but there are also many different circumstances within each type of location. Taking dwellings for instance, there can be variations in terms of size, design, building materials, geographical location, fire safety arrangements, number of occupants, activities of occupants, among others. As for the occurrence of fire itself, each incident will be unique in terms of time of day, type of fire, state of occupants, fire cues, etc. What all these variations signify is that the potential magnitude of the next fire event and its consequences are generally unpredictable. Because of the complicated scenarios, unpredictability of outcomes, and high frequency of incidents, fire and rescue services have to be both capable and flexible in operation; however resources are limited and finding the optimal way of managing fire and rescue services is a complex and ongoing task. This research aims to contribute in some way towards this cause.

Finding an effective and adaptable risk assessment technique which can be applied to fire and rescue planning is an intricate challenge. Whatever the method, it must be capable of dealing with uncertainty both in data and the interrelation of variables, it must be adaptable in terms of being able to model various fire and rescue scenarios, and must provide practical outputs which can then be incorporated into strategic planning. Upon this background, this paper introduces the concept of probabilistic modelling under uncertainty through the application of the Bayesian Network (BN) technique. BNs are also intrinsically effective tools for dealing with situations involving multiple dependencies and complex structures. A model has thus been built to represent fire development within dwellings from the point of ignition through to extinguishment. The model is broken down into three parts; this paper presents part I which tackles the initial fire development and human reaction with parts II and III presented in a follow-on paper. The model incorporates both hard and soft data, delivering posterior probabilities for selected outcomes. Case studies demonstrate how the model functions and provide evidence that it could be used for planning purposes and accident investigation; by varying input values to the model, experiments can be conducted to verify current safety arrangements and to predict the outcome off making changes. Finally, a further development of part I of the model is proposed which would allow studies to be undertaken into social aspects of housing and their effect upon the probability of various fire situations.

SELECTED REFERENCES

Brannigan, V. & Kilpatrick, A. (2000). Fire Scenarios in the Enforcement of Performance-Based Fire Safety Regulations. *Journal of Fire Sciences*. Vol. 18, pp. 354–375.

Communities & Local Government (2004). *The economic cost of fire: Estimates for 2004*. Available at: http://www.communities.gov.uk/

Hanea, D. & Ale, B. (2009). Risk of human fatality in building fires: A decision tool using Bayesian networks. *Fire Safety Journal*. Vol. 44, pp. 704–710.

Holicky, M. & Schleich, J. (2000). Fire safety assessment using Bayesian causal network. *Foresight and Precaution*. Cottam, Harvey, Pape, and Tait (eds), pp. 1301–1306.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Concept of operations for data fusion visualization

T.R. McJunkin, R.L. Boring, M.A. McQueen, L.P. Shunn,
J.L. Wright & D.I. Gertman
Idaho National Laboratory, Idaho Falls, ID, US

O. Linda, K. McCarty & M. Manic
University of Idaho, Idaho Falls, ID, US

ABSTRACT

Data fusion is a collection of techniques by which information from multiple sources is combined in order to reach a better inference. In considering the design of the Human-Machine Interface (HMI), the presentation of the fused data is optimized for end use. Such a design process ideally makes use of first principles and practical experience from human-computer interaction and user-centered design. Yet, extensive insights and experience with such systems remains elusive, and there is currently no specific guidance to help the designer of a data fusion system to present information in an optimized or usable manner. This paper outlines current efforts to create a style guide of design principles for the presentation of data fusion information, specifically for a hybrid fuel production system and generally for a process control context.

Process control involves an operator interacting with a control system to ensure the effective and safe startup, operation, and shutdown of a production process. Process control can take the form of manufacturing and fabrication—including especially chemical processing—to energy production and distribution. The degree of operator interaction with the control room interface varies considerably. A modern, highly automated petrochemical production system may feature an operator in a primarily monitoring role. In contrast, an all-analog power plant control room may feature multiple operators to monitor and actively control energy production.

Current process control interfaces provide key indications on process and plant states such as temperature, flow, pressure, etc. These indications are typically provided for every available component sensor in the system. In analog process control interfaces, these sensor indicators comprise multiple panels across a control room, resulting in hundreds and sometimes thousands of indicators for the operator(s) to monitor. Digital control rooms typically employ the advantages of software windowing technology, allowing sensor readings to be displayed for only the system or components that are of interest, often coupled with an overview Piping and Instrumentation Diagram (P&ID).

Data fusion may encompass both sensor input and alarms. In terms of sensor input in a process control interface, data fusion represents the attempt to group multiple component sensor readings into a high-level system indication. For example, separate indications for temperature, flow, and pressure might be merged into a single gauge. For alarms, data fusion takes the form of aggregating multiple alarms into a single alarm. Two current approaches accomplish such aggregation: alarm filtering and root cause alarms.

A predictor system includes the challenges of data fusion interfaces for existing sensor indicators—the tradeoff between displaying parsimonious indications and providing precise diagnostic information to the operator, and the challenge of down-selecting the most appropriate or relevant alarms. In addition, a predictor system presents new interface issues for data fusion. Most noteworthy of these issues is the fact that a predictor system is an uncertain indication. While the operator may assume a high degree of system integrity and sensor reliability with conventional data fusion, the operator is confronted with the new challenge that the predictor system provides a probabilistic, extrapolated outcome for the process control, but there is no guarantee that such an outcome will actually occur. Essentially, the predictor system must win and maintain operator trust.

This paper presents a process that is being used to arrive at a style guide for data fusion interfaces in process control as well as for the inclusion of predictor system data in data fusion interfaces. Currently, no clear guidance exists to determine the optimized presentation of fused sensor data in process control. By employing a concept of operations approach to data fusion interface design, initial design guidance has been crafted.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Developing and evaluating the Bayesian Belief Network as a human reliability model using artificial data

Y. Stempfel & V.N. Dang
Paul Scherrer Institute, Villigen PSI, Switzerland

ABSTRACT

A frequent assumption of Human Reliability Analysis (HRA) methods is that Performance Shaping Factors (PSFs) are independent in terms of their effects on the human failure probability. This work examines the Bayesian Belief Network (BBN) as a means to model the factors and to estimate failure probabilities when this assumption is set aside. The development and testing of the BBN, as well as the comparison of the BBN model with a more traditional model, is based on the use of artificial data sets. Artificial data refers to the generation of data with known properties, in order to test a modeling approach and evaluate its performance. In this case, the data represents a series of observations of performances, each with a set of PSF ratings and a record of whether a human failure event occurred. It is used to train a BBN and determine its parameters. The resulting BBN model's predictions of the failure probabilities are compared against the empirical (artificial) failure probabilities. In addition, the BBN model is compared against a traditional PSF-HFE model; in this case, a model with PSF multipliers is selected.

The results show that the BBN model was able to capture the relationships among the factors and, in particular, to estimate the HEPs fairly accurately. The empirical HEPs to be predicted ranged from 0.03 to 0.74. The maximum error for the set of PSF configurations defined to be of most interest was 30%, for a configuration with very few observations (26 observations in the overall sample of 10000) and a probability of occurrence of 0.12. The average absolute percentage error was 8%.

A key assumption of the artificial data was that in addition to their individual effects on performance, some PSFs interacted producing an additional contribution to the HEP. In other words, their joint effect was more than the sum of their individual effects. The formalism of the BBN clearly supports the modeling of such interactions. To investigate whether this interaction term could be neglected, a multiplicative model was fitted to the data. As expected, it performed poorly on all configurations where more than one PSF was LTA (Less than Ade-quate).

Third, the performance of the BBN with smaller data sets was evaluated. Instead of five sets of 2000 observations, five sets of 500 observations were used. A few of the HEPs estimated with the BBN model were moderately accurate in HRA terms (percentage error less than 50%). It was found that the critical determinants of the model performance, not surprisingly, were the inclusion of the relevant PSF configuration in the data set and the observation of some HFEs for these configurations.

Among the strengths of the BBN is the ability to combine expert judgment with data within a structured framework. In this examination, expert judgment input to a BBN model was not used, focusing instead on learning from data. The performance of the BBN was favored by not including any distortions in the data (discrepancies in the PSF ratings in the data set resulting from unreliable ratings) or missing data. On the other hand, the error mechanisms were assumed to be completely unobservable. Expert judgment on the structure of the model and the observability of the error mechanism can be expected to increase the performance of BBN models. Consequently, treating these and other aspects of realistic data while incorporating expert judgment into the modeling process are important topics for future work.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Implementing of new methods for assessing human risk in maintenance

R. Doležal
Department of Dependability and Risk, Technical University of Liberec, Liberec, Czech Republic

ABSTRACT

Popularization and actual implementation of new methods of assessing human performance in maintenance faces many challenges. In order to successfully fulfill their role, their real application has to be approved by company management and also have influence the organizational structure and provide the necessary new managerial control. This managerial control becomes a major obstacle to the implementation of these methods in practice.

During the implementation of practically any methods for optimizing maintenance, we encounter the same problems and same questions from maintenance personnel. Often are identified critical decision of management with a much greater impact on effectiveness and safety of maintenance than the process that is "necessary to optimize".

They are also identified very critical relationships with outside firms engaged in the maintenance of some equipment. Communication, sharing risk and the attempt to own profit of these companies often adversely affects the reliability, maintainability and safety. In many accidents have been identified these problems as a key factor in negative course of accident scenario. Although the relationships of outside firms are under intense supervision—the supervision is not methodical and built on solid theoretical grounds, which are today already available.

Risk assessment includes risk identification, risk analysis and risk assessment. The organization should identify sources of risk, the impact of events and their causes and potential consequences. The aim of this approach is to create a comprehensive list of risks. List of identified risks should include a risk regardless of whether the organization is able or wants it to inspect and check.

For each identified risk must be developed also its criteria. These criteria should reflect values, goals and resources of the organization.

Complete list of accepted (decided) risks associated with technology should be transparent tool for managerial control. This list can be entered into logical hierarchical tree, as well as other appropriate graphic diagrams showing the flow of risks in the organization. The basic inputs should be self-reports. They should be properly assessed and controlled methodologically in managerial control. By using the tools of agent theory should be constantly examined whether the values correspond to reality, and if taking risk is adequate and meets the goals of the organization.

These experiences will be explored in the coming years in a research project in selected chemical and petrochemical plants. It will investigate the effect of managerial control to company risk, together with the results of real application of agency theory knowledge. The project will also focus on new methods of assessing human performance in maintenance.

Figure 1. Risk Flow in hierarchy.

REFERENCES

Dhillon, B.S. 2009. Human Reliability, Error, and Human Factors in Engineering Maintenance: with Reference to Aviation and Power Generation, CRC Press, ISBN: 978-1-4398-0383-7.

Doležal, R. 2010. A stand with human factors in maintenance. In Reliability, Risk and Safety. Taylor & Francis. pp. 1781–1785. ISBN 978-0-415-60427-7.

Eisenhardt, K. 1989. Agency Theory: An Assessment and Review. In The Academy of Management Review. 14: pp. 57–74.

ISO. 2008. Risk management—Principles and guidelines on implementation. ISO 31000, International Organization for Standardization.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Information foraging in nuclear power plant control rooms

R.L. Boring
Idaho National Laboratory, Idaho Falls, ID, US

ABSTRACT

Information foraging theory articulates the role of the human as an "informavore" that seeks information and follows optimal foraging strategies (i.e., the "information scent") in finding meaningful information. This theory has been successfully applied to human-information interaction environments such as Internet use. There are considerable differences between consumer Internet surfing and operator interactions with control rooms in nuclear power plants. A major difference is that the information in control rooms has already been distilled to only the information that is relevant to some aspect of operations. Nonetheless, information needs vary considerably across different power and operation modes of the plant, and the operator needs to navigate to the most relevant information amid an abundance of plant indicators.

This paper briefly reviews the findings from information foraging theory outside the nuclear domain and then discusses the types of information foraging strategies operators employ for normal and off-normal operations in the control room. For example, operators may employ a predatory "wolf" strategy of hunting for information in the face of a plant upset. However, during routine operations, the operators may employ a trapping "spider" strategy of waiting for relevant indicators to appear. This delineation corresponds to information pull and push strategies, respectively, both of which are found in the control room. Yet, no studies have been conducted to determine explicitly the characteristics of a control room interface that is optimized for both push and pull information foraging strategies, nor has there been empirical work to validate operator performance when transitioning between push and pull strategies.

This paper explores four examples of control room operators as wolves vs. spiders in terms of information foraging:

- Cases of information masking, in which the plant provides specific indicators of plant status, but these indicators may be absent or misleading. Such incidents are examples of operators following the wrong information scent or overrelying on a particular patch of information—i.e., over-foraging.
- Display layouts that optimize for foraging strategies in operator searches for information. Failing to provide indicators along a relevant foraging path may result in operators consistently overlooking or ignoring these indicators. While in practice, this is not different than designing a good layout, information foraging offers a sound theoretical basis for explaining good display layout as one optimized for information search strategies.
- Automation of plant functions, in which operator engagement is lost with some automation systems. By applying a varying process of push and pull information display, it is possible to help maintain operator engagement through creating a dynamic interaction between the plant and the operator.
- Alarm response, in which current annunciator systems feature a high number of nuisance alarms, which drive operators down the wrong information path. Similarly, alarm flooding results in an overabundance of push information. The problem may be recast not simply as information overload but as information scent overload. The key to effective alarm systems may be the effective management of the information scent provided to the operator.

Information foraging strategies are reviewed in terms of how they increase or decrease the operators' opportunity for successful operations. This paper concludesby proposing a set of research questions to investigate information foraging in control room settings.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Integration of human factors in project uncertainty management, a decision support system based on fuzzy logic[1]

S. Hassanzadeh, F. Marmier & D. Gourc
Université de Toulouse, Mines Albi, Centre Génie Industriel, Albi, France

S. Bougaret
Pharmaceutical R&D Management Consulting Company, Francarville, France

ABSTRACT

Project management involves making decisions in a context of uncertainty. These decisions result from some inference rules on some quantitative or qualitative variables, with usually uncertain values that come from different sources and could become progressively complete and precise. Generally, it is only at the end of the project that precise and accurate values of most variables are available. However, a project manager has to make decision, throughout the different phases to make the project evolves, even if the information is uncertain or the inference rules are not strict.

It might be difficult to process all the uncertain information and alarm signals in the decision-making process. In such circumstances, usually the decision-maker adopts a reductive approach to make a decision only based on the piece of information that is available and looks more important. In doing so, the risk is that the decision is made without some crucial information.

We propose a Fuzzy Decision Support System (FDSS) that takes into account both quantitative and qualitative variables and tolerates the lack or imprecision of information. In this approach, a sequence of decisions leads to a final choice, taking progressively into account new information. Human representation and reasoning mode are modeled respectively by fuzzy sets and fuzzy inference rules.

The basis of this approach is our definition of uncertainty that includes both subjective and objective aspects contributing to identification of uncertainty. A typology of uncertainty generators is then proposed that helps explore its sources. The proposed typology is based on three axes: subject (manager), object (project), and context (organization).

The main elements of the model are as follows: 1) input variables (criteria, parameters with different degrees of uncertainty) on which decision is based, 2) output or decision modalities which specify possible options, 3) inference rules (that are usually non-strict) to designate a modality of the decision to each combination of the values of input variables.

The main steps of the proposed approach are as follows. First, the variables that influence decision are identified, collected, and organized according to the classes of the proposed typology of uncertainty generators. The typology helps complete the list of variables and gives the variables a structure. Second, a set of characteristics that describes each variable is established. Third, the availability of each variable according to different project's phases is studied. Fourth, the variables are evaluated and ordered according to the importance of their impact on the decision. Fifth, the inference rules are created, taking into account the order of the importance of the variables.

An application case for a ski resort project illustrates the proposed method. The main characteristics of our problem are gathered in this case study: a series of decisions based on uncertain and dynamic information that becomes more accurate step by step. The application case is based on 3×3 formula, that is a strategy to help a guide decide whether to change his itinerary to avoid avalanches, developed by Werner Munter, a Swiss mountain guide.

The results are compared with a naive decisional approach to cope with uncertainty and shows the proposed approach is effective.

[1]This work was supported by the Foundation for an Industrial Safety Culture (Fondation pour une Culture de Sécurité Industrielle).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Offshore supply vessels design and operation: A human factors exploration

V. Rumawas & B.E. Asbjørnslett
Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

ABSTRACT

This article is a part of a study which investigates human factors in marine design. The study was triggered by the fact that most accidents at sea were caused by human errors or human related factors (McCafferty & Baker, 2006, Moore, Bea & Roberts 1993). Some experts blame that less adequate design is one significant factor that lead to human errors (Meister, 1971, Reason, 1990, Perrow, 1999). A prior study shows that there are more than sufficient standards and guidelines that regulate designers to consider human factors in marine design (Rumawas & Asbjørnslett, 2010). The scope of this article is to check if the reality complies with the regulations, by doing field surveys. The Offshore Supply Vessels (OSVs) are taken as the sample of the study. An exploratory research was conducted by using qualitative approaches which includes observation method, interviews and discussions. Some problems were identifiedin previous study (Hansson, 2006):

– A deckhand hit by the hook in the head
– Person squeezed between moving containers
– A deckhand fall against a hose
– Person slip or twisted a foot
– Fall caused by slippery deck or obstacles
– Fall down the ladder
– Collision between vessel and installation.

Collisions and contacts were some of the most severe incidents recorded, while accidents on the deck during loading unloading at sea were one of the most frequent. Some improvements in the vessel's design are identified, such as increasing the height of bulwarks or side walls to prevent water on deck, installing automated cargo securing system, and developing hose securing system. Some efforts in the operating procedures are also recognized, likeforbid 'cherry picking', the five-hundred meter safety zone restriction,voyage planning and no deckhand is allowed to help suspended cargo. A set of guidelines is published to ensure and improve the safety of offshore supply vessels operations (NWEA, 2009).

Most incidents mentioned in Hansson (2006) have been prevented, but the risk of being hit by the hook and falling down from the ladder still exist.

Further exploration was conducted to assess habitability, workability, controllability, maintainability, maneuverability, survivability, and safety on board (LR, 2008).

Some typical problems were still found, such as disturbing noise, ergonomics issues, layout and arrangement related problems, flooding of alarms, and limited space. However, significant improvements were also noticed. Some novel problems were identified:imperfect automation, abundant checklists and procedures, redundant data entry, and overflow of information are among those downsides.

It can be concluded that human factors is already been considered seriously in OSV's design. Theresult is not perfect, but is improving.

REFERENCES

Hansson, L. 2006. *Safety Management for Prevention of Occupational Accidents.* Doctoral thesis at Norwegian University of Science and Technology. IMT-2006-17. Trondheim: Tapir Uttrykk.

Lloyd's Register (LR). 2008. *The Human Element An Introduction*. Booklet. ISBN 1-900839-31-8.

McCafferty, D.B. and Baker, C.C. 2006. Trending the Cause of Marine Incidents. *Learning from Marine Incidents Conference.* London, 25–26 Jan 2006. RINA, London, UK.

Meister D. 1971. *Human Factors: Theory and Practice*. Wiley Series in Human Factors. USA: John Wiley & Sons, Inc.

Moore, W.H., Bea, R.G. and Roberts, K.H. 1993. Improving the Management of Human and Organization Errors (HOE) in Tanker Operations. *Ship Structures Symposium*, Arlington, Virginia.

NWEA *Guidelines for the Safe Management of Offshore Supply and Rig Move Operations*. Updated June 2009. [Online: http://www.nwea.info/]

Perrow, C. 1999. *Normal accidents: living with high-risk technologies*. Princeton, NJ. Princeton University Press.

Reason, J. 1990. *Human Error.* Cambridge: Cambridge University Press.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Participant motivation in experiment of emergency operating procedures

F. Song
Shanghai Nuclear Engineering Research & Design Institute, Shanghai, China

S. Xu & Z.Z. Li
Department of Industrial Engineering, Tsinghua University, Beijing, China

ABSTRACT

Operators in emergency response are often subjected to high pressure and fear of accidents. It is highly expected that in an emergency related experimental study, such pressure and fear could be simulated. However, this is very difficult since participants of the experiment know well that their performance will not cause any catastrophic consequences. Except possibly introducing anxiety and flurry, the pressure and fear would make the operators more accountable and responsible and thus would try their best effort in task performance. It was hypothesized that participants could be motivated to make their best effort during an experiment, so that the experiment results would more likely to represent human performance in emergency response.

The objective of this study was to examine whether motivation by performance-based payment could improve the performance of participants in the experiment of computerized EOPs of Nuclear Power Plants (NPPs).

Totally nineteen participants were recruited to participate in the between-subjects experiment. They were arranged into two groups: fixed payment group (10) and performance-based payment group (9).

The experiment platform of the SGTR (Steam Generator Tube Rupture) procedure was developed by Microsoft Visual Basic™ and Microsoft Access™. Time pressure was applied and simulated by using a clock at the up-right corner of the screen showing the left operation time of the current step. Operation time and error for each step of the SGTR procedure were recorded automatically for later data analysis.

Dependent variables include average procedure completion time and error rate. The participants were aware of their errors because of the termination of current trial, and could have a subjective feeling of their completion time, but no information on their overall performance and the corresponding payment were provided during the test.

It is surprising that the performance, either error rate or completion time, under the performance-base payment method seemed to be even a little worse than the fixed payment method, although statistical analysis indicated that the differences were not significant. The standard deviations associated with the performance-based payment method were greater than those with the fixed payment method. One explanation to this phenomenon is that the group with the performance-based payment method might be distracted by considering the payment, and thus showed worse performance under the condition that there was certain time pressure.

Motivation by performance-based payment did not show its supposed positive effect on improving the performance of the participants, but it seemed to cause the participants unable to concentrate their effort on performing the emergency operating procedure.

This study may suggest the application of time pressure and determination of suitable payment—to be good for the participants but not based on performance, in an emergency related human factors experimental study.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Pendulum shifts, context, error, and personal accountability

H.S. Blackman & O.V. Hester
Center for Advanced Energy Studies, Idaho National Laboratory (INL), ID, US

ABSTRACT

In recent years the quality of human performance causal investigations has drastically improved. A variety of processes, tools and techniques have been developed and applied across many industries. What has resulted is a balanced and deeper understanding of why a specific event occurred and why a given individual acted in a certain way. Prior to this advent, these analyses were primarily focused on who took what action and then simply remediating that individual—often through training, procedure modification and/or some form of punitive measure.

What was long overlooked was the contribution of the machine system, organization system, and specific situational context to the event itself. Today INL spends a great deal of effort studying these aspects of events to identify existing (Latent) Organizational Weaknesses (LOW), and to understand the context of the event itself, in order to fully appreciate what was in the mind of the person(s) involved. INL efforts to look at human error as a symptom that is systematically connected to features of people's tools, tasks, and operating environment has assisted it in progressing toward a culture where the reporting of events and near misses is more common, and individuals feel empowered and safe in doing so, ultimately resulting in better performance and safety for the organization. These efforts have also helped INL think about the issue of individual accountability and culpability in a new way that takes into account many of the situational and organization factors that influence human behavior—continually moving toward what has been termed a "just culture." Within a just culture, "an atmosphere of trust exists where employees are encouraged, even rewarded, for providing essential safety-related information—but in which they are also clear about where the line must be drawn between acceptable and unacceptable behavior." (Reason 1997).

INL emphasis on latent organizational weaknesses (LOWs) has created a new problem: a tendency to attribute *all* undesired behaviors to LOWs; this "over correction" has unintended consequences. It has led the organization away from the human component that includes personal accountability and understanding the intrinsic elements of why undesired behaviors occurred. This occurs when investigators explain "what" people failed to do or should have done without explaining why an individual did what they did. Investigators may stop short of asking those final "tough" questions and instead superficially apply tools and processes that lead to more antiseptic and easy answers. Further, it diminishes expectations for institutional honesty and accountability and inhibits organizational learning. Not every event or incident is due to a weakness in the organization; often, a lapse, omission, or error by one person or a very few people results in degradation of the safety envelope, process disruption, a near miss or even injury. Humans make errors, and a balanced accountability for those errors is a necessary part of a just culture. If a human error is mislabeled as a LOW, the resulting remedy potentially fails to address the true cause. Both safety and institutional honesty can be weakened as a result.

The goal is to achieve a balance in understanding LOWs and the human component of events (including accountability) as the INL continues its shift from a culture of fear (where people are afraid to report due to unjust reprisal and action) to a reporting culture (where people are accountable and interested in making a positive difference—and want to report because information is handled correctly and the result benefits both the reporting individual and the organization).

This paper discussed our model for understanding these interrelationships; the initiatives that were undertaken to improve overall performance.

REFERENCE

Reason, James. 1997. Managing the Risks of Organizational Accidents. Ashgate Publishing Company.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Quantitative retrospective analysis of CREAM in maritime operations

Z.L. Yang & J. Wang
Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, UK

ABSTRACT

Modern shipping activities are carried out via a highly sophisticated man-machine system within which technological, social and environmental factors often contribute to the occurrence of human action failures. Due to the high risks caused by such failures, human reliability analysis (HRA) has always been a serious concern of maritime safety analysts. However, the problems of subjectivity and lack of data, together with the complexity of operator behaviour involved, have weakened the applicability of well-established HRA methods (i.e., Cognitive Reliability and Error Analysis Method (CREAM)) in the maritime context. The prospective quantification process of a Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel, 1998), normally producing an interval approximation analysis result, cannot provide a quantitative point estimate of the consequences of human performance on maritime system safety.

This paper therefore develops a generic methodology in which the prospective analysis of CREAM is modified to facilitate the quantification of maritime human failures by effectively incorporating both fuzzy evidential reasoning and Bayesian inference logic. The kernels of the proposed framework are to use evidential reasoning to establish fuzzy IF-THEN rule bases with belief structures and to employ a Bayesian inference mechanism to aggregate all the rules associated with a seafarer's task for estimating its failure probability. To realise this aim, a five step HRA methodology is developed to include:

1. Construct a rule base to model the relations between the CPCs and four COCOMs.
2. Assign belief degrees to the four control modes.
3. Use BN to adjust CPC dependency.
4. Aggregate rules using Bayesian reasoning.
5. Validate the model developed.

Consequently, the framework can be used to model the relationship between the nine Common Performance Conditions (CPCs) and the four control modes in the Contextual Control Model (COCOM) in a realistic and systematic way. The multiple-input multiple-output rule concept, together with evidential reasoning, makes estimation of human failure probabilities reasonable in a way of being sensitive to the minor changes of fuzzy input. It also makes it possible to realise the instant calculation of human failure probabilities in specific task analysis onboard ships. The advantages of the newly developed method are shown through the illustrative example of analysing an oil tanker COP shutdown scenario. The outcomes of this work can also provide safety engineers with a transparent tool to realise the instant estimation of human reliability performance for a specific scenario/task.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Tailoring the HEART technique for application in the rail industry

W.H. Gibson, C. Dennis, K. Thompson & A. Mills
RSSB, London, UK

B. Kirwan
EUROCONTROL, Bretigny, France

ABSTRACT

Human error is a key contributor to risk in both existing and future railway systems. Human Reliability Assessment (HRA) can be used to assess human performance and to better understand the contribution of human performance to risk. Human error quantification can be a critical element in HRA. One approach which continues to be used and adapted across industries is the Human Error Assessment and Reduction Technique (HEART). It has been identified that developing an understanding of how the HEART approach can support quantification in the rail context, would provide benefits in terms of more efficient, and greater consistency in, assessments. This approach was selected in preference to developing a new rail-specific quantification technique, as it means that there are less significant issues with technique validation. This initial project reported in this paper had a particular focus on train driver tasks, although the method is designed to be generic for rail tasks. The paper particularly focuses on the HEART Generic Task Types.

The review of Generic Task Types has aimed to define the HEART GTTs in the context of a generic model of human performance and train driver tasks. This process has led to the removal of some existing GTTs and addition of new GTTs.

The EPC review has been based around grouping the EPCs into topic areas and reviewing the EPC set against performance shaping factors used in other techniques.

Users will also be supported through the development of guidance on potential overlaps between EPCs, and between GTTs and EPCs, and fuller definitions and guidance for GTTs, EPCs and estimating the assessed proportion of affect.

The revised approach will be presented to technique users as a paper-based manual with an excel calculation sheet. In addition, guidance will be developed which aims to define the strengths and limitations of the approach and place it in the wider context of human reliability assessment. Detailed plans for delivery of this information to the GB industry will be developed based on consultation with industry stakeholders. Testing of the usability of the tool with users is also planned.

Quantified risk assessment or probabilistic safety assessments, and the use of human reliability assessment are not mandated for the GB rail industry. There will therefore not be a mandated requirement for the tool to be used within the industry. However, human error quantification forms a component of a range of safety assessments, and the GB industry-wide safety risk model is a quantified risk assessment which includes human error probability data (www.safetyriskmodel.co.uk).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Task Analysis and modelling based on Human-Centred Design approach in ATC work

S. Inoue & Hisae Aoyama
Air Traffic Management Department, Electronic Navigation Research Institute, Tokyo, Japan

K. Yamazaki
Department of Design, Chiba Institute of Technology, Chiba, Japan

K. Nakata
Informatics Research Centre, University of Reading, Reading, UK

K. Furuta
Department of Systems Innovation, The University of Tokyo, Tokyo, Japan

ABSTRACT

To accomplish the mission smoothly, we need to have good cooperation with human partners and artefacts in a complex systems. In particular, it is a critical factor to establish good relationships between human partners and artefact systems. This type of system is also the work of Air Traffic Control (ATC). The tasks involved in ATC make heavy demands on the information processing capacities of air traffic controllers. Air Traffic Controllers are expected to continue maintaining the safety of the air space and maintaining air traffic flow to run smoothly in such a complex systems. As the work and tasks of controllers become more complex and the volume and types of information required to carry out these tasks become increasingly larger and more complex, the need for systems that are designed to support controllers becomes greater. In this situation, the cognitive aspects of ATC have not yet been studied sufficiently, in particular with regard to teamwork settings, and no consistent measures for ATC performance assessment have been established either. Controller teams are presently in charge of ATC; it is expected that good team cooperation can contribute to reducing their workloads and preventing human error. Team cooperation processes, however, have not yet been understood well compared with individual cognitive processes. Thus, we need to understand the details of the basic functions of the air traffic controller tasks in the system, in order to design more reliable interfaces and training programs for the controllers. Moreover, to be of use, supporting systems require an accurate model of the controller's behaviour. In this research, we focused on the task analysis of air traffic controllers in actual en-route ATC in an experimental activity based on a Human-Centred Design approach. We discuss the method of design to develop a system of human consciousness, especially for Air Traffic Controllers. And then, we attempt to help a good understanding of the knowledge structure and logical relations of ATC expertise.

Though the HCD process is defined with ISO13407 or ISO9241-210(2010) shown in Figure 1, in this paper, we try to consider the method of using the analysis technique based on the distributed cognition which is devised as a method of the analysis to understand the situation. In order to design the system that can assure system safety, enhance usability, and support human reliability in the future, the idea of HCD process can help a developer's engineer for considering the feature in the control system operation and the intention of the controller. In this paper, firstly, we propose the observation survey technique that can obtain the result of the survey in which effectiveness is high in the process of the human centred design that can be simply executed compared with a conventional technique.

Moreover, we attempt to analyze and model interactions that take place in current en route ATC work based on distributed cognition. Distributed cognition is one of the analysis methods in ethnomethodology that serves as a framework for understanding interactions between people and technology so as to inform the design of interactive systems (Hollan et al., 2000). We have taken the activity of a cooperative team of en route controllers as the unit of analysis from cognitive process perspective. We discuss the application of ethnographical analysis in en route controllers' work as team, and report on findings from ethnographical analysis.

REFERENCES

Hollan, J., Hutchins, E. & Kirsh, D. 2000. Distributed Cognition, ACM Trans. on Computer-Human Interaction, Vol. 7 (2), 174–196.

ISO 9241-210:2010. Ergonomics of human system interaction - Part 210: Human-centred design for interactive systems (formerly known as 13407), International Organization for Standardization (ISO), Switzerland.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Teamwork competencies required by members of integrated operations teams in the petroleum industry

A.B. Skjerve & G. Rindahl
Institute for Energy Technology, Halden, Norway

ABSTRACT

Introduction of the operational concept Integrated Operation (IO) by petroleum companies operating on the Norwegian Continental Shelf implies an increased use of distributed teams (IO teams) in operation of petroleum installations.

To develop teamwork training programs for members of IO teams, it is necessary to understand what teamwork competencies IO team members need to work proficiently as a team. This paper accounts for the development of the MAITEC model. The model comprises what is suggested to be ten main attributes of IO teamwork competence: IO-mindset, IO team-technology competence, team leadership, inter-personal relations, inter-positional resources, personal resources, communication, shared situation awareness, mutual trust, and decision making (see Figure 1).

These ten teamwork competencies are taken to *jointly* constitute the central part of the teamwork competence, i.e., the *skills*, *knowledge* and *attitudes*, required to work in an IO team. The teamwork competence attributes are distributed across four layers, centering on the attribute *decision making*. The model assumes that the attributes at the outer layers are needed to achieve *practical excellence in an IO setting* with respect to the attributes located at the inner layers.

The MAITEC model was developed based on a literature survey. The survey comprised 30 papers on co-located teamwork, distributed teamwork, and/or teamwork in offshore operation. It was structured in three parts. The first part aimed at identifying generic attributes of teamwork competence, and was based, mainly, on studies of co-located teams. The second part focused on establishing attributes of teamwork competence based on studies of distributed teams. The last part aimed at understanding the attributes of teamwork competence required in offshore operations.

The content of the MAITEC model was assessed in an empirical study. The research questions were: 1) Do the attributes of teamwork competence contained in the MAITEC model adequately cover the competencies observed in practice? 2) Are the inter-relationships between the attributes of IO teamwork competence sufficiently pronounced to validly use a layered structure in the MAITEC model? The study was based on observations of 19 morning status meetings in an IO team, across the period 2008–2010. The outcome of the empirical study did not disprove the significance of the attributes contained in the MAITEC model, nor did they indicate that the layered structure was not valid.

The next step will be to further assess the MAITEC model based on date obtained in other teamwork settings of IO teams.

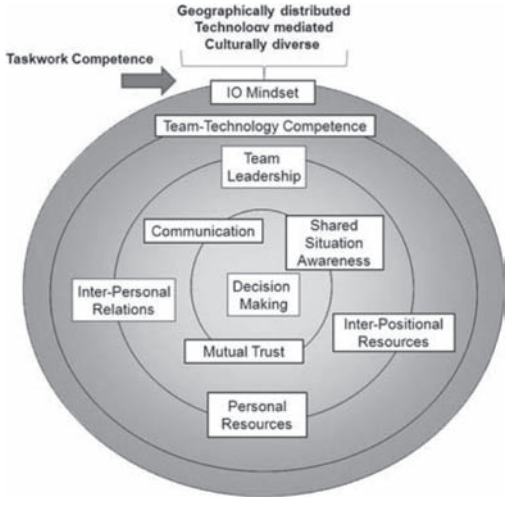


Figure 1. The MAITEC model of the main attributes of IO teamwork competence (Skjerve, 2009).

REFERENCE

Skjerve, A.B. 2009. IO Teamwork Training. In: A.B. Skjerve & M. Kaarstad (eds.), *Building Safety. Literature Surveys of Work Packages 2 and 3,* IFE/HR/F-2009/1388, 94–143. Halden: Institute for Energy Technology.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The development and application of CARA—a HRA tool for Air Traffic Management systems

B. Kirwan & A. Kilner
Eurocontrol, Bretigny, France

W.H. Gibson
RSSB, London, UK

D. Piccione
FAA, US

M. Sawyer
TASC Inc, Washington DC, US

ABSTRACT

Air Traffic Management (ATM) is a highly human-centred operation, with air traffic controllers handling live traffic every day. It is also a very safe industry, with a very low accident rate. In the coming decade there will be significant developments in ATM infrastructure and automation, in an effort to improve efficiency and capacity given the anticipated growth rate in Europe and the US in air traffic. It is essential that such high human performance and safety levels are maintained. This paper documents the CARA HRA approach for the ATM industry.

This paper charts the development and application of a Human Reliability Assessment (HRA) tool called CARA (Controller Action Reliability Assessment). CARA is thematically based on the HEART and NARA HRA approaches, rendered into the ATM context and populated with data from the air traffic industry, both from live operations and high fidelity human-in-the-loop simulation studies. The tool has been applied to several early safety cases, and has been found to be useful. At present the tool supplants the widespread use of engineering judgement, and the avoidance of quantifying the human element in many system change proposals, and so offers an advance in safety capability for the industry. CARA has recently been proposed as a way forward in the EUROCONTROL/FAA Action Plan 15 White Paper on Human Performance and Safety, which has recently received tacit endorsement by the European Aviation Safety Agency (EASA). The CARA approach is already documented and exists on the web. http://www.thinkresearch.co.uk/HRA/index.html

The paper describes CARA and the data underpinning it, as well as early applications in both Europe and the USA, the first an aircraft landing ('Approach') study, the second data communications for arrival route and taxiway instructions, showing the types of insights gained and how they help designers. The case for using CARA, and for it becoming part of the safety risk management 'machinery, as well as further development needs, are outlined in the paper.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The meaning of human performance data observed from simulator studies on human reliability analysis

Jinkyun Park & Wondea Jung
Korea Atomic Energy Research Institute, Daejeon, Republic of Korea

ABSTRACT

It is well perceived that several key factors are crucial in securing the safety of socio-technical systems, such as Nuclear Power Plants (NPPs).

Of them, the importance of human performance related problems has been demonstrated over the past several decades through well publicized events (Forester et al., 2009). Accordingly, extensive effort has been continuously spent on understanding why the performance of human operators deviates from certain expected level (i.e., human error). In the case of NPPs, one of the main activities to answer this question is to carry out a Human Reliability Analysis (HRA).

Unfortunately, although there are significant benefits in conducting HRA, many people have criticized the quality of HRA results because of a lack of available data (Boring 2009; NEA 2009). Subsequently, in many countries, the use of full-scope simulators has been regarded as one of the most cost- and effort-effective alternatives to unravel this problem. In other words, the full-scope simulator is very useful tool for understanding human behaviors that can result in human performance related problems, since it allows HRA practitioners to systematically observe human behaviors in coping with a hypothetical accident (Boring 2009, Forester et al., 2009, NEA 2009). Thus, it is possible to anticipate that a set of serviceable data or insights that are indispensable for conducting HRA can be elicited from simulators.

However, the use of human performance data observed from simulators is still careful because of the appropriateness of human performance data observed from simulated conditions. In other words, it is necessary to answer a critical question such that: are human performance data obtained from simulated conditions comparable with those from a real world?

From this concern, human performance data that have been collected by KAERI (Korea Atomic Energy Research Institute) for over 10 years are reinvestigated in this study. In this regard, major findings extracted from plant-specific and domain-specific human performance data were compared with those identified from operating experience and existing studies. As a result, it is expected that human performance data observed from simulated conditions can be used as a reliable data source for HRA to some extent, especially under the situation in which human operators have to accomplish the required tasks using a procedure.

REFERENCES

Boring, R.L. 2009. Using nuclear power plant training simulators for operator performance and human reliability research. In Sixth American nuclear society international topical meeting on nuclear power plant instrumentation, control and human-machine interface technologies (NPIC&HMIT), 5–9 Apr. Knoxville:Tennessee.

Forester, J.A., Cooper, S.E., Kolaczkowski, A.M., Bley, D.C., Wreathall, J. & Lois, E. 2009. An overview of the evolution of human reliability analysis in the context of probabilistic risk assessment, Sandia Report, SAND2008-5085.

NEA. 2009. Workshop on simulator studies for HRA purposes. 4–6 Nov. Budapest:Hungary.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The right HRA model for the right HRA application

V. Fauchille
IRSN, Fontenay-aux-Roses, France

ABSTRACT

In order to have its own expertise, IRSN develops level 1 and level 2 PSA models for each reactor series operated by the French utility EDF. Human Reliability Analysis (HRA) data are obtained from two HRA methods: PANAME in case of level 1 PSAs and HORAAM in case of level 2 PSAs.

- PANAME evaluates the probability of failure of an operating team that carries out Emergency Operating Procedures (EOPs);
- HORAAM evaluates the probability of failure of the emergency response organization on the basis of operating guides which calls for actions once certain criteria are reached indicating core damaged.

The article briefly presents both HRA methods and highlights the strong points of each of them.

Afterwards, the article focuses on level 2 PSAs and the Severe Accident Management Guide (SAMG).

After core melt, there are two types of human actions:

- "Immediate actions" that can be performed immediately because they don't need the expertise of the national emergency response organization. Mainly these actions consist in a confirmation of corrective actions already defined in the EOPs. The quick execution of these actions may reduce the consequences of the accident. To implement these actions, operators only need the permission of the Local Management Command Center.
- "Delayed actions" that need the expertise of the National Emergency Organization. The implementation of delayed actions requires somehow a risk analysis to draw the benefits and the drawbacks of the considered actions.

The main difference between SAMG immediate actions and SAMG delayed actions is a need for expertise.

HORAAM predicts Human Error Probabilities (HEPs) given a number of factors which affect human and organizational reliability:

- the time available,
- the availability of correct information,
- the adequate representation of the plant state,
- the necessary compromise in the decision,
- the availability of experts and their ability to make the right decision based on their understanding.

It is not suitable for modeling immediate actions because there is no expertise and few parameters of the model are used. The article gives comments on each parameter.

It appears that PANAME is more appropriate to model this type of actions which are similar to recommended actions in the EOPs (before core melt). When operators are allowed by the Local Management Command Center to terminate the application of EOPs, they implement a list of actions as it was the case previously with event based procedures. An estimated probability of failure modulated by a worsening context factor and the probability to fail in the recovering of a safe state depending on the time available to implement actions seems suitable. PANAME is able to model such scenarios.

HORAAM model is not questioned as such but the way it is used may be questioned. Clearly defined actions that do not require decision making cannot be modeled as actions that require decision making.

REFERENCES

Fauchille, V. Esteller, L. Raimond, E. & Rahni, N. PSAM 9. Application of the Human and Organizational Reliability Analysis in Accident Management (HORAAM) method for the updating of the IRSN level 2 PSA model.

Ménage, F., Vogel, A. & Chaumont, B. PSA 99. Using a decision tree to estimate human error probabilities in a level 2 PSA: the HORAAM method.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Three Human Reliability Analyses under the MERMOS light

P. Le Bot & H. Pesme
EDF R&D, France

ABSTRACT

In the recent ongoing works about Human Reliability Analysis (HRA), the International HRA Empirical study is a major step. This OECD project has been performed with Halden laboratory and fourteen HRA teams from several countries. EDF R&D's team was one of the French contributions with the MERMOS HRA method. The goal was "to develop an empirically-based understanding of the performance, strengths, and weaknesses of the methods". As contributors to the study, we have learnt a lot of lessons about our own method and about the other HRA methods. Since the study was focused on the comparison of different HRA analyses of the same Human Failure Events (HFE), it allowed us to better understand the theoretical and practical specificities of the other methods.

The goal of this paper is to attempt an exercise of comparison of the analyses with four HRA methods: MERMOS, CESA-Q and CBDT-THERP. CESA-Q has been used by the Paul Scherrer Institute's team (from Switzerland) and CBDT-THERP has been used by the EPRI team (from USA). We try to highlight the different assumptions and characteristics of modelling of the three methods by rewriting the CESA and CBDT-THERP analyses of one HFE of the International Study within the form and structure of MERMOS analyses.

Indeed we argue that the MERMOS analyses structure allows to describe the other methods analyses since with the structure of "failure scenarios" it has a larger level of modelling and less hypotheses of modelling. The exercise shows the strengths and the weaknesses of each method in the same light. It allows to illustrate the differences between first generation HRA methods as THERP and second generation HRA methods as MERMOS and CESA-Q, regarding the way the different methods use the input data, the assumption they make about human failure and why they differ or not in their quantification.

The conclusion is that this transposition of the CESA and the CBDT-THERP analyses into the MERMOS frame is feasible and is a great help indeed to compare these methods, regarding the concepts and the quantification process. One important result is hat for these four methods we can describe several independent "scenarios" of failure even if the description is more or less precise depending on each method. Then for the four methods the HEP (probability of HFE failure) is the sum of the probabilities of all these quantified failure scenarios. We think that this presentation of results through failure scenarios is an explicit way of describing failure.

Another result is that this exercise gives us good cues to improve MERMOS: by adding a PSF item in the frame of the MERMOS structure we have a good frame to be compared to many other HRA methods, which are based on PSFs. We think that the specificity of the MERMOS failure scenarios is an advantage because it explicits how PSF can combine to lead to failure.

REFERENCE

Lois, E., Dang, V.N., Forester, J.A., Broberg, H., Massaiu, S., Hildebrandt, M., Braarud, P.Ø., Parry, G., Julius, J., Boring, R., Männistö, I. & Bye, A. International HRA Empirical Study—Phase 1 Report: Description of Overall Approach and Pilot Phase Results from Comparing HRA Methods to Simulator Data, HWR-844, Halden Reactor Project, Halden, Norway and NUREG/IA-0216, Vol. 1., U.S. Nuclear Regulatory Commission, Washington, DC, (2009).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Towards a unified human reliability model

P.A. Baziuk, S. Rivera & J. Nuñez Mc Leod
Instituto CEDIAC, Universidad Nacional de Cuyo, Mendoza, Argentina

ABSTRACT

The two fields included in the study of human reliability (human behavioral science and engineering) have not been integrated sufficiently. Following this line, this article works towards a unification of the present models of human reliability, including the cognitive aspects and the last conception of the human cognition cycle.

In the attempt to integrate the several overlapping models require that each of the models be appropriately adjusted. The adjustments done are:

a. For error modes models (commission and omission errors): are include in the fail of some of the three process (sensorial, perceptive or cognitive).
b. For error levels models (input, mediation and output errors): are considered as cuts in the conduct cycle, because of internal or external factors.
c. For skill-, rules- and knowledge-based behavior model: is include in the different activations and responses of the conduct cycle.
d. For slips, lapses, mistakes and violations model: lapses are considered as a fail in the cognitive process, slips can occur by a fail of any of the three process and mistakes are a fail of the cognitive process.

The information included in the unified model is:

a. The concept of limited cognitive resources
b. The concept of cycle process
c. The concept of supervisory attention system
d. The concept of problem space in problem solving
e. The knowledge from expert judgment-based models

Therefore, human error can be defined as a cut of the cycle process of behavior, produced by a difference between the cognitive resources required by the task and the cognitive resources available by the person performing the task. This proposes a change in the phases of HRA modeling. In this point, the inclusion of PSFs and crew factors it's an important outstanding challenge.

This model also shows the importance of uncertainty and facilitates its identification and treatment. Since human performance is assumed to be derived and driven by complex and uncertain procedures of cognitive, psychological and behavioral process, it is unlikely to be defined using crisp sets quantified with probability and statistics, instead fuzzy set theory was introduce to the partial membership status set and measure of membership on the basis of the possibility theory.

Arrive to a unified model promises to be useful to identify human response (errors are the main focus) in QRA (Quantitative Risk Assessments) context estimating response possibilities and precisiation (GTU) and causes of errors to support development of preventive or mitigating measures. Also promises to derive in a methodology of HRA that can be successfully experimental validated.

REFERENCES

Dougherty, E.M. 1990. Human reliability analysis - where should'st thou turn? Reliability Engineering and System Safety, 29: pp. 283–299.

Kim, B.J. & Bishu, R.R. 2004. Uncertainty of human error and fuzzy approach to human reliability analysis. International ournal of Uncertainty, Fuzziness and Knowledge-Based Systems, 14 (1): pp. 111–129.

Mosleh, A. & Chang, Y.H. 2004. Model-based human reliability analysis: prospects and requirements. Reliability Engineering and System Safety 83: pp. 241–253.

Reason, J. 1990. Human Error. Cambridge, England: Cambridge University Press.

Rowe, W.D. 1993. Understanding Uncertainty. Risk Analysis, 14 (5): pp. 743–750.

Swain, A.D. & Guttmann, H.E. 1983. A handbook of human reliability analysis with emphasis on nuclear power plant applications. Applied Ergonomics, 16 (1): p. 68.

Wickens, C. 1992. Engineering Psychology and Human Performance (Second Edition). New York: HarperCollins.

This page intentionally left blank

Maintenance modelling and optimisation

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A complete probabilistic spare parts stock model under uncertainty

J. Lonchampt & K. Fessart
EDF R&D Division, Chatou, France

ABSTRACT

The classic way to optimize the number of spare parts for a population of components is to consider the failures as a Poisson process (Hadley & Whitin, 1963) and to calculate the number of spare parts that minimizes the costs or maximizes the Net Present Value of supplying spares. This approach has two weaknesses in the case of spare parts for major components:

1. The Poisson process for modelling failures assumes that the components are not experiencing ageing and that the failure rate is constant. It also assumes that the transient behaviour of the spare parts stocks, may be ignored. The fact to ignore the transient state in the optimization of the number of spares may lead to some wrong decision such as an oversized stock that generates useless holding costs or purchasing costs or an undersized stock that may generate unavailability.
2. One of the specificity of major maintenance tasks is that they are unlikely to be carried out several times during a plant life-time, that is to say the probabilities of the events that would lead to maintenance are very low. Moreover the failure consequences are often high. This is why mean indicators may not be sufficient as they often don't represent the residual risk. The fact to only consider mean values of indicators is in some case not sufficient for decision making, as a mean positive value may hide the fact that it is most probable that the indicator is negative. This is why it is important to provide complete probabilistic distributions in order to help decision making taking into account risks through enhanced indicators, such as the standard deviation, the probability that the indicator is negative (therefore making a strategy non profitable) …

For these reasons EDF R&D developed a methodology and a tool, that are not only focused on the average value of the NPV but also on providing complete probabilistic distributions in order to help decision making taking into account risks through enhanced indicators, such as the standard deviation, the probability that NPV is negative making a strategy non profitable …

The methodology and tool have been applied to a real industrial case dealing with pooling spares for two different companies and evaluating the profitability for each of them to pool and share common spares.

The global mean results show that supplying a spare on its own for Company 1 is profitable and not for Company 2. If we look at the mean value of the NPV, the decision to pool a common spare for the two companies seems to be indubitably a good decision, as the cost of purchasing the spare and to hold the stock is divided by two for each company.

As for risk indicators, without a spare, the probability to experience a forced outage is above 80%. Purchasing a spare reduces this risk from 84% to 10% for Company 1 and from 97% to 22% for Company 2. The spare sharing strategies increases the risk of forced outages by about 10% for each company, although the probabilities to regret the investment (probability that the NPV is negative) are smaller for the common spare strategy, this indicating that the fact to share costs is worth this higher risk of forced outage, the global risk being lower.

REFERENCES

Hadley, G. & Whitin, T.M. 1963. Prentice-Hall Inc *Analysis of inventory systems*.

Lonchampt, J. 2007. *Stock level and maintenance tasks selection for exceptional maintenance strategies under uncertainty: methodology, tool and application* 32nd ESReDA Seminar on Maintenance Modelling and Applications.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A framework for selection of test method for safety critical valves

E.B. Abrahamsen
University of Stavanger, Stavanger, Norway

W. Røed
Proactima AS, Norway

ABSTRACT

In the European oil and gas industry hydrocarbons are transported long distances in pipelines. In order to reduce the severity of potential hydrocarbon leaks to the atmosphere safety critical valves are normally installed. It is vital that such valves close on demand, and to assure this, the valves are normally tested periodically. Several test methods exist, and the choice of test method should be made in the test planning phase. The alternative methods test different properties of the valve in terms of valve functions and associated failure modes. The potential consequences of performing the test, for example in terms of production loss and costs, may also vary greatly from one test method to the next. Also the reliability of the test varies greatly between the test methods. Additionally, some test methods introduce emission of greenhouse gases to the atmosphere and challenges with regard to the safety of the personnel performing the test. Due to the above, the ideal test method is the one that balances the gained information by carrying out the test with the potential negative consequences of performing the test. To obtain this balance, the test method decision should be based on a structured approach. In this paper we suggest a qualitative framework that can support test method decisions for safety critical valves. The main focus of the framework is large hydrocarbon pipeline inventories. The framework is, however, general and can be adapted to other hydrocarbon systems onshore and offshore as well.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A maintenance strategy for systems subject to competing failure modes due to multiple internal defects and external shocks

I.T. Castro
Department of Mathematics, University of Extremadura, Spain

ABSTRACT

The deterioration of a system is the irreversible accumulation of damage through of its lifetime. A degradation relevant stochastic model is the *threshold model* where the system fails whenever its degradation level reaches a critical threshold. Besides degradation failures, systems may also be subjected to external shocks which may lead to failure. Lemoine and Wenocur may have been the first to consider these two competing causes of failures and these models are called Degradation-Threshold-Shock models (DTS-models).

Frequently, in the deteriorating systems literature, the degradation of the system is an unique measure modeled as a stochastic process. Castro *et al.,* and Kuniewski *et al.,* analyzed a system subject to multiple defects. Each defect follows a degradation process and the system fails when the deterioration of one of these defects exceeds a failure threshold.

This paper analyzes a maintenance policy for a DTS model assuming the system is subject to multiple internal defects. Internal defects initiate following a Non-Homogeneous Poisson Process (NHPP). Gamma processes model the degradation of each defect. External shocks arrive to the system and they are catastrophic with probability $1 - p$ and non-catastrophic with probability p.

An age-based maintenance strategy is developed in this presentation. Under this strategy, a preventive replacement is performed when the age of the system exceeds the value T. Corrective replacements are performed after a degradation failure or after a catastrophic shock. Minimal repairs are performed after a non-catastrophic failure. Costs are associated with the different maintenance actions and the objective is to determine an value of T that minimizes the expected cost rate. Under the assumptions of nondecreasing intensities for the arrival of defects and external shocks, the optimal value of T is obtained analytically.

Figure 1 shows a simulation of the expected cost rate versus T for a set of parameters. Internal defects arrive following a NHPP of intensity 0.002 defects per unit time (u.t). The length of these defects is modeled using gamma processes of parameters $\alpha = 0.004$ and $\beta = 1.5$. When the length of a defect exceeds 10 units of length (u.l.), a degradation failure occurs. External shocks arrive according to a NHPP of rate 0.003 shocks per u.t. With probability $p = 0.95$ (0.05) the shock is non-catastrophic (catastrophic). A preventive maintenance costs 10000 monetary units, 100000 monetary units a corrective replacement and 500 the minimal repair.

By inspection, the value of T that minimizes the expected cost rate is reached for $T_{opt} = 2300$ u.l. with an associated expected cost rate of 10.55 monetary units per unit time.

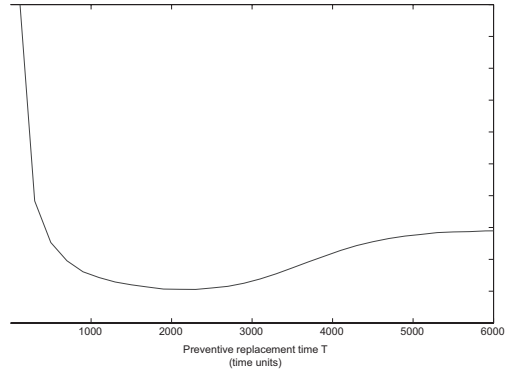


Figure 1. Expected cost rate as function of T.

REFERENCES

Castro, I.T., Barros, A. and Grall, A. (2011). Age-based preventive maintenance for passive components submitted to stress corrosion cracking. *Mathematical and Computer Modelling 54*(1–2), 598–609.

Kuniewski, S.P., van der Weide, J.A.M. and van Noortwijk, J.M. (2009). Sampling inspection for the evaluation of time-dependent reliability of deteriorating systems under imperfect defect detection. *Reliability Engineering and System Safety 94*(9), 1480–1490.

Lemoine, A.J. and Wenocur, M.L. (1985). On failure modeling. *Naval Res. Logist. Quart. 32*(3), 479–508.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A new modeling framework of component degradation

P. Baraldi, A. Balestrero & M. Compare
Energy Department, Politecnico di Milano, Italy

E. Zio
Energy Department, Politecnico di Milano, Italy
Ecole Central Paris-Supelec, France

L. Benetrix & A. Despujols
EDF R&D, Chatou, France

ABSTRACT

In this work, we address the problem of building a model in support of maintenance optimization, when the only available information comes from experts. This situation, very common in industrial contexts, calls for the development of novel modeling solutions. In fact, the information elicited from experts is subjective, qualitative and very often in implicit form; thus, it needs to be properly interpreted, represented and propagated through the model. To do this, the present work resorts to the theoretical framework of fuzzy logic, due to its capability of dealing with imprecise variables and linguistic statements.

From the modeling point of view, we resort to the concept of 'effective age' to take into account the influence of the environment on the component degradation process, which may evolve faster or slower than chronological time in adverse or favorable working conditions, respectively. The effective age is here considered alike a physical variable that is representative of the health state of the component, in the same way as the crack length may be used to indicate the degradation state of a mechanical component. Under this concept, the objective of degradation modeling becomes the identification of the relations between the operating conditions of the component and its effective age.

On the other side, the practical view undertaken in this work of building a degradation model based only on the expert's information requires that such model gives due account to the two following modeling constraints:

1. The degradation process is a discrete-states process, in recognition of the fact that experts are more familiar with this way of thinking of the degradation mechanisms.
2. There is no stochastic model available to describe the degradation behavior in normal operating conditions.

The degradation model is then embedded in a Monte Carlo scheme, in which a large number of trials or histories (i.e., random walks of the system from one configuration to another) are simulated. Averaging all the relevant quantities upon the entire mission time, we evaluate a set of useful indicators (i.e., the mean unavailability of the component) which constitute the basis to assess the performance of a given maintenance policy.

Finally, we show how the proposed methodology can be applied in practice, by way of a real case study dealing with a medium voltage test network.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A Petri net model of aircraft maintenance scheduling

D.R. Prescott
University of Nottingham, Nottingham, UK

ABSTRACT

This paper addresses the Time-Limited Dispatch (TLD) of aircraft (FAA Memo 2001, SAE ARP5107 2005). TLD is a maintenance methodology that allows aircraft dispatch with known faults present in the engine control systems for a limited period of time, see Figure 1. This allows aircraft operators to take advantage of the inherent reliability of system components and utilise system redundancy to enable maintenance to be scheduled at such a time that maintenance disruption can be minimise.

Important aspects of TLD and the associated certification requirements are discussed. A Petri Net (PN) model of the application of TLD to a system is presented, which builds on work presented by Prescott (2011). PN provide a flexible, graphical and mathematical framework for dynamic system modelling (Murata 1989, Schneeweiss 1999). The developed model is modular, with modules which relate to different aspects of processes relating to the application of TLD to a system, such as component failure and repair, maintenance scheduling in the event of revealed and unrevealed failures and maintenance after system failure. The PN model addresses one of the key disadvantages of previously-developed MC simulation models (Prescott & Andrews 2006, 2008) because it is easily auditable due to its graphical construction.

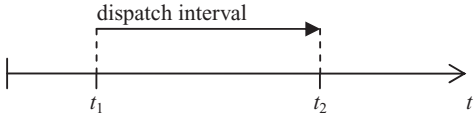


Figure 1. TLD—a fault occurs at t_1 and dispatch is allowed with that fault until t_2.

Quantitative analysis of the PN model is performed using a Monte Carlo (MC) simulation technique and a system failure rate is calculated. The rate of occurrence of this particular failure mode is important since it is crucial in the certification of systems to which TLD is applied. The result is validated against the results of a previously-developed MC simulation model (Prescott & Andrews 2006, 2008).

Examples of further results that can be obtained from such a model are also presented. These results are explained in the context of the application of TLD to the example system and further validate the structure of the developed PN model.

REFERENCES

FAA Memorandum. 2001. *Policy for Time-Limited Dispatch (TLD) of Engines Fitted With Full Authority Digital Engine Control Systems*. Policy No. ANE-1993-33.28TLD-R1.

Murata, T. 1989. Petri Nets: Properties, Analysis and Applications. *Proceedings of the IEEE*, 77(4): 541–580.

Prescott, D.R. 2011. Using Petri Nets to Model Time-Limited Dispatch. *Proceedings of the 19th AR²TS, Stratford-upon-Avon, UK*: 297–309.

Prescott, D.R. & Andrews, J.D. 2006. A Comparison of Modelling Approaches for the Time-Limited Dispatch of Aircraft. *IMechE Part O Journal of Risk and Reliability* 220(O1): 9–20.

Prescott, D.R. & Andrews, J.D. 2008. Modelling and Specification of Time-Limited Dispatch Categories for Commercial Aircraft. *ASME Journal of Dynamic Systems, Measurement and Control* 130(2).

SAE ARP5107 Rev A. 2005. *Guidelines for Time-Limited Dispatch (TLD) Analysis for Electronic Engine Control Systems*. Warrendale: SAE International.

Schneeweiss, W.G. 1999. Petri Nets for Reliability Modeling, Hagen: LiLoLe.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A simulation model for complex repairable systems with inter-component dependencies and three types of component failures

J. Malinowski
Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

ABSTRACT

This paper presents an attempt to construct a possibly general framework for simulating reliability behavior of complex systems. The concept stems from the research carried out by the author on the reliability of commodity transportation networks (e.g. power distribution networks), but it can also be applied to other types of systems. So far many simulation models have been designed for complex systems reliability analysis. However, most of them have drawbacks which include: restrictive assumptions (e.g. components independence, exponential times-to-failure and/or times-to-repair, repairs started immediately after failures' occurrences), narrow applicability (only to special classes of systems), or poor correspondence to real-world systems.

The author sought to construct a reliability model free of those shortcomings. This model is built on several basic assumptions that make it close to reality. First, failures of the system's components have impact on the functioning of other components, thus inter-component dependencies exist within the system. Second, three types of failures are distinguished—intrinsic (due to a component's wear), propagated (induced by other components' failures), and caused by external factors. Third, failed components are replaced or repaired by a limited maintenance personnel, thus it may happen that a maintenance action does not start immediately after a failure occurs, which makes it necessary to manage a repair queue. Fourth, functioning components are under (variable) load which causes their wear. The wear level of a component influences its failure and repair rates.

For the purpose of mathematical description the components are assigned two types of states—reliability (binary numbers) and operational (integer numbers). The system's functioning is described by two vector-valued stochastic processes, $X = \{X_1(t), \ldots, X_m(t)\}$ and $Y = \{Y_1(t), \ldots, Y_m(t)\}$, which represent the evolution of reliability and operational states of individual components over time, where m is the number of all components. The reliability state 1 represents an operable component, 0 – a failed one. If a component is operable then its operational state is positive and it specifies the component's load. If a component is failed then its operational state is non-positive and it specifies the component's place in the repair queue. The load on an operable component is assumed to depend on other components' reliability states. Over time, a component accumulates wear which depends on the component's load history. Thus $X_i(t) = 1$ if the i-th component is operable at t, otherwise $X_i(t) = 0$. Furthermore, $Y_i(t) > 0$ if $X_i(t) = 1$, where $Y_i(t)$ is a function of $X_j(t)$, $j \neq i$, while $Y_i(t) = -q$ if $X_i(t) = 0$, q being the i-th component's place in the repair queue, where $q = 0$ for a component currently under repair. Two types of repair are distinguished—minimal and complete. A component after a complete repair is as good as new, i.e., it has zero wear. A minimal repair does not reduce a component's wear, i.e. the wear remains as it was just before the failure occurred.

Modeling failure-repair process with the use of two types of states—reliability and operational—is the author's own concept which significantly facilitates the simulation of that process. This is because Y is a deterministic function of X whose evolution is fairly simple to simulate.

In the Appendix two illustrative examples are given. The first one shows how the processes X and Y evolve in case of a simple system. The second—how data obtained by simulation are used to estimate certain reliability parameters of a power distribution network.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A study of the effect of imperfect inspection on the efficacy of maintenance for a non-repairable system with a defective state

M.D. Berrade
Departamento de Métodos Estadísticos, Universidad de Zaragoza, Zaragoza, Spain

P.A. Scarf
Salford Business School, University of Salford, Salford, Manchester, UK

C.A.V. Cavalcante
Department of Production Engineering, Federal University of Pernambuco, Recife, Brazil

ABSTRACT

In this paper we consider a repairable system that is subject to imperfect inspection. Our aim is to explore the efficacy of inspection in circumstances in which it is subject to error. The system may be in one of three states: good, defective or failed, and the system is operational while in the defective state. The purpose of inspection is to prevent failure by allowing the replacement of the system while in the defective phase. However, if inspection is poorly executed then inspection may not be economic. Failure is detected as soon as it occurs. We present a model in which the system undergoes inspections at instants kT, $k = 1, 2, \ldots, M$ to detect if it has entered into the defective state. If so, the system is replaced by a new one with a cost c_m. If the system fails, a cost c_r, with $c_m << c_r$, is incurred. In addition false positive and false negative inspection can occur. A false positive occurs when the inspection says the system is defective when in fact it is good. A false negative occurs when the inspection says the system is good when in fact it is defective. In the latter case, a failure can subsequently occur and such a failure would be due to the poor quality of inspection. In this paper we assume that there is no opportunity to gain other information apart from that derived directly from the inspection and thus a false positive leads to replacement of the system with cost c_m. The maintenance policy is completed with a preventive replacement at MT with cost c_m provided that at an earlier moment there has not been a false alarm, or a failure, detection of the defective state at inspection. False alarms and false negatives have been considered in previous works Badía *et al.*, Berrade *et al.*, but only for a two-state protection system. In this paper, our aim is to provide additional insight about the effect of imperfect inspection for a system in which failure has direct consequences. We anticipate an application in which the user would investigate, for example, the values for the probabilities of a false positive and a false negative for which it is cost-optimal to perform inspection. In our model, we can also determine the system reliability implications of imperfect inspection. The model can also consider in a rather simple way the cost-benefit of condition based maintenance: for a system that is subject to condition monitoring, the monitored variable is often used as a surrogate for the system state; consequently, false positives and false negatives will occur with non-zero probability, and circumstances in which it is economic to carry out monitoring may be investigated.

REFERENCES

[1] Badía, F.G., Berrade, M.D. & Campos, C.A. 2010. Optimal inspection and preventive maintenance of units with revealed and unrevealed failures. Reliability Engineering and System Safety, 78, 157–163.

[2] Berrade, M.D., Scarf, P.A. & Cavalcante, C.A.V. 2010. Imperfect testing, false alarms and maintenance scheduling. Reliability, Risk and Safety: Theory and Applications. B. Ale, I. Papazoglou and E. Zio (editors), Taylor & Francis Group, London, 1361–1366.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Adaptive condition-based maintenance models for deteriorating systems operating under variable environment and indirect condition monitoring

K.T. Huynh, A. Barros & C. Bérenguer
Institut Charles Delaunay and STMR UMR CNRS 6279—Université de technologie de Troyes, Troyes, France

ABSTRACT

With the development of engineering structures, maintenance operations play an important role in efforts to improve the durability, reliability and maintainability of industrial systems. The dissemination and the expansion of instrumentation techniques and sensor technologies impulse the integrating of diversified monitoring information in describing the system health and providing reliable condition-based maintenance decisions. The present paper deals with the efficient use of different types of covariate information in modeling and optimising condition-based maintenance policies for a deteriorating system operating under variable environment.

Specifically, we aims to build a general degradation/measure model for a system subject to fatigue crack growth phenomenon. The degradation model of crack growth is basically described by a deterministic physical law of Paris-Ergodan, and then the randomness is incorporated into the model to preserve the stochastic nature of degradation process (Cadini et al., 2009). Since the system operates under variable environment, the speed and variance of crack growth is driven by environment states (i.e., external covariates which can be directly observable with reasonable accuracy). Moreover, the crack depth is considered to be hidden and can be only accessed through internal covariates which are diagnostic results of an indirect non-destructive inspection by ultrasonic technique. Such a model can describe most realistic aspects of single-unit systems operating under variables environment: physical characteristics of degradation phenomenon, relation among the real degradation and covariates (internal or external), as well as the nature of measurement approaches (direct or indirect). This model is therefore hopefully realistic, and offers a good case study for discussion about the relevance of different types of monitoring information in maintenance decision-making.

In the framework of the system under consideration, our objective is to develop Condition-Based-Maintenance (CBM) policies that use efficiently the information on both internal and external covariates. Two adaptive condition-based maintenance policies where the decisions rule is based on the estimated degradation state (reconstructed from noisy internal covariate by a particle filter technique (Doucet et al., 2000)) and adapt to the current condition of external covariate are introduced. In the first model, the environment adaptive approach relies on the inspection period, while in the second, it relies on the preventive replacement threshold. These policies allows us to study the efficiency of each adaption decision. The cost model of these policies are developed, optimized and compared with a more classical periodic inspection/replacement policy (Huynh et al., 2011).

The numerical results show that the environment adaptive policies are more general and more flexible than the classical one, hence always guarantee significant maintenance cost savings. Then, when we compare both adaptive maintenance policies, the saving of each of them depends closely on the intervention costs and the characteristics of operating environment. In this manner, it is indeed useful to integrate different information types in making an adaptive maintenance decision, however, there are no obvious way to choose an adaptation approach, and thus the choice should be decided through analyzing the maintenance cost saving.

REFERENCES

Cadini, F., Zio, E. & Avram, D. (2009). Model-based monte carlo state estimation for condition-based component replacement. *Reliability Engineering & System Safety 94*(3), 752–758.

Doucet, A., Godsill, S. & Andrieu, C. (2000). On sequential monte carlo sampling methods for bayesian filtering. *Statistics and computing 10*(3), 197–208.

Huynh, K., Barros, A. Bérenguer, C. & Castro, I. (2011). A periodic inspection and replacement policy for systems subject to competing failure modes due to degradation and traumatic events. *Reliability Engineering & System Safety 96*(4), 497–508.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An optimal periodic preventive maintenance policy of a deteriorating system subject to a bivariate state process

R. Ahmadi & M. Newby
School of Engineering and Mathematical Sciences, City University, London, UK

ABSTRACT

In this paper we present a new approach to preventive maintenance policy for a stochastically deteriorating system which is subject to repair and maintenance. The failure state of the system is determined by the failure probability measure $\overline{R}_t^{(X,V)}, t \in \mathbb{R}_+$ described by a general stochastic process (damage process) X with monotone paths and a virtual age process V induced by repair. The structure of the optimal maintenance strategy is formed under periodic inspection policy. The damage state of the system is revealed by inspections at periodic times. At inspection times the decision maker with respect to the failure state process $\overline{R}_t^{(X,V)}$ and the decision thresholds ξ_r, ξ_f that respectively refer to the preventive partial repair and replacement rule has disposition to perform a repair. The repair action updates the virtual age of the system: the virtual age process V is adjusted (imperfect repair), left unchanged (minimal repair) or reset to that of a completely restored system (perfect repair).

The critical threshold ξ_r is used as definition of partial repair action. If the system state process $\overline{R}_t^{(X,V)}$ crosses the boundary ξ_r a partial repair is made. The acceptance performance of the process is limited by the critical level ξ_f, $(0 < \xi_r < \xi_f < 1)$. The threshold ξ_f is the level at which failure and replacement occur. The replacement action (renewal) is determined by the first hitting time to the failure threshold ξ_f. The problem is to minimize the long-run average cost subject to the system parameters given periodic inspection policy. Because the model presented under periodic inspection policy allows replacement if the system state crosses ξ_f, the replacement cycles constitute a renewal process. This embedded renewal process is used to derive expressions for the long-run average cost based on the decision rules ξ_r, ξ_f and the period of inspection parameter. An analytical method for a degrading system modeled by Gamma process is presented. To demonstrate the use of this maintenance policy in practical applications, using Gamma process describing evolution of damage process X, an analytical method is presented.

REFERENCES

[1] Aven, T. & Jensen, U. 1999. Stochastic Models in Reliability. Springer, New York.
[2] Bremaud, P. 1981. Point Processes and Queues. Springer, New York.
[3] Cox, D.R. 1972. The Statistical Analysis of Dependencies in Point Processes. Stochastic Point Processes. Wiley, New York, pp. 55–66.
[4] Kahle, W. 2007. Optimal maintenance Policies in Incomplete Repair Models. Reliability Engineering and System Safety, 92, 563–565.
[5] Makis, V. & Jardine, A.K.S. 1992. Optimal Replacement in the Proportional Hazard Model. IN-FOR, 30(1), 172–183.
[6] Newby, M. & Dagg, R. 2004. Optimal Inspection and Perfect repair. IMA Journal of Management Mathematics, 15, 175–192. IMA Journal of Management Mathematics, 15, 175–192.
[7] Ross, S.M. 1970. Applied Probability Models with Optimization Applications. Holden-Day, San Francisco.
[8] Serfozo, R.F. 1990. Point Process. In: Heyman, D.P. and Sobel, M.J. (eds.). Stochastic Models 2. North-Holland, Amsterdam.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Application of RFMEA to risk analysis of maintenance of electric facilities

M. Ko & T. Nishikawa
Toshiba Corporation Research & Development Center, Japan

ABSTRACT

It is often difficult to detect risks with the severe losses which rarely occur by evaluating RPN (Risk Priority Number) with FMEA or expected loss with FMECA. Risk Failure Mode and Effect Analysis (RFMEA) is an FMEA which is added the function to evaluate such a risk. In this study, we applied RFMEA to risk analysis of maintenance of electric facilities, and we identified high risk tasks in Maintenance process.

Maintenance process is divided into 5 sub processes, which are Order Acceptance, Schedule Planning, Preparation of Manuals, Field Work, and Reporting. From a result of risk analysis, we found that over 80% of high risk failure modes were listed in the Schedule Planning and Field work. And the number of high risk failure mode of Schedule Planning was as same as that of Field work while both process had almost same number of tasks. This means the Schedule Planning has high risk tasks more than others.

In RFMEA, there are 4 parameters for risk calculation. The explanations of each parameter are below.

Occurrence : The number of failures in a predetermined period.
Detectability : According to the conditional probability of the failure affecting the equipment or the workers, given the occurrence of the failure.
Crisis Rate : According to the conditional probability of the worst-case scenario, given the occurrence of the failure affecting the equipment or the workers.
Severity : The size of loss in the worst-case scenario.

These 4 parameters are numerical values. We can calculate the probability of the worst-case scenario occurring in one day, p, by multiplying Occurrence, Detectability, and Crisis Rate. And we obtain expected loss in the worst-case scenario by multiplying p and loss amount corresponding severity. We define the latent loss as 1 percentile point of a loss distribution which is considered to be a numerical value expressing a risk. We use a binomial distribution as the probability of loss occurrence. This indicator can detect the accidents which rarely occur but which cause severe losses even though the expected loss is small.

We found most of the high risk failure modes of Schedule Planning have high Occurrence and high Detectability. High Detectability means that Preparation of Manuals and Field work perform the roles of checking and covering the defects of output from Planning. But the failure modes can occur in Schedule Planning as much as the processes following it cannot detect fully. The maintenance phase often moves from Schedule Planning to Preparation of Manuals while the specification of client is not fixed perfectly. We considered that why there are high Occurrence failure modes in Schedule Planning is that this factor affects the risk evaluation.

REFERENCES

Clifton, A. & Ericson, 2. 2005. *Hazard Analysis Techniques for System Safety.* New Jersey: John Wiley & Sons, Inc., 2005.

Takeichiro Nishikawa, Torii Kentaro & Kaho Hirano. 2008. Modified FMEA Focused on Latent Loss. s.l.: The 26th International System Safety Conference 2008, 2008.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Combined representation of coupling effects in maintenance processes of complex engineering systems

V. Volovoi & R. Valenzuela Vega
School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, US

ABSTRACT

Modern engineering systems consist of thousands of components; developing a coordinated maintenance policy for such systems presents a challenge from the complexity perspective due to the coupling among individual maintenance schedules for each component. The focus of this paper is on opportunistic (economic) maintenance and induced failure, as both of these coupling mechanisms are caused by competing risk phenomena. Modeling the maintenance process of an individual component, even if it includes modern condition-based considerations, can be described by a relatively small number of distinct states. In contrast, creating a system-level model that captures all relevant coupling leads to a state-space explosion; an implementation of such models is either not feasible at all or very expensive. To address this issue, the present paper explores the idea of developing component-level models that incorporate the aggregate effects of other components by providing a compact statistical representation of the combined influence of all other system components on a given component. This approach is analogous to the mean-field theory used in physics to avoid explicit description of pair-wise interactions. An analytical method based on asymptotic considerations is developed for combining effects of multiple components into a single Weibull distribution (inspections intervals are assumed to be smaller than the Weibull scale). Specifically, so-called "winning ratio" γ parameter is introduced that measures the odds that one of the components fail first within an interval of interest (given that both components fail during this interval). It is shown that in the practical range of interest this parameter shows very little sensitivity with respect to the scale of Weibull distribution (see Figure 1) In fact, it tends to a simple ratio determined by the shape parameters of Weibull distributions $\gamma = ß_1/(ß_1 + ß_2)$. This enables to evaluate a "weighted average" of multiple ratios when a component competes with many components, and select a matching Weibull shape parameter of the opportunity distribution. Finally, the scale parameter for the opportunity distribution is evaluated based on the total changes of failure during that interval. The accuracy of this approach was demonstrated for representing the combined effect of Weibull distributions. In particular, it is shown that the proposed method provides a superior match to the combined distribution in the relevant time range as compared to standard methods of approximating a distribution (e.g., matching moments or maximum likelihood). The resulting approximation of the targeted function does not provide a good global match for all the range, but instead targets the left tail of the distribution, which is the most relevant for the realistic maintenance scenarios. It was further shown that a combination of lognormal distribution can be well approximated by a Weibull distribution as well.

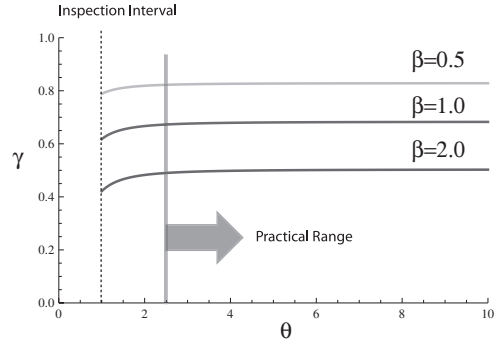


Figure 1. Scale sensitivity for race ratio γ when the first component follows Weibull distribution with shape ß = 2 and scale θ = 5 for different shape values. Interval of interest is unity.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Developments of time dependencies modelling concepts

T. Nowakowski & S. Werbińska-Wojciechowska
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

One of the concepts which provide useful means of modelling the effect of periodic inspections on the failure rate of repairable technical systems is a delay time concept, developed by Christer et al., see e.g. (Christer 1982, Christer & Waller 1984a, Christer & Waller 1984b).

Delay-time models can be used for decision-making, for example choosing the optimal maintenance and inspection interval with minimization of cost or system downtime.

The delay time concept defines a two-stage process for a component. First, a fault which has developed in the system becoming visible at time u from new with probability density function, pdf $g(u)$, if an inspection is carried out at that time. If the fault is not attended to, the faulty component fails after some further interval h which is called the delay time of the fault and is described by probability density function, pdf $f(h)$ (Fig. 1). During period h there is an opportunity to identify and prevent failure.

Once these two distributions are known, there is possible to model the reliability, operating costs and availability. The variables u and h depends upon the inspection technique adopted, see e.g. (Christer & Waller 1984a, Christer & Waller 1984b).

Presented paper is organized as follows: in the Section 2 we present a classification of the most often applied delay-time models. There are defined three main groups of delay-time models according to the maintenance strategy used.

First group is devoted to time-based inspection models. Plenty of studies regard to block-replacement inspection policy, where inspection takes place every T time units. Those models usually are developed for complex systems, although few single-unit or multi-unit system models one can find.

The second group of models which deserve to be mentioned is condition-based maintenance models. There one can find models especially developed for production plant maintenance.

The last group of models introduce the delay time concept in reliability cantered maintenance. However, there is only few works regard to this maintenance area.

In the presented article, authors focus on one group of models called models of equipment reliability. In these models, there is used the time based inspection strategy. The known works in this area are characterized in the Section 4. Other groups of models are reviewed in (Nowakowski & Werbińska 2011).

Later, there is provided a briefly summary, which underlines the possible directions for further research.

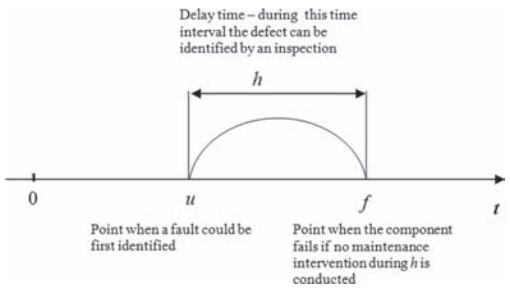


Figure 1. Time-delay modelling concept.

REFERENCES

Christer, A.H. 1982. Modelling inspection policies for building maintenance. *Journal of the Operational Research Society* Vol. 33, 723–732.

Christer, A.H. & Waller, W.M. 1984a. Reducing production downtime using delay-time analysis. *Journal of the Operational Research Society* Vol. 35, No. 6, 499–512.

Christer, A.H. & Waller, W.M. 1984b. An operational research approach to planned maintenance: modelling P.M. for a vehicle fleet. *Journal of the Operational Research Society* Vol. 35, No. 11, 967–984.

Nowakowski, T. & Werbińska, S. 2011. Delay-time models – state of art. *Article in publ.*

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Dynamic grouping maintenance strategy with time limited opportunities

Phuc Do Van, Florent Brissaud, Anne Barros & Christophe Bérenguer
Troyes University of Technology, Institut Charles Delaunay & UMR CNRS STMR, Troyes, France

Keomany Bouvard
Volvo Technology, Lyon, France

ABSTRACT

In the framework of grouping maintenance strategies for multi-component systems with positive economic dependence which implies that combining maintenance activities is cheaper than performing maintenance on components separately, a major challenge of the maintenance optimisation consists in joining the stochastic processes regarding to the components (time-dependent probabilities of failure) with the combinatorial problems regarding to the grouping of maintenance activities. While a long term or infinite planning horizon can be assumed to solve this problem in case of stable situations, dynamic models have been introduced in order to change the planning rules according to short-term information (e.g., failures and varying deterioration of components), using a rolling (finite) horizon approach (Wildeman, Dekker & Smit 1997). This approach is however applicable only when maintenance durations are neglected. From a practical point of view, the system may be stopped during maintenance of its components, maintenance durations should therefore take into account, especially when the system unavailability cost rate is expensive. Moreover, each component is assumed to be preventively maintained only one time within the scheduling interval. This assumption seems to be not relevant since a system may be composed of different components with different life time cycles, maintenance frequencies of components are thus different. For example, engine oil has to change more frequently than driving belt on a heavy vehicle. The first objective of this paper is to develop the rolling horizon approach by taking into account both the preventive maintenance durations and the occurrences of maintenance operations in the considered scheduling horizon.

Moreover, in presence of opportunities with limited durations in which some maintenance activities could be executed with reduced maintenance costs (Dekker 1995), the current grouping maintenance planning could be no longer the optimal one. The second objective of the present paper is to propose a new algorithm in order to optimally update online the grouping maintenance planning.

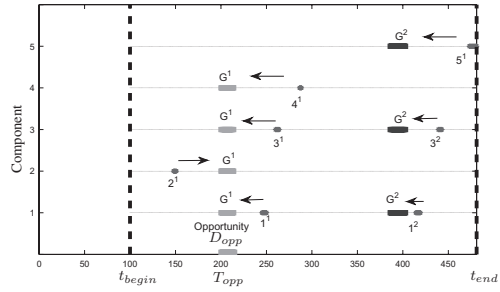


Figure 1. Illustration of the proposed dynamic grouping maintenance strategy. i^j is the $j(j = 1, 2)$th maintenance occurrence of component $i(i = 1, 2, 3, 4, 5)$ in the scheduling horizon. G^k is the maintenance group $k(k = 1, 2)$.

ACKNOWLEDGMENTS

This work has been supported and partly financed by the European project MoDe—Maintenance on Demand (http://fp7-mode.eu) funded from the European Community's 7th Framework Program (Project SCP8-GA-2009-233890 - FP7 Sustainable Surface Transport).

REFERENCES

Dekker, R. (1995). Integrating optimisation, priority setting, planning and combining of maintenance activities. *European Journal of Operational Research 82*.

Wildeman, R., Dekker, R. & Smit, A. (1997). A dynamic policy for grouping maintenance activities. *European Journal of Operational Research 99*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Dynamic maintenance requirements analysis in asset management

R.A. Dwight & P. Gordon
University of Wollongong, Wollongong, Australia

P.A. Scarf
University of Salford, Salford, UK

ABSTRACT

In this paper we propose that maintenance requirements analysis should be considered in the context of a dynamic business environment. Consequently, maintenance requirements analysis must be designed to adapt to changing asset circumstances. Furthermore, this adaptation should be multi-dimensional. In one dimension a review should be adapted to events in the life of the asset; that is, there should be an appropriate review of the maintenance program in response to the changing circumstances of an asset. In another, second dimension, the review for an asset should be adapted to the resources available in the organization for maintenance planning; that is, there should exist within the organization flexibility to choose the scope and the depth of the analysis in the review. Yet a further, third dimension is information available to conduct the review.

While the notion of a dynamic review process is not new, other review processes, for example that advocated by IEC 60300-3-11 presuppose that a formulaic approach to the analysis has previously been conducted and to a large extent should be repeated. Our suggestion is that the approach must be tailored to all of the dimensions set out here. Furthermore, in the first and third dimensions, an organization should have in place a system that triggers a review of the maintenance program for an asset as events in the life of the asset occur. Typical events in the life of an asset that would trigger a review are: acquisition; installation and testing/trials; modification; end of warranty; the outsourcing of maintenance; switch to in-house maintenance; accident findings that implicate maintenance; repeat failures that implicate maintenance; new maintenance technique available; new resources available for maintenance; downgrade; re-deployment; retirement; cannibalization; scrapping. Typically, such events will not occur over time with a fixed frequency. Periodic review, say every *n* years, may therefore not be ideal.

The decisions about when to review and how much resource to allocate to a review might be formalized hierarchically within a decision tree. This would prioritize high value assets for which there is scope to change maintenance practice and for which information exists as a basis for a thorough review. Otherwise one would advocate a lighter touch. Statutory requirements, for example, may mean there is little opportunity to modify inspection frequency. Also, documentation of changes to the maintenance requirements needs to be mandated and based on updates to an existing master document.

Our ideas are put forward understanding that normal logic and some standard practices may go some way to satisfying our criteria for a sensible approach to maintenance program review. Equally it is observed from the literature and also from practice that too often a laborious and slavish adherence to standardized approaches to maintenance requirements analysis persists and mitigates against the potential improvement to maintenance programs that would be achieved by focusing efforts on the appropriate application of the basic logic of maintenance requirements analysis to the assets that would benefit from such detailed attention. Conversely ad-hoc reviews driven by 'knee-jerk' reactions to calamitous events should invoke both the logic of maintenance requirements analysis and be recorded as a review of the existing documented analysis and resulting maintenance program. An advantage of the less rigid review is that it can be very responsive and targeted inexpensively and easily at a single component. An overly formal process supports retention of the status quo because it is too hard to mount a case for review. It can also become a box-ticking exercise. It can also encourage maintenance personnel to run double systems where they do not actually follow the formal program. Through this paper, we aim to indicate how organizations might take a more flexible approach to the application of maintenance requirements analysis.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Failure risk analysis and maintenance effectiveness in a windturbine according to its history of unavailability and applied maintenance

M.A. Sanz-Bobi, R.J.A. Vieira & X. Montilla
Comillas Pontifical University, IIT—Institute of Technological Research, Madrid, Spain

ABSTRACT

The industrial sector at present is in a dynamic process continuously improving the products produced or services supplied and their quality. The cost-effective and efficient use of their available assets is crucial in the current context, and the efficient application of maintenance and asset management techniques are the most important instruments used to reach these objectives (Anders et al., 2007, Scheider set al., 2006). All these techniques require information about the life of the assets in order to make decisions regarding maintenance planning and the future use of assets. Many approaches have been developed over the last decades to analyze different aspects of the life of the equipment or assets used in an industrial process. Also, many maintenance models have been proposed over a long period of time normally centered on preventive maintenance models (Jardine & Tsang 2006). They have been refined in several aspects and, in particular, some proposals of imperfect maintenance models can be found in (Nakagawa 1988, Bartholomew-Biggs et al., 2009, Liu & Huang, 2010.). All these models are basically based on unavailabilities occurred, failure rates and maintenance times.

This paper proposes a new maintenance model, inspired from the imperfect maintenance models, able to characterize the effectiveness of the maintenance applied and the risk of failure. This model named MAOL is based on the historical information of events including both unavailabilities and maintenance times. MAOL integrates an evaluation of possible failure risk of a windturbine according to the historical unavailabilities which have occurred with an analysis about the effectiveness of the maintenance applied. MAOL supplies important information about the effectiveness of the maintenance applied and an evaluation of possible unavailability risks. The information required by the MAOL model is obtained from an analysis of historical information using a tool which was developed for this purpose. This tool has several options that allow, among others, the evaluation of a set of impact indexes that can guide the application of maintenance to those failure modes that have the most important effect on the life of a component. Also, this tool allows for the evaluation of the MAOL model parameters: effectiveness of the applied maintenance, the reminder factor of previous applied maintenance and failure rate estimated without maintenance applied.

The MAOL model has been applied to a set of windturbines at a windfarm and the results are included in the paper. They are very significant and important in the asset management of the windturbines which were analyzed confirming the good foundations of the MAOL model proposed.

The MAOL model opens a new way to support the process of making decisions in industrial maintenance and asset management. New improvements of its parameters will be investigated in future works.

REFERENCES

Anders, G., Bertling, L., Cliteur G., Endrenyi, J., Jardine, A. & Li, W. 2007. Tutorial book on Asset Management - Maintenance and Replacement Strategies. *IEEE Power Engineering Society General Meeting*, *Tampa, Florida USA, 24–28 June 2007*.

Bartholomew-Biggs, M, Zuo, M. & Li, X. 2009. Modelling and optimizing sequential imperfect preventive maintenance. *Reliability Engineering & System Safety* 94(1): 53–62.

Jardine, A.K & Tsang, A.H. 2006. *Maintenance, replacement, and reliability. Theory and applications*. CRC Taylor & Francis.

Liu, Y. & Huang, H. 2010. Optimal replacement policy for multi-state system under imperfect maintenance. *IEEE T. on Reliability*, 59(3):483–495.

Nakagawa, T. 1988. Sequential imperfect preventive maintenance policies. *IEEE Trans Reliability* R-37: 295–298.

Schneider, J., Gaul, A., Neumann, C., Hogräfer, J., Wellssow, W., Schwan, M. & Schnettler, A. 2006. Asset management techniques. *Electrical Power and Energy Systems*, 28(9): 643–654.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Functional and economic obsolescence of assets in network utilities according to different environmental factors

J.F. Gómez
School of Engineering, University of Seville, Spain

V. González & Luis Barberá
Industrial Management PhD Program at the School of Engineering, University of Seville, Spain

A. Crespo
Associate Professor of Industrial Management School of Engineering, University of Seville, Spain

ABSTRACT

Maintenance in Network Utilities, such as distribution companies of water, electricity, gas, telecommunications, etc, customer oriented organizations, has to take into consideration the reliability of the assets among different areas of distribution.

The same type of equipment could operate under different environmental conditions in dissimilar areas depending on, for example, temperature or humidity. These variations could accelerate the deterioration of the asset, called "obsolescence" whose implications have to be evaluated in terms of costs. Maintenance contributes with its activities to extending asset life minimizing the failures, and so to reducing the obsolescence, which is defined as one of the key negative drivers of property depreciation and has the potential to have a significant and immediate impact upon the investment value of property in all operating sectors. For that reason, the estimation about performance according to the service life of the assets has to contain an obsolescence analysis, even generating warnings when the total costs during the asset lifecycle are exceeded or deviate from the prevision. There are four main causes of obsolescence: functional related to changes within the uses of the assets, economic referring to the cost of continuing to use the assets, technological related to the efficiency of the actual technology, social referring to preferences, recommendations or obligations such us changes on Health and Safety laws or on social ecological tendencies. According to this, maintenance activities are linked to the functional and economic obsolescence, keeping the asset value in a physical sense but also in an economic sense. There is a time-dependent relationship between obsolescence analysis and the reliability-based analysis according to functional factors. On the other hand, economic obsolescence is related to assets depreciation according to the financial value of such assets to the business. In this study, we will use reliability-based analysis to calculate the deterioration of the assets, focusing on the operation conditions within areas affected by environmental stressors which could accelerate the degradation of the asset. The obsolescence in a failure analysis context could not be considered from a deterministic point of view, due to the uncertainty of fault occurrence, so it must be handled from a probabilistic approach, quantifying the risks by non-reliability using statistical methods such us "Analysis of Survival data". Therefore, we will study the reliability of repairable equipments, through the Generalized Renewal Process (GRP) method applied on the Weibull distribution function. In GRP the variable (q) or Efficient Repairing is introduced to show the quality of the repairing as a virtual age. Therefore, this methodology will allow us, searching for the maximization the operation of the equipment, to prioritize and to make decisions focused on reliability comparing the maintenance for different: geographical areas, technical groups, procedures, changes in operations or organization, equipment from different vendors, environmental conditions and operation, etc. In network utilities companies, the indicator of equipment reliability affects to the equipment aging as an amortization of the equipment purchase value. This methodology considers the relations between effects and causes, and including the potential to produce value in the future.

REFERENCES

Kijima, M. & Sumita, N. [1986]. A useful generalization of renewal theory: counting process governed by non-negative Markovian increments. Journal of Applied Probability 23: 71–88.

Mansfield, J.R. & Pinder, J.A. [2008]. Economic and functional obsolescence: Their characteristics and impacts on valuation practice. Property Management Vol. 26 No. 3: 191–206.

Mettas, A. & Wenbiao Z. [2005]. Modeling and analysis of repairable systems with general repair. Reliability and Maintainability Symposium, 2005. Proceedings. Annual. Jan. 24–27: 176–182, ISBN: 0-7803-8824-0.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Impact of maintenance on the replacement investment under technological improvement

T.P.K. Nguyen, T.G. Yeung & B. Castanier
Ecole des Mines de Nantes, Nantes, France

ABSTRACT

The investment decision is clearly a strategic objective of a company as it defines its future competitiveness and the potential large costs incurred. This decision must, to ensure optimality, be based on the maximum information available in the company. However, we can summarize the motivations leading to an investment by the estimated performance (technical and economic) gap between the current system and competing technologies available on the market, taking into account budgetary opportunities. Numerous models for optimizing the investment decision were proposed in the economic, management science and operations research areas but few of them tackle the strong stochasticity and the uncertainty of the costs and the associated revenues. On the other hand, an unexplored important area in the investment problem under technological improvement is the impact of maintenance policy, maintenance defined here in complement to the replacement as a partial repair of the system. In fact, maintenance option not only helps us to maximize the profitability of the available asset, but also allows us to prolong its economic life for waiting the apparition of better technology in the near future.

Therefore, we propose a model that considers the impact of maintenance on the investment decisions in a new or improved asset, based on information about the profitability of the current asset and the technological environment. The profitability is modeled a stochastic process defined by both the technical performance of the asset, and the uncertainty of market. Let assume that the technical performance is decreasing in the deterioration state of the asset. Furthermore, a new technology is characterizes by its non decreasing probability of being available into the market, its degradation characteristics and also its stochastic purchase cost function. For maintenance processes, we also consider the dependency of its cost and its efficiency on the deterioration state of asset that is characterized by profit parameter.

Finally, we propose to model the optimization problem as a non-stationary Decision Markov Process. Different numerical analysis will be provided to highlight the potential benefits of integrating maintenance issues in the investment strategy.

REFERENCES

Bethuyne, G. 2002. The timing of technology Adoption by a cost-minimizing firm. *Journal of Economics* 76: 123–154.

Borgonovo, E., Marseguerra, M. & Zio, E. 2000. A Monte Carlo methodological approach to plant availability modeling with maintenance, aging and obsolescence. *Reliability Engineering and System Safety* 67: 61–73.

Clavareau, J. & Labeau, P.E. 2009a. A Petri net-based modeling of replacement strategies under technological obsolescence. *Reliability Engineering and System Safety* 94: 357–369.

Elton, E.J. & Gruber, M.J. 1976. On the optimality of Equal life policy for equipment subject to technological improvement. *Operational Research Quarterly* 27: 93–99.

Hopp, W.J. & Nair, S.K. 1994. Markovian deterioration and technological change. *IIE Transactions* 26: 74.

Huisman, K.J.M. & Kort, P.M. 2003. Strategic technology adoption taking into account future technological improvement: A real options approach. *European Journal of Operational Research* 159: 705–728.

Mauer, D.C. & Ott, S.H. 1995. Investment under uncertainty: The case of replacement investment decisions. The journal of financial and quantitative analysis 30: 581–605.

Nair, S.K. 1995. Modeling strategic investment decisions under sequential technological change. *Management Science* 41: 282–297.

Nguyen, T.P.K., Yeung, T. & Castanier, B. 2010. Optimal maintenance and replacement decisions under technological change. *International conference ESREL* 2010 – *Reability, Risk and Safety* 2010: 1430–1437.

Nguyen, T.P.K., Yeung, T. & Castanier, B. 2010. Optimal Maintenance and Replacement Decisions under Technological Change with Consideration of Spare Parts Inventories. *Technical paper.* 11/05/AUTO.

Smith, R.L. & Torpong, C. 2003. A paradox in equipment replacement under technological improvement. *Operations Research Letters* 31: 77–82.

Yor, M. 2001. Exponential functional of Brownian motion and related process. *Springer Finance*. ISBN 3-540-65943-9.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Integrating production and maintenance planning for a parallel system with dependent components

M. Nourelfath
Université Laval, Québec, Canada

E. Châtelet
Université de technologie de Troyes, Troyes, France

ABSTRACT

In practice, production and maintenance planning activities are usually performed independently. Therefore, it cannot be guaranteed that the obtained plans are optimal with respect to the objective minimizing the total maintenance and production cost. The integration of PM and production decisions may reduce not only the interruption time, but the total expected cost also. For highly reliable equipment, PM schedules may be performed at a lower frequency (monthly, quarterly or even semi-annually). As a result, PM activities should be integrated with tactical production planning. The objective of this paper is to develop an integrated production and PM planning model dealing with tactical aggregate production planning decisions. At the tactical level, it is often dealt with items from a product family viewpoint. A product family is defined as a grouping of end items that share a common manufacturing set-up. Set-up is the process of actually converting the equipment. This may be achieved by adjusting the equipment to correspond to the next product family or by changing non-adjustable "change parts" to accommodate the product family. As already suggested by the Total Productive Maintenance approach, the successful implementation of a maintenance program requires that its tasks be considered as parts of the production plan rather than as interruptions to that plan. Within this in mind, we consider that preventive maintenance activities are performed by machine operators responsible of set-up activities. The set-up activities are achieved at the beginning of planning periods. Thus, knowing that the production and maintenance requirements share common labour and time resources, PM tasks can be advantageously integrated to these set-up activities at the beginning of planning periods. In this case, because PM tasks are executed by machine operators responsible of set-up activities, the time and the cost of PM actions will be clearly lower than interrupting production to PM tasks during a production cycle.

Unlike some existing models, we do not assume that the components are stochastically and economically independent. We rather deal with the problem of integrating preventive maintenance and tactical production planning, for a production system composed of a set of parallel components, in the presence of economic dependence and common cause failures. The latter correspond to events that lead to simultaneous failure of multiple components due to a common cause. We use the β-factor model to represent common cause failures. This means that we assume two possible causes for system failure: the independent failure of single components, and the simultaneous common cause failure of all components. The suggested preventive maintenance is a T-age group maintenance policy in which components are cyclically renewed all together. Furthermore, between the periodic group replacements, minimal repairs are performed on failed components. We are given a set of products that must be produced by this parallel system in lots during a specified finite planning horizon. The objective is to determine an integrated lot-sizing and preventive maintenance strategy of the system that will minimize the sum of preventive and corrective maintenance costs, setup costs, holding costs, backorder costs and production costs, while satisfying the demand for all products over the entire horizon. A method is proposed to evaluate the times and the costs of preventive maintenance and minimal repair, and the average production system capacity in each period. For each chosen PM solution, the problem is solved as a multi-product capacitated lot-sizing problem. We show how the formulated problem can be solved by comparing the results of several multi-product capacitated lot-sizing problems. For large-size problems, a heuristic algorithm is proposed for the preventive maintenance selection task in the integrated planning model. Numerical examples are used to illustrate the potential benefits of using the proposed approach.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Maintenance effect modelling and optimization of a two-components system

W. Lair & R. Ziani
Direction de l'Innovation et de la Recherche, SNCF, Paris, France

S. Mercier
Laboratoire de Mathématiques et de leurs Applications, Université de Pau et des Pays de l'Adour, Pau, France

M. Roussignol
Laboratoire d'Analyse et de Mathématiques Appliquées, Université Paris Est, Champs sur Marne, France

For a railway infrastructure like SNCF (French National Railway Society), maintenance of the infrastructure is a major task because a failure causes delays and client dissatisfaction. Moreover, failures increase maintenance cost. The SNCF has hence initiated research in order to model the involved systems, in view of some improvement in their preventive maintenance. This article deals with a two-components system used at the SNCF. Both components have two failure modes and the system functioning mode makes the components dependent. This system is presently submitted to a periodic preventive maintenance policy. The aim of this paper is to study the eventual benefits provided by some adjustments on this periodic policy. The nature of the system is not revealed because of confidentiality issue.

To ensure the proper functioning of the system and to prevent undesirable events to occur, a preventive maintenance action is annually undertaken. During a maintenance action, the SNCF agent replaces the broken components if any and adjusts the working components. The data base at our disposal only provides information on the maintained components, which complicates the estimation of the unmaintained components life-time distribution. Models exist which separate the intrinsic degradation from the maintenance actions effect. One of them is the ARA_1 (first-order Arithmetic Reduction of Age) model described in (Doyen and Gaudoin 2004). We propose a slight modification of this model which we call the first-order Arithmetic Reduction of Age with Bertholon Adaptation ($ARABA_1$) model.

The modelling of the maintained system, with two dependent aging components regularly adjusted cannot be made with classical tools such as Markov jump processes with finite state space. We here propose to use Piecewise Deterministic Markov Processes (PDMP). Those processes are described in (Davis 1984).

Table 1. System cumulative mean quantities over T years for three maintenance strategies compared to the current one.

Preventive maintenance step	1	2	2
Components renewal	yes	no	yes
Cost	–16%	–0.2%	–17%
Undesirable events	–42%	+200%	+66%
Classical failures	–31%	–0.5%	–31%

Thanks to an $ARABA_1$ model, we are able to quantify the preventive maintenance effect on the components lifetime. This model appears to fit better than an ARA_1 model with Weibull intrinsic failure rate. Thanks to PDMP, the system is modelled by taking into account the components life time distributions, the adjustments effect and the maintenance strategy. A deterministic scheme presented in the article allows us to quantify mean maintenance cost, mean number of failures and mean number of undesirable events. A new preventive maintenance strategy based on the preventive renewal of the two components which reduces both of the maintenance mean cost and the mean number of undesirable events has been found, see Table 1.

REFERENCES

Davis, M. (1984). Piecewise Deterministic Markov Processes: a general class of non-diffusion stochastic models. *Journal Royal Statistical Soc. (B) 46* (pp. 353–388).

Doyen, L. & Gaudoin, O. (2004). Classes of imperfect repair models based on reduction of failure intensity or virtuel age. *Reliability Engineering and System Safety 84(1)* (pp. 45–56).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Multicriteria paradigm and Multi-objective Optimization on maintenance modeling

C.A.V. Cavalcante & A.T. de Almeida
Federal University of Pernambuco, Brazil

ABSTRACT

Maintenance planning consists of the process of taking into account the failure behavior of an item, the consequences of failure and possible actions that could effectively translate everything into a management systematic in order to provide some improvement for the system. This meaning of maintenance planning is very old. McCall (1965) argues that the techniques used to analyze maintenance problems are necessarily included within the theme of decisions under uncertainty. The general structure of these problems has the elements that are characteristic of models of decision theory. Since then, many changes have occurred and more concerns have appeared on the management of maintenance activities (Kobbacy & Murthy, 2008). Therefore, the formalization of the decision process is facing the challenge of dealing with multiple objectives in order to provide a broader view for the decision-maker. Consequently, we have seen many papers in the literature promising a better approach in order to support the decision maker by taking into account multiple objectives. The problems are that sometimes the use of the multicriteria and the multi-objective approaches do not follow consistent steps, some mistakes have been found in some applications and sometimes the problem is treated as having multiple objectives but only one aspect is taken into account or the decision maker is not considered.

Thus, in this paper we discuss in general terms a suitable structure for models to support maintenance planning; situations where the MCDA (MultiCriteria Decision Aiding), the field that comprises the multicriteria and multiple Objective approaches, is suitable, and we also discuss some mistakes in the application of MCDA. For the sake of a best understanding we dived the MCDA in two sub-classes: Discrete MultiCriteria (DMC), and the approach that tackles continuous problems (MOP).

We clarified some differences between the DMC and MOP approaches. In this way, some characteristics of maintenance problems, which might help to decide about the kind of approach that is best suited, were discussed. As a result, we advocate that more conceptual problems on maintenance can be better handled by DMC approaches, especially those methods that are more constructive, where the elements of the decision problem arise while the method is being carried out. On the other hand, for problems with a more technical emphasis, the MOP might be seen as a very suitable approach that is capable to found the non-dominated alternatives.

We understand that despite the fact that these two approaches have developed separately, because of the focus of each one is not the same, a great potential of an integrated use begins to be glimpsed. Actually, the best contribution from an integrated approach is that the most common mistakes on the application of a MCDM approach might be mitigate.

REFERENCES

Kobbacy, K.A.H. & Murthy, D.N.P. 2008. *Complex System Maintenance Handbook*, London, Springer Series in Reliability Engineering.

Mccall, J.J. 1965. Maintenance Policies for Stochastically Falling Equipment: a Survey. *Management Science* 11(5): 493–624.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Optimal preventive maintenance schedules using specific genetic algorithms and probabilistic graphical model

I. Ayadi, L. Bouillaut & P. Aknin
Laboratory of Land Transport Networks Engineering and Advanced Computer sciences, French National Institute for Transport Development and Risk Sciences and Technologies, University of Paris-Est, France

P. Siarry
Lissi—Laboratory of Images, Signals and Intelligent Systems, University of Paris-Est Créteil, France

ABSTRACT

Equipments used in industrial environments such as production lines, engineering or mass transport system, are generally complex, multi-components and Multi-States Systems (MSS). These equipments are subject to degradation mechanisms caused by operating conditions/environment (temperature, vibrations …). In addition to these degradation mechanisms, the deployed maintenance policy affects directly the dynamics of the occurrence of failure states. Given this situation, we should consider establishing Preventive Maintenance (PM) strategies to ensure an adequate trade-off between system availability and its maintenance costs.

Solving this issue requires a prior modeling of the system degradation. This modeling must represent faithfully the evolution of the operating states of a multi-components system, during time. Given that, an evaluation model of PM policies can be considered, inorder to look for the optimal schedules of the PM. A common way, in PM optimization, is to assume algorithms relying on classical degradations modeling approaches like deterministic models, stochastic processes or Markov chains. These approaches allowo ptimization algorithms to go faster, but they require, necessary, exact knowledges of degradation processes or strong assumptions about so journ-time distributions. This limitation can be overcomed by the use of a particular structure of Probabilistic Graphical Temporal Model named Graphical Duration Models (GDM). GDM allows to represent duration models of MSS, regardless of the exact nature of their so journ-time distributions.

This work can be divided mainly into two steps. The first one proposes an utility model for the evaluation of maintenance policies. This model is mainly based on the GDM. It involves essential parameters like maintenance probabilities, utilities or system availability. In the second step, two Genetic Algorithms (GAs) were developed. They seek for the optimal PM schedules. The 1st one named GA_1 seeks for periodic schedules contrarily to the 2nd one, GA_2, which look for non-periodic schedules. GA operators are redesigned according to the specific characteristic of the problem. Figure 1 summarize the preventive maintenance optimization solving process.

To demonstrated the applicability of the proposed methodology, a Distribution Fluid System (DFS) has been chosen as case study. This approach provides good results and allows a specific analysis of the weight of the different parameters of the utility function.

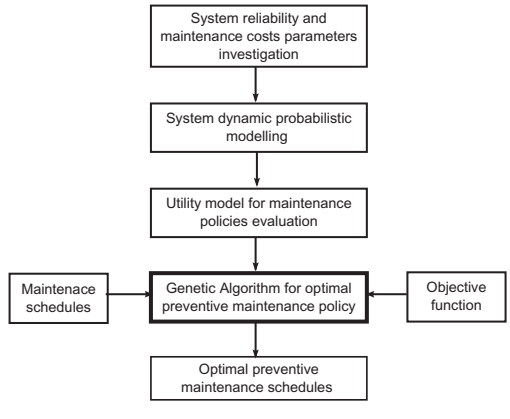


Figure 1. Preventive maintenance scheduling procedure using a genetic algorithm.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Optimal prognostic maintenance planning for multi-component systems

A. Van Horenbeek & L. Pintelon
Catholic University of Leuven, Heverlee, Belgium

ABSTRACT

Many models and methodologies to predict the Remaining Useful Life (RUL) of a component or system are investigated nowadays. However, decision making based on these predictions (RUL) is still an underexplored area in maintenance management. The real value of this prognostic information for scheduling maintenance actions on multi-component systems with different levels of dependence between components is not yet quantified. The link between prediction algorithms and decision making based on the resulting remaining useful life distributions should be established. The objective of this paper is to optimally plan maintenance for a multi-component system considering different levels of dependencies (economic, structural and stochastic dependence as defined by Nicolai & Dekker (2007)) based on prognostic information. By doing so the added value of this prognostic information (RUL) in maintenance planning and decision making is quantified. This is achieved by constructing a stochastic discrete-event simulation model, which optimizes maintenance action scheduling, based on prognostic information on the different components. A multi-objective optimization is performed by taking into account both cost and availability criteria as the maintenance objectives. Considering cost and availability as two separate objectives makes it possible to adapt and find the optimal maintenance policy according to the business environment at the time of decision making. A genetic algorithm is used to search for the optimal maintenance schedule which takes into account the predicted deterioration of all components. The added-value of scheduling maintenance actions based on prognostic information is determined by comparing this maintenance policy to five other conventional maintenance policies, which are: corrective maintenance, block-based and age-based preventive maintenance, offline condition-based maintenance and online condition-based maintenance.

A multi-component manufacturing system is investigated as a real life case study to illustrate the ability of the prognostic maintenance policy to react to different and changing deterioration patterns and dependencies between all considered components. To quantify the effect of different levels of dependencies between components on the optimal maintenance schedule a dependence parameter α, which ranges from 0% to 100%, is introduced. This parameter α reflects the advantage on cost and downtime of performing maintenance on multiple components at once compared to maintenance on a single component. A cost comparison between different maintenance policies for the multi-component manufacturing system with different levels of dependence between components is performed, which clearly shows the added value of prognostic information in maintenance decision making (Fig. 1). In this way an optimal maintenance policy is guaranteed all of the time and not only over time.

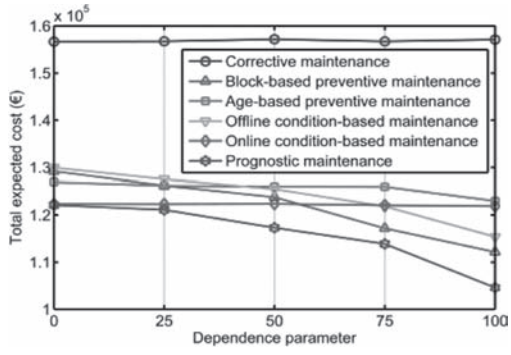


Figure 1. Total expected cost versus dependence parameter α for all considered maintenance policies.

REFERENCE

Nicolai, R.P. & Dekker, R. 2007. Optimal Maintenance of Multi-component Systems: A Review. *Complex System Maintenance Handbook*, Springer London: 263–286.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Optimization of redundancy and imperfect preventive maintenance for series-parallel multi-state systems

M. Nourelfath
Université Laval, Québec, Canada

E. Châtelet
Université de Technologie de Troyes, Troyes, France

ABSTRACT

This paper formulates a joint redundancy and imperfect preventive maintenance planning optimization model for series-parallel multi-state degraded systems. Non identical multi-state components can be used in parallel to improve the system availability by providing redundancy in subsystems. Multiple component choices are available on the market for each subsystem. The status of each component is considered to degrade with use. It is assumed that the system can consecutively degrade into several discrete states, which are characterized by different performance rates, ranging from perfect functioning to complete failure. The latter is observed when the degradation level reaches a certain critical threshold such as the system efficiency may decrease to an unacceptable limit. In addition, the system can fail randomly from any operational or acceptable state and can be repaired. This repair action brings the system to its previous operational state without affecting its failure rate (*i.e.,* minimal repair). The used preventive maintenance policy suggests that if the system reaches the last acceptable degraded state, it is brought back to one of the states with higher efficiency. System availability is defined as the ability to satisfy consumer demand that is represented as a piecewise cumulative load curve. A procedure is used, based on Markov processes and universal moment generating function, to evaluate the multi-state system availability and the cost function. The objective of the newly developed optimization model is to determine jointly the maximal-availability series-parallel system structure and the appropriate preventive maintenance actions, subject to a budget constraint. A large size numerical example is used to illustrate the proposed approach. As the number of possible solutions and the number of subspaces are huge for this example, and it is then impractical to use an exhaustive enumeration method, a heuristic approach is suggested to solve the formulated problem. This heuristic is based on a combination of space partitioning, Genetic Algorithms (GA) and Tabu Search (TS). After dividing the search space into a set of disjoint subsets, this approach uses GA to select the subspaces, and applies TS to each selected sub-space. The importance of the TS/GA heuristic in finding quickly a near optimal solution is discussed in the context of joint redundancy and imperfect preventive maintenance optimization. While the proposed optimization model is new, the idea of partitioning the search space was first introduced in (Ouzineb et al., 2008), where TS is used to solve efficiently the RAP of homogenous series-parallel multi-state systems. However, when the number of subsets is too high, it was shown in (Ouzineb et al., 2010, 2011) that the heuristic in (Ouzineb et al., 2008) is not able to give good quality solution in a reasonable time. (Ouzineb et al., 2011) extends this heuristic to solve the RAP of non-homogenous series-parallel multi-state systems by adding a GA that selects a limited number of spaces. In (Ouzineb et al., 2010, 2011), we have shown that by applying TS only to the subspaces selected by GA (instead of the high number of possible subspaces), the SP/TG approach, when tested on problems from previous research and on larger problems randomly generated, proved efficient not only at reducing computing time but also at improving overall solution quality. Following this work, *i.e.* (Ouzineb et al., 2008, 2010, 2011), the SP/TG heuristic is used in this paper to solve the newly proposed model.

REFERENCES

Ouzineb, M., Nourelfath, M. & Gendreau, M. 2008. Tabu search for the redundancy allocation problem of homogenous series-parallel multi-state systems. *Reliab Eng Syst Saf* 93(8): 1257–1272.

Ouzineb, M., Nourelfath, M. & Gendreau, M. 2010. An efficient heuristic for reliability design optimization problems. *Computers & Operations Research* 37: 223–235.

Ouzineb, M., Nourelfath, M. & Gendreau, M. 2011. A heuristic method for non-homogeneous redundancy optimization of series-parallel multi-state systems 17(1): 1–22.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Predicting rail geometry deterioration by regression models

F.P. Westgeest & R. Dekker
Erasmus School of Economics, Erasmus University Rotterdam, The Netherlands

R.H. Fischer
Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands

ABSTRACT

The Eurailscout measurement train is regularly used by the rail infra manager ProRail as well as by the maintenance contractors to assess the railway track geometry deterioration data on characteristics like scant, horizontal, vertical alignment. So far these data have only be used to determine whether maintenance is directly needed. After a long data processing phase we are able to compare measurements on same segments in time. We applied statistical regression techniques to assess the influence of environmental characteristics, like subsoil, tonnage and underlying objects.

The regression analysis on the degradation data resulted in the following model;

$$\begin{aligned} KPI^{D} = {} & -0.87 + 1.07 \cdot KPI^{-1} - 0.36 \cdot \text{Switch} \\ & - 0.10 \cdot \text{Tamping object} - 0.19 \cdot \text{Non} \\ & - \text{tamping object} + 0.16 \cdot \text{Monoblock} \\ & + 0.15 \cdot \text{Twinblock} + 0.07 \cdot \text{Subsoil clay} \\ & - 0.03 \cdot \text{Tonnage group} + \varepsilon \end{aligned}$$

KPI^{D} is the estimated KPI value for the degradation model. The standard errors in all coefficients were small (0.06 in the fixed term, 0.02 to 0.04 in all other terms except 0.01 for the tonnage term). We can see that the constant parameter is negative, which can be expected when no positive values are included. It indicates the yearly deterioration. The coefficient of the lagged KPI value, KPI^{-1}, is larger than 1, which means that the quality of observations with higher lagged KPI values decrease less than observations with low lagged KPI values. If it would be 1 than the present quality would not have any effect on the drop. The variables *Switch*, *Tamping object* and *Non-tamping object* have a negative coefficient, which means that segments containing one of these objects degrade faster than other segments. Segments with concrete sleepers degrade less fast than segments with hardwood sleepers, shown by the positive coefficient of the variable *Monoblock* en *Twinblock*. *Subsoil clay* has a little positive influence on the KPI value and the variable *Tonnage group* has a little negative influence. As the lightest tonnage group is 6, we would in fact expect a positive value. The result may be due to the small variation in the tonnage values as the value is constant over each of the three trajectories. For this estimated model the R-squared is 0.96, which is very high.

We also assessed the direct quality improvement because of maintenance. The results are used to make a forecasting model for deterioration and to assess the amount of maintenance necessary to maintain the track quality.

REFERENCES

Eurailscout, 2008. Retrieved July 3, 2008, from http://www.eurailscout.com/NL_index.shtml

Ferreira, L. & Murray, M.H. 1997. 'Modelling rail track deterioration and maintenance: current practices and future needs'. *Transport Reviews,* Vol. 17, No. 3, 207–221.

Jovanovic, S. 2004. 'Railway track quality assessment and related decision making', Proceedings IEEE Systems, Man and Cybernetics conference, 6, pp. 5038–5043.

Westgeest, F.P. 2009, Development and Application of a Degradation and Maintenance Model for Railway Track Geometry, MSc thesis, Erasmus University Rotterdam.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Probability distribution of maintenance cost of a repairable system modeled as an alternating renewal process

T. Cheng & Mahesh D. Pandey
Department of Civil and Environmental Engineering, University of Waterloo, Waterloo, Ontario, Canada

J.A.M. van der Weide
Department of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology, Delft, The Netherlands

ABSTRACT

Critical engineering systems, components and structures in power plants, chemical processing industry, and automotive industry are vulnerable to failure due to damage caused by shocks or over-stress that occur over the service life of the system. The failure occurs when the damage in the system exceeds its capacity. To maintain reliability of such systems, periodic inspection and preventive maintenance programs are implemented by engineers.

In most of the literature, maintenance optimization is based on minimization of the asymptotic cost rate, because the renewal theorem provides a simple expression for its computation. The asymptotic cost rate is equal to the expected cost in one renewal cycle divided by its expected length or duration.

The asymptotic formulation has a wide appeal, because it basically reduces the stochastic renewal process model to the first failure problem. However, this simplification may not be realistic for many engineering systems with a relatively short and finite operating life. The expected maintenance cost in a finite time horizon is only discussed in a few papers (Christer & Jack 1991, Pandey, Cheng & van der Weide 2010, Cheng & Pandey 2011).

This paper presents the derivation of the probability distribution of maintenance cost of a repairable system that is modeled as a stochastic alternating renewal process. The key idea of the paper is to formulate a renewal equation for computing the characteristic function of the maintenance cost incurred in a fixed time interval. Then, the inverse Fourier transform of the characteristic function leads to the complete probability distribution of cost. This approach also enables the derivation of probability distributions of the down time and the number of failures in a given time period. The distribution of the cost can be used to evaluate the Value-at-Risk (VaR) and other measures needed for the financial planning of a maintenance program.

REFERENCES

Cheng, T. and Pandey, M.D. 2011. An accurate analysis of maintenance cost of structures experiencing stochastic degradation. Structure and Infrastructure Engineering. In press.

Christer, A. and Jack, N. 1991. An integral-equation approach for replacement modelling over finite time horizons. IMA Journal of Mathematics Applied in Business & Industry, 3(1), 31–44.

Pandey, M.D., Cheng, T. and van der Weide, J.A.M. 2010. Finite time maintenance cost analysis of engineering systems affected by stochastic degradation. Journal of Risk and Reliability. In press.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Robustness of maintenance decisions: Uncertainty modelling and value of information

A. Zitrou & T. Bedford
Department of Management Science, University of Strathclyde, Glasgow, UK

A. Daneshkhah
Department of Statistics, Shahid Chamran University, Ahvaz, Iran

ABSTRACT

Maintenance optimisation models are essentially concerned with the minimisation of the overall maintenance cost—usually expressed as the average cost per unit of time (cost rate). The cost rate depends on a number of parameters related to reliability and cost aspects of the system. Like in any kind of model, here as well, studying the sensitivity of the model output with respect to the changes in the model parameters (e.g., reliability parameters) is of great interest. Typical methods for sensitivity analysis include the brute-force approach (where the effect of a number of deviations from the parameter in question is examined directly) and variance-based methods (where the contribution of each parameter to the variance of the output is determined analytically). Sensitivity analysis is important because if the cost-calculations are not sufficiently robust, use of the maintenance model can lead to optimization recommendations that are themselves not robust. However, the variance-based methods will not necessarily highlight this problem. In this paper we use the concept of the Expected Value of Perfect Information (EVPI) to perform decision-informed sensitivity analysis.

EVPI calculations allow us to identify the key parameters of the problem and quantify the value of learning about certain aspects of the system. This information is of great importance within a maintenance context, where decisions may not only relate to replacement timings, but also to accumulation of information about aspects of the system, like the ageing process. Unfortunately, decision-theoretic sensitivity analysis within a maintenance optimisation context is very demanding: the computation of expected utility requires the use of numerical integration techniques. Following from the work of Oakley (2009) this paper presents sensitivity analysis by using Gaussian process emulators. This approach is more suitable for complex models like this, as it allows for sensitivity analysis to be performed by using a smaller number of model runs.

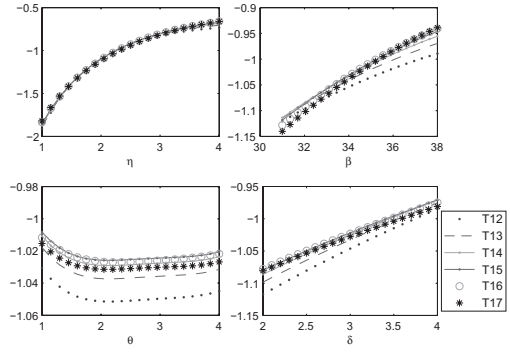


Figure 1. Expected utilities when θ_i is completely known before the maintenance decision.

To illustrate this methodology, we are using two maintenance settings: the first setting concerns a one component system subject to age-replacement policy and the second setting describes a multi-component system subject to block-replacement policy. In both settings the challenge is to identify the maintenance timings (critical age or periodic interval) that minimise the cost rate. Based on a GP emulator process, we have derived both point and interval estimates of value of learning, and explored how the optimal decision may vary. Figure 1 portrays the expected cost of the different maintenance options for the age-replacement model, assuming that a parameter can be known completely before a decision about the critical age is made. EVPI-based sensitivity analysis allows for the identification of the parameters with the highest learning value and can ensure not only that maintenance decisions are sufficiently robust, but also that processes like further testing or training are economically justified.

REFERENCE

[1] Oakley, J. (2009). Decision-theoretic sensitivity analysis for complex computer models. *Techno-metrics 51*(2), 121–129.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Semi-Markov processes for coverage modeling and optimal maintenance policies of an automated restoration mechanism

H.C. Grigoriadou, V.P. Koutras & A.N. Platis
Department of Financial and Management Engineering, University of the Aegean, Chios, Greece

ABSTRACT

In this paper, a two unit computer system is considered. The system consists in one operational and one standby unit, with imperfect coverage and an automated restoration mechanism, which is a switching device setting in operation the standby unit when a failure occurs on the primary unit. The units are affected by failures depending on random environmental factors and consequently the failure rates can be assumed as constant. Therefore, corrective maintenance is considered for each of the units. On the other hand, the automated restoration mechanism is affected by failures depending mainly to the frequency of use and simultaneously by the time spent at the standby mode. Hence, for the automated mechanism preventive maintenance at constant time intervals is considered. Nevertheless, when a failure occurs on the switching device corrective maintenance takes place.

In such a system, when a failure occurs at the operational unit, the restoration mechanism may be in a failure mode and hence unable to accomplish the switching procedure. In this case, the system is switched to the standby unit manually. Such phenomena can be prevented by adopting preventive maintenance. Since, preventive maintenance can be performed while the system is in operational mode, it is of critical importance to distinguish the optimal maintenance frequency. The optimal maintenance frequency aims to prevent failures that may occur during the maintenance of the switching device.

The modeling of imperfect coverage is based on the probability of success for the automated restoration mechanism. Firstly, the system is modelled by a Semi-Markov process since the time to maintenance for the restoration mechanism is considered as constant. To evaluate the model, two performability indicators are introduced representing the downtime and the corresponding operational cost. By optimizing the performability indicators, we propose two optimal maintenance frequencies. Additionally, the case when the automated restoration mechanism is taken only under corrective/preventive maintenance and the case when the automated restoration mechanism is replace, are also studied using semi-Markov processes. Numerical results are presented to illustrate the theoretical framework and the optimal downtime and the corresponding operational cost are derived with respect to the automation mechanism time for maintenance or/and replacement. It turns out that the downtime and the overall cost are almost identical independently of replacement or maintenance. Nevertheless, a sensitivity analysis shows that the overall cost decreases when replacement takes place, since it lasts less than maintenance and hence we avoid failures during the maintenance phase which incur an increased cost due to manual switching procedure.

REFERENCES

Goel, L.R. & Sharma, S.C. 1986. Stochastic analysis of a two unit standby system with two switching devices and sliding preventive maintenance. Microelectronics and Reliability 26(6): 1033–1037.

Limnios, N. & Oprisan, G. 2001. Semi-Markov Processes and Reliability, Birkhauser, Boston.

Platis, A. & Drosakis, E. 2009. Coverage modeling and optimal maintenance frequency of an automated restoration mechanism. IEEE Transactions on Reliability 58(3): 470–475.

Trivedi, K.S. 2001. *Probability and statistics with reliability, queuing, and computer science applications*. NY: John Wiley and Sons.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Semi-parametric estimation and condition-based maintenance

M. Fouladirad & A. Grall
Université de Technologie de Troyes, Institut Charles Delaunay, FRE CNRS2, Troyes, France

C. Paroissin
Université de Pau et des Pays de l'Adour, Pau Cedex, France

We consider a multi-component deterioration system whose condition can be summarized by a scalar ageing variable. The mean deterioration rate is supposed to be an unknown function of the life time. The ageing variable increases with the system's deterioration and the failure occurs as soon as the system state crosses a known fixed threshold called failure threshold.

As an example of such system we can consider the steel structures such as bridges, tanks and pylons which are exposed to outdoor weathering conditions. In order to prevent them from corrosion they are protected by an organic coating system. Unfortunately, the coating system itself is also subject to deterioration. To have a better monitoring procedure the area affected by corrosion can be divided in sub-areas and the deterioration of each sub-area can be separately monitored and maintenance action is to be done as soon as the maximum of all deterioration exceeds a fixed threshold. In (Nicolai 2008) this example is considered and a stochastic process is proposed to model the deterioration.

In this paper the scalar ageing variable is modelled by a non-homogeneous gamma process with unknown parameters, see (van Noortwijk 2009). It should be recalled that gamma process is a positive process with independent increments. It implies frequent occurrences of tiny increments which make it relevant to describe gradual deterioration due to continuous use such as erosion, corrosion, concrete creep, crack growth, wear of structural components. Furthermore, the gamma process allows feasible mathematical developments. It has been widely applied to model condition-based maintenance.

The system is periodically inspected and at each inspection time three decisions can then be taken (preventive maintenance, corrective maintenance or choice of the next inspection). A preventive maintenance takes place if the deterioration level of the system exceeds a preventive threshold. The preventive threshold is lower than the failure threshold.

Recently Wang proposed a semi-parametric estimator for a non-homogeneous gamma process, with random effects (Wang 2008). In this paper this semi-parametric estimation method is used to deal with the unknown deterioration rate and this information is used in the maintenance decision rule in order to adapt the maintenance parameters to the deterioration rate. During the beginning of the monitoring period, a very conservative preventive maintenance threshold is considered. By a sequential estimation the parameters of the deterioration process are estimated all along the monitoring process. According to the estimated values of the deterioration parameters the preventive maintenance threshold is readjusted and the maintenance decision rule is adapted.

We consider a long run average maintenance cost taking into account the cost of each type of maintenance action as well as the unavailability duration. The aim is to propose maintenance parameters leading to a low global maintenance cost.

REFERENCES

Nicolai, R. (2008). *Maintenance models for systems subject to measurable deterioration*. Ph.D. thesis, Erasmus Universiteit Rotterdam.

van Noortwijk, J. (2009). A survey of the application of gamma processes in maintenance. *94*(1), 2–21.

Wang, X. (2008). A pseudo-likelihood estimation method for nonhomogeneous gamma process model with random effects. *Statistica Sinica 18*, 1153–1163.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Simple Non-Markovian models for complex repair and maintenance strategies with LARES+

Max Walter
Lehrstuhl für Rechnertechnik und Rechnerorganisation, Technische Universität München, Germany

In recent publications (Walter, Gouberman, Riedl, Schuster & Siegle 2009; Walter & Lê 2011) we have introduced the 'language for reconfigurable systems plus (LARES+)', a modeling language for quantitative dependability evaluation of fault tolerant systems. When compared to traditional state-based methods like stochastic Petri nets or process algebras, LARES+ can be learned more quickly, and model creation requires less time and is less error-prone. In particular, the only formalisms used in LARES+ are state machines and Boolean terms; both are well-known in most engineering disciplines. Moreover, LARES+ models can be constructed by stepwise refinement, are modular and hierarchic as well as easy to modify, and allow for re-using sub-models. In our previous work, we have shown the applicability of LARES+ to complex examples taken from the literature.

So far, the stochastic process defined by a LARES+ model is restricted to a homogeneous continuous time Markov chain (CTMC). Thus, all timed transitions in a LARES+ model must follow exponential distributions. While this can be accurate for modeling the failure behavior of components with constant failure rates, it clearly is a gross approximation when modeling failures of components which are subject to wear-out, or deterministic time intervals such as repair times, maintenance intervals, or the duration of reconfiguration. Thus, LARES+ cannot be used for the evaluation and optimization of maintenance strategies, where these aspects are of crucial importance.

Therefore, this article proposes an extension of LARES+ which introduces transitions with non-exponential timing behavior (e.g. deterministic or Weibull distributed firing times), timer variables, and rules to modify the timer variables. Timer variables can for example be used to model the age of components and the progress of repair. They are modified e.g. if a component is replaced or if shocks occur. Each timed transition of a LARES model is attributed with a timer variable; thus the probability and duration of events depends on the current values of the timers.

We have used the novel features of LARES+ to model a K-out-of-N:G system with a complex repair and maintenance scheme. In this model, we consider silent failures of standby aging components, which fail according to a bi-Weibull distribution, and a single repair person which is responsible for both preventive and reactive maintenance serving the system components in a round robin fashion. Furthermore, reactive maintenance has priority over preventive maintenance which is interrupted if one of the components fails. It is further shown how timer variables of LARES+ can be used to model the fact that an interrupted maintenance procedure can be continued from the point where it had been interrupted before.

REFERENCES

Walter, M., Gouberman, A., Riedl, M., Schuster, J. & Siegle, M. (2009). LARES - A Novel Approach for Describing System Reconfigurability in Dependability Models of Fault-Tolerant Systems. In *ESREL 2009*.

Walter, M. & Lê, M. (2011). Clear and concise models for fault-tolerant systems with limited repair using the modeling paradigm LARES+. In *19th AR2TS Advances in Risk and Reliability Technology Symposium*, pp. 310–321.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

SIS-design automation by use of Abstract Safety Markup Language

K. Machleidt & L. Litz
Institute of Automatic Control, University of Kaiserslautern, Kaiserslautern, Germany

T. Gabriel
Institute of Automatic Control, University of Kaiserslautern
Currently with: Bayer Technology Services GmbH, Leverkusen, Germany

ABSTRACT

Failure tolerant Safety Instrumented Systems (SIS) contribute to companies' profitability. Operational requirements need to be considered in SIS design in addition to safety requirements defined by Safety Integrity Level (SIL). Consequently, the task to design SIS for given safety requirements is extended to provide best possible operational performance.

SIS are widely applied in process industry and the machinery sector to make potential hazardous applications safe. Faults of SIS can result in severe accidents. The SIL requirements derive from IEC 61508 (2010) and related international safety standards. SIL requirements involve architectural constraints, quantitative, and qualitative requirements. Qualitative requirements regulate work processes and procedures in each phase of the SIS life cycle and are not treated here. In contrast, the other two SIL requirements directly impact SIS design. The architectural constraints regulate the Hardware Fault Tolerance (HFT)—a design parameter for the hardware redundancy level of the SIS. The quantitative requirements involve SIS unavailability modeling and calculations.

In this publication the design process of SIS is analyzed and SIL requirements as well as operational requirements are elaborated. It is explained that formal SIS design is superior to manual SIS design. The *Advanced SIS Design Approach* is outlined as a new formal multi-stage procedure for computer-aided SIS design. It provides the most advantageous SIS configuration for a given application taking into account user-defined demands. The architectural constraints defined for SIS by international standards are formally interpreted to be applicable to the formal procedure. Contrary, conventional manual SIS design produces less advantageous SIS due to simplifications considerably reducing the number of potential configurations considered.

The main focus of this publication is on the complete formal description of SIS via the adapted Abstract Safety Markup Language (ASML). An arbitrary SIS configuration is formally described by ASML additionally featuring a graphic representation via ASML graph. ASML is required to achieve a formal and computer-aided procedure for SIS design. ASML was first defined in Gabriel (2011). Moreover, SIS unavailability calculation models can be automatically generated from ASML as demonstrated in Gabriel (2011). In Machleidt & Litz (2011) life cycle costs are applied as selection criteria for SIS.

In contrast to previous publications treating formal description and unavailability modeling of individual SIS, in this paper the authors propose an integrated approach to formally generate the most advantageous SIS configurations. A multi-stage *Advanced SIS Design Approach* is proposed for this purpose. The first stage is the systematic procedure to evaluate SIS configurations complying with architectural constraints for a given SIL. Different configurations may vary in hardware redundancy, voting schemes, and choice of components. Further stages are briefly described and will be further treated in future publications.

REFERENCES

Gabriel, T. 2011. *Generic construction of availability calculation models for safety loops in process industry*. Kaiserslautern: PhD thesis. in press.

IEC 61508 (2010). *Functional safety of electrical/electronic/programmable electronic safety related systems. Parts 1–7*. Geneva: International Electrotechnical Commission.

Machleidt, K. & Litz, L. 2011. An optimization approach for safety instrumented system design. *Proc. Ann. Reliability & Maintainability Symp. (RAMS 2011)*: 409–414.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

SPAMUF: A behaviour-based maintenance prediction system

Pedro Bastos
Instituto Politécnico de Bragança, Bragança, Portugal

Isabel Lopes
Universidade do Minho, Escola de Engenharia, Guimarães, Portugal

Luís Pires
Instituto Politécnico de Bragança, Bragança, Portugal

ABSTRACT

In the last years we have assisted to several and deep changes in industrial manufacturing. Many industrial processes are now automated in order to ensure the quality of production and to minimize costs. Manufacturing enterprises have been collecting and storing more and more current, detailed and accurate production relevant data. The data stores offer enormous potential as source of new knowledge, but the huge amount of data and its complexity far exceeds the ability to reduce and analyze data without the use of automated analysis techniques.

The industrial production has suffered considerable changes, becoming more complex, contributing to this a need for increased efficiency, greater flexibility, product quality and lower costs (Bansal*, et al.,* 2004).

Maintenance process is usually performed by integration of maintenance and process engineering functions at the phase of selection and application of machines and equipment; and also through proactive actions on those machines and equipments that will necessarily passes by preventive and predictive maintenance (Palmer 1999).

Nowadays, the amount of data generated and stored during industrial activities exceeds the capacity to analyze them without the use of automated analysis techniques. Thus, in the late 80's emerged the area of Knowledge Discovery in Databases (KDD), using models and data mining techniques for extract useful knowledge, patterns and tendencies previously unknown, in a autonomous and semi-automatic way (Apte, *et al.,* 2002).

The paper addresses an organizational architecture that integrates data gathered in factories on their activities of reactive, predictive and preventive maintenance. The research is intended to develop a decentralized predictive maintenance system (SPAMUF—Prediction System Failures for Industrial Units Globally Dispersed) based on data mining concepts. Predicting failures more accurately will enable taking appropriate measures to increase reliability.

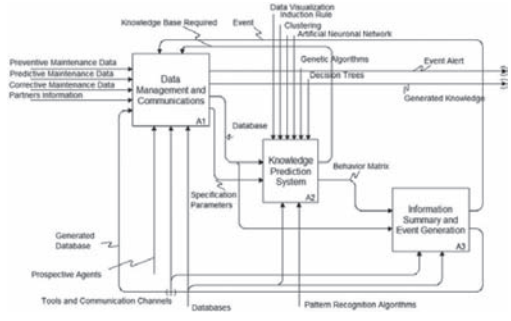


Figure 1. Main system in IDEF0 format.

The global system will be based on three main processes, as shown in the Figure 1 data management and communications (A1), knowledge prediction system (A2) and information summary and events generation (A3).

The A1 activity will be responsible for data collecting. The A2 activity is the main module of knowledge production and inference of behavior patterns related to each equipment of a factory unit. This activity will generate as an output a behavior matrix that will be the input of the synthesis of information module and events generation (A3).

REFERENCES

Apte, C., Liu, B., Pednault, E.P.D. & Smyth, P. (2002). Business Applications of Data Mining. *ACM* 45(8): 49–53.

Bansal, D., Evans, D.J. & Jones, B. (2004). A real-time predictive maintenance system to a production machine systems. *International Journal of Machine tools and manufacture* 44: 759–766.

Palmer, R. (1999). Maintenance planning and scheduling handbook. New Jersey, McGraw Hill.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Spare parts provision for a maintained system with a heterogeneous lifetime

P.A. Scarf
University of Salford, Salford, UK

C.A.V. Cavalcante
Federal University of Pernambuco, Recife, Brazil

ABSTRACT

We consider an inspection and replacement policy for a simple system comprising a single component installed in a socket. The component has a mixed lifetime distribution, so that a component may be weak or strong, reflecting perhaps the possibility of poor installation. When the component fails the system fails and the component is subject to a replacement. A common assumption for the majority of maintenance policies studied is that a spare component is available whenever the original component is replaced. We relax this assumption and suppose that the replaced component is overhauled and returned to the spares inventory. We further suppose that the system is subject to age based replacement. Our aim is to simultaneously optimize the age at preventive replacement and the stock level. In so doing, we focus on the effect of component heterogeneity on cost and system availability taking account of the maintenance policy and inventory related factors. Component heterogeneity is regarded here as a surrogate for the quality of maintenance.

The simultaneous optimization of inventory and maintenance policy is not new. Much of the benefit of the joint optimization of preventive replacement and spares provisioning may be due to the fact that the requirement for spares under a periodic replacement policy is predictable. Ordering times and stock levels can then be better planned. However, if the effectiveness or quality of replacement (and hence maintenance) is uncertain then demand for spares may be more erratic. Our paper makes a contribution by investigating the effect of such variation in maintenance quality. It is related to recent work on maintenance quality (Scarf and Cavalcante, 2010). It is also related to work of Armstrong and Atkins (1996) who look at a simple problem in which there is only room for one spare part. They are concerned with when to order the spare to minimize holding cost and the cost of maintenance, and numerically investigate the benefit of joint optimization.

We suppose: the system is replaced on failure or at age T whichever occurs sooner; replacements are not instantaneous; and a simple inventory policy is used in which there are only two components (one in use; the other in stock). A component whether good or failed is overhauled and returned to stock. Overhaul takes considerably longer to complete than a replacement. When the system is unavailable, revenue is lost at a particular rate. The inventory policy is compared to one in which three components rotate between stock and use. For a high value system, the effect of component heterogeneity upon cost and availability is quite large, with the increased cost being predominantly driven by the requirement for an additional spare. Thus the manager will avoid large costs from lost production not so much by making more frequent preventive replacements, but by having more spare parts. The system of interest may correspond to a gas turbine on oil production platform, or military equipment in the field. Our work can be extended to consider: a more a complex system or a fleet of systems; block replacement; spare parts provisioning for systems that are subject to wear and monitoring; more sophisticated inventory policies.

REFERENCES

Armstrong, M.J. & Atkins, D.R. 1996. Joint optimization of maintenance and inventory policies for a simple system. *IIE Transactions* 28, 415–424.

Scarf, P.A. & Cavalcante, C.A.V. 2010. A model of quality in preventive maintenance. In *Reliability, Risk and Safety*, Ale et al. (eds.) Taylor and Francis, London, pp. 1424–1429.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

State based models applied to offshore wind turbine maintenance and renewal

Z. Hameed & J. Vatn
Department of Production and Quality Engineering, Norwegian University of Science and Technology Trondheim, Norway

ABSTRACT

The reliability of Offshore Wind Turbines (OWT) has posed new challenges due to the complex nature of operations due to its location in sea. The weather is heavily influencing the availability of wind turbine for power due to the access and logistic issues. One way to address such operational challenges is to devise ways to approximate the ongoing state of the component. When the state is demanding to take some action, then it is important to devise the strategy regarding when to access the wind turbine depending upon the weather forecast. The decision regarding conducting any corrective action will depend on the condition of the component and if the state is critical but the weather is harsh, then to wait. This waiting time will depend on the duration of bad weather and the severity of the component.

Maintenance and renewal of OWT poses new challenges due to number of factors like marine environment, weather conditions, and uncertainties regarding new failure modes and mechanisms. To address these issues, it is proposed to evaluate the state of the component (gearbox) using the gamma process or phase type distribution. The determination of effective failure rate, renewal rate and the frequency of inspection will depend upon the current state of the component and then the next action will be suggested keeping in view the present condition. So for undertaking such action, it is proposed to determine the effective failure rate and renewal rate as function of state and the maintenance interval. Furthermore, two separate limits has been defined to calculate the effective failure rate and the renewal rate. So we have put specially focus on degradation modeling of OWT components where the state information is used to determine when to perform maintenance and renewal taking into accounts the fact that the OWT will be unavailable in randomly distributed periods of times due to the weather conditions. The model includes maintenance and renewal costs, cost of loss production, and a simple weather window model. The proposed scheme is implemented on the gearbox which has the highest downtime in case of failure.

After determining the optimal maintenance interval, then a simple weather model has been introduced. The modeling framework has been proposed how to formulate the strategies if the duration of harsh weather will coincide with the optimal maintenance intervals. Two strategies, either to advance or delay the maintenance activity, have been suggested and their formulation has been proposed. Furthermore, it has been suggested how to link these two strategies as the function of condition and maintenance interval.

It is expected that the efficient maintenance of gearbox will enhance the availability of OWTs in a better and cost effective way.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The analysis and conversion of warranty maintenance tasks for a power plant

B.M. Alkali
Glasgow Caledonian University, Glasgow, UK

P. McGibney
Moneypoint Coal-fired Power Generating Station, Kilrush Co. Clare, Ireland

ABSTRACT

A new scrubber plant in an existing power generating plant is considered in this study. The plant has a two year warranty maintenance tasks to be observed during operation. The main aim of this project is to examine the warranty period maintenance task list and propose adequate methods for assessing the preventive maintenance task in order to improve the whole maintenance process. Statistical approach is used to give an insight with reference to equipment status and a modeling approach is proposed to also assess maintenance information defined by experts with the focus on availability of systems in the context of actual operating regimes. A full review examination of each preventive maintenance task is conducted using expert judgement elicitation to ensure accuracy in all aspect of the task. This study focuses on the power plant's critical equipment. The Booster fans have been identified as critical equipment as they are vital to the plant process. Failure Mode and Effect Analysis (FMEA) is conducted on the power plant Booster Fans. A quantitative model structure is proposed that could give an insight about equipment failure pattern to review the maintenance warranty tasks.

We started our investigation by identifying where warranty and maintenance are carried out. We examine maintenance schedule and explore maintenance modelling options. The process of modelling is to aid in determining the duration time between each maintenance task to ensure a more efficient process. The reviewed task investigated is to be populated on to CMMS. Engineering judgement is often applied to bridge the gap between hard technical evidence and unknown characteristics of a technical system, (Cooke & Goossens, 2004). Intuition and judgement permeate engineering analysis from very basic decisions and techniques to adapt to more complicated assessment, (see Otway & Winterfeldt 1992; O'Hagan et al., 2006). This investigation is conducted in conjunction with the information elicited from the Front Line Managers (FLM) of the power plant. The FLM are considered as experts in this study. Expert's opinion on the review of maintenance tasks is vital in supporting the decision on the tasks selection process. Maintenance optimisation models with expert judgement is discussed by (Bedford & Alkali, 2009, Noortwijk et al., 1992). The maintenance task review checklist is used for maintenance information gathering to support decisions on the required task that need to be retained for in-dept analysis. In the context of our proposed quantitative model structure, we describe a set of degradation signals coming from the equipment that are indicators of higher failure rate, and which are observed by decision makers. The decision maker is given option to choose a series of PM tasks. The basic principle of this model is to use expert judgement for assessment, and the use of plant data information to calibrate the overall model.

REFERENCES

Bedford, T. and Alkali, B.M. 2009. Modelling competing risks and opportunistic maintenance with expert judgement. 34th ESReDA seminar San Sabastian, Spain.

Berner, R. 2004. The Warranty Windfall. Bloomberg.

Cooke, R.M. and Goosends, R.L. 2004. Expert judgement elicitation for risk assessmetn of critical systems. Journal of Risk Research, 7(6), 643–656.

Lenthes1, L. 2006. MERP Project Overview.

Lugtigheid, D., Jardine, A.K.S. and Jiang, X.Y. 2007. Optimizing the performance of a repairable system under a maintenance and repair contract. Quality and Reliability Engineering International, 23, 943–960.

O'Hagan, A., Buch, C.E., Alireza, D., Eiser, J.R., Garthwaite, P.H., Jenkinson, D.J., Oakley, J.R. and Rakow, T. 2006. Uncertain Judgement: Eliciting Expert's Probabilities. John Wiley & Sons. Chichester, p. 338.

Otway, H. and vonWinterfeldt, D. 1992. Expert judgement in risk analysis and management: Process Context, and pitfalls. Risk Analysis, 12(1): 83–93.

van Noortwijk, J., Dekker, J., Cooke, R. and Mazzuchi, T. 1992. Expert judgement in maintenance optimization. IEEE Transaction on Reliability, 41, 427–432.

Mathematical methods in reliability and safety

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A block replacement policy for a bivariate wear subordinator

Sophie Mercier
Laboratoire de Mathématiques et de leurs Applications, Université de Pau et des Pays de l'Adour, France

Michel Roussignol
Laboratoire d'Analyse et de Mathématiques Appliquées, Université Paris-Est Marne-la-Vallée, France

ABSTRACT

In case of a system submitted to an accumulative random damage, classical stochastic models are compound Poisson processes and Gamma processes, which both are increasing Lévy processes, see [1], [3] or [4] e.g. Such classical wear models typically are univariate. However, the deterioration level of a system cannot always be synthetized into one single indicator and several indicators may be necessary, see [2] for an industrial example. In that case, a multivariate wear model must be used to account for the dependence between the different univariate indicators of the system. Another context where multivariate wear models are required is the case of different systems submitted to common stresses, which make their wear indicators dependent. Multivariate increasing stochastic models hence are of interest in different contexts. We here propose to use multivariate increasing Lévy processes (or multivariate subordinators) as multivariate wear processes.

Considering bivariate subordinators as bivariate wear processes, the aim of this presentation is to revisit a classical block replacement policy within this new context, with the optimization of a cost function as an objective. A system is hence considered, with deterioration level measured by a bivariate subordinator. The system is not continuously observed. It is perfectly and instantaneously repaired periodically at a given cost. If the system was down at repair time, a unitary cost is induced per unit time for the down period just before the repair. After a repair, the future evolution of the system is similar as from the beginning and is independent of its past. We are interested in the asymptotic unitary cost (per unit time).

We first recall classical results for a block replacement policy, which we next specialize to our specific context. The influence of the dependence between the marginal wear indicators on the optimal policy is pointed out. For instance, the optimal cost is proved to be monotone with respect to the dependence. When the correlation is unknown, the safest attitude hence is to consider the correlation which leads to the highest cost, which may correspond to independent or completely dependent marginal indicators, according to the envisionned system failure mode. Numerical experiments illustrate the study.

REFERENCES

[1] Abdel-Hameed, M. 1975. A Gamma wear process. *IEEE Trans. Reliability*, 24(2):152–153.
[2] Mercier, S., Meier-Hirmer, C., & Roussignol, M. 2011. Bivariate Gamma wear processes for track geometry modelling, with application to intervention scheduling. *Structure and Infrastructure Engineering*, available on-line.
[3] Nakagawa, T. 2007. *Shock and damage models in reliability theory*. Springer-Verlag New York Inc.
[4] van Noortwijk, J. 2009. A survey of the application of Gamma processes in maintenance. *Reliab. Eng. Syst. Saf.*, 94(1):2–21.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A Monte Carlo approach for evaluation of availability and failure intensity under g-renewal process model

O. Yevkin
Dyadem International Ltd (has been acquired by IHS), Toronto, Canada

ABSTRACT

Several models have been developed for imperfect repairs that assume that the component is "better than old but worse than new" following the repair. One of the most attractive among them is the g-renewal process introduced by Kijima & Sumita (1986). The process is characterized by repair effectiveness parameter q, defining a virtual age of the unit at the given time after several repairs. Unfortunately, there is no closed form solution of corresponding g-renewal equation except the case when the system is "same as old" after restoration ($q = 1$) or for special (exponential) underlying failure distribution functions. Different approximate methods have been developed for other cases. The most general among them is the Monte Carlo approach introduced by Kaminskiy & Krivtsov (1998). The method was used for estimation of the expected number of repairs in warranty data analysis (Kaminskiy & Krivtsov, 2000; Yanez et al., 2002).

In the present paper, we have generalized and implemented the Monte Carlo algorithm for evaluation of other reliability characteristics like unavailability and failure intensity (frequency of failures), which are also very important in maintainability and its cost efficiency analysis (Vaurio, 2003). In addition, these reliability parameters are main inputs for system components, for example represented as basic events in a fault tree by modeling a system behavior. It is very important to have an efficient algorithm to define input at the component level. Therefore, some improvements of the Monte Carlo algorithm (including multithreading approach) are considered in the paper as well. The accuracy of the algorithm has been evaluated by calculating standard error and comparing the result of calculation with exact solution in the case when $q = 1$.

Underlying Weibull distribution function is considered in the provided numerical examples, however the algorithm can be easily applied to any types of distribution of underlying function and any functions describing repair process.

Table 1. Failure intensity function ($\alpha = 0.5$, $q = 0.25$).

t	0.600	1.80	3.00	4.20	6.00
N = 1E+7	0.743	0.461	0.373	0.324	0.281
SE	3.0E-3	1.3E-3	8.4E-4	6.5E-4	5.0E-4
N = 4E+3	0.749	0.466	0.372	0.323	0.276

Data represented in tables and graphs can be useful for deriving approximate solutions of the reliability problem.

The algorithm was significantly improved using representation of the g-renewal process as a continuous semi-Markov chain. An example represented in Table 1 (Weibull shape parameter $\alpha = 0.5$, scale parameter $\lambda = 1$) illustrates the efficiency of improved method. The result of raw simulation with number of trials $N = 10^7$ for different time points t is shown. Corresponding standard error (SE) is submitted in the next row. Almost the same accuracy was achieved using improved method, but with only 4000 trials (last row in the Table 1).

REFERENCES

Kaminskiy, M.P. & Krivtsov, V.V. 1998. A Monte Carlo Approach to Repairable System Reliability Analysis. In *Probabilistic Safety Assessment and Management*: 1063–1068. Lodnon: Springer-Verlag.

Kaminskiy, M.P. & Krivtsov, V.V. 2000. G-Renewal Process as a Model for Statistical Warranty Claim Prediction. In *Proc. Annual Reliability and Maintainability Symposium:* 276–280, Los Angeles.

Kijima, M. & Sumita, N. 1986. A Useful Generalization of Renewal Theory: Counting Process Governed by Nonnegative Markovian Increments. *Journal of Applied Probability* (23): 71–88.

Vaurio, J.K. 2003. Availability and Failure Intensity under imperfect repair virtual age model. In *Proc. of ESREL2003 Conference*, Maastricht, The Netherlands, (2): 1595–1599. Lisse: Balkema.

Yanez, M., Joglar, F. & Modarres M. 2002. Generalized renewal process for analysis of repairable systems with limited failure experience. *Reliability Engineering and System* (77): 167–180.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A new criterion for design of brittle components and for assessing their vulnerability to brittle fracture

M.T. Todinov
Oxford Brookes University, Oxford, UK

ABSTRACT

Unlike ductile fracture, brittle fracture occurs suddenly, proceeds at a high speed and in order to progress, there is no need for the loading stress to increase. Brittle fracture also requires a relatively small amount of accumulated strain energy. These features make brittle fracture a dangerous failure mode and require a conservative design criterion.

Vulnerability to brittle failure initiated by flaws, is a common type of mechanical vulnerability, caused by an unfavourable combination of several factors—existence of a defect with a critical size, missing the defect by the non-destructive inspection, unfavourable location of the defect in a highly stressed zone of the component and unfavourable orientation of the defect with respect to the local stresses. To improve the safety of loaded brittle components, and to reveal the vulnerability to brittle fracture which has often materialised as high-impact failures, a new, mixed mode, conservative failure criterion has been proposed.

The new conservative design criterion incorporates the worst possible orientation of a flaw with size just below the detection threshold of the inspection method. The new criterion has a simple analytical form and can be used as a solid basis for design of brittle components and for revealing their vulnerability to brittle fracture.

It is assumed that the component under consideration contains a globular flaw with a worst-case size, equal to the threshold flaw size of the non-destructive inspection technique. It is also assumed that around the globular flaw, a sharp penny-shaped crack has been initiated, with size equal to the size of the flaw.

The proposed new design criterion is superior to all existing methods used in the design of brittle components.

It can also be applied for determining the degree of vulnerability to brittle fracture. Suppose that the distribution of the principal stresses is known from a finite-elements solution. Testing the vulnerability of the component then reduces to going sequentially through all finite elements, applying the new design criterion and verifying whether a defect with a threshold size will cause brittle failure. The ratio of the number of finite elements where brittle failure 'has been initiated' to the total number of finite elements is a measure for the degree of vulnerability to brittle failure.

An important part of the paper is the optimal allocation of a fixed budget towards a non-destructive inspection, to achieve a maximum reduction of the risk of brittle failure. We present for the first time an efficient exact solution of the optimal budget allocation problem, based on an efficient dynamic programming algorithm. No constraints have been imposed on the functions defining the amount of removed risk. In this respect, the classical definition of risk has been challenged. It is argued that for a single failure occurrence, the classical definition of risk, as a product of the probability of failure and the average value of the consequences given failure, is inadequate. For a single failure occurrence, the distribution of the consequences of failure is sampled only once, and there is no guarantee, that the realization of the consequences will be close to the mean of the consequences. As an alternative, a new risk measure has been introduced—a combination of the average expected potential loss and the squared positive deviation from the mean of the consequences towards higher values.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Application of competing risks and generalized renewal processes in reliability analysis

R.J. Ferreira, M.C. Moura & E.A.L. Droguett
Center for Risk Analysis and Environmental Modeling, Department of Production Engineering, Federal University of Pernambuco, Recife, Brazil

P.R.A. Firmino
Department of Statistics and Informatics, Rural Federal University of Pernambuco, Recife, Brazil

ABSTRACT

In Risk and Reliability Analysis, the behavior of failure is of a great importance, given its impact on longevity of a System or Component (SC). Also, the occurrence of failure is related with costs—loss of production, expansive maintenance actions and acquiring new components.

In these cases, the best way to prevent high valued events is to construct an optimum maintenance policy regarding the failure behavior. However, between programmed preventive maintenance, the system can have failures and these failures occur in a random way. The literature presents several models to model the failure behavior regarding corrective actions. Between them, one can cites the virtual age models, which are capable of analyze the failure distribution via a concept called virtual age—what is the status of the SC after repair or how good the SC had returned after repair? This is measured through a parameter called renewal parameter presented on Generalized Renewal Processes, one of the virtual age models.

Preventive actions are also modeled by several models or methodologies. One can cite Competing Risks (CR) models, which are capable to model not only failure times, but also the group of failure modes that can cause failure events. This analysis can be done through the study of a pair of observation (Y, J) where Y is the event time—it is considered in this paper two kinds of events: corrective (a failure) and preventive (a maintenance) actions—and J is an indicator variable (0 for failure and 1 for maintenance). CR models, however, consider that after a repair action (corrective or preventive), SC returns as good as new, what in practice rarely occurs.

The gap between the two methodologies presented above can be solved with the construction of a hybrid model. This paper presents the development and application of a hybrid model of CR and virtual age models. Therefore, one can model the relation between corrective and maintenance actions, besides of analyzing the quality of repair made. Actually, the likelihood function is presented besides the results of the hypothesis test developed in previous works.

REFERENCES

Crowder, M.J. 2001. Classical Competing Risks. London, Chapman and Hall/CRC Press.

Doyen, L. & Gaudoin, O. 2006. Imperfect maintenance in a generalized competing risks framework. *Journal of Applied Probability* 43: 825–839.

Ferreira, R.J., Moura, M.C., Firmino, P.R.A., Droguett, E.L. & Braga, E. 2010. (In Portuguese) Desenvolvimento de um teste de hipóteses para um modelo híbrido de Riscos Competitivos dependentes e Processos de Renovação Generalizados. *XLII SBPO - Simpósio Brasileiro de Pesquisa Operacional*, Bento Gonçalves, Rio Grande do Sul.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Early detection of change-point in occurrence rate with small sample size

Laurent Bordes, Christian Paroissin & Jean-Christophe Turlot
Université de Pau et des Pays de l'Adour, Laboratoire de Mathématiques et de leurs Applications—UMR CNRS 5142, Pau, France

ABSTRACT

We address here the problem of deciding if either n consecutive independent inter-event times (i.e., the time that elapses between two consecutive failures) have the same distribution or if there exists some $k \in \{1, ... ,n\}$ such that the common distribution of the first k inter-event times is stochastically larger than the common distribution of the last $n - k$ inter-event times. It is the so-called change-point detection problem.

Many change-point detection methods are based on classical maximum type statistic. To detect a change-point on a sample having small size we have to face two problems. The first one is that it is difficult to base a decision on large sample properties of involved statistics since it is well known that the convergence rates of maximum type statistics is rather low. The second problem is that statistics are generally not free of the underlying distribution of the sample (under the null hypothesis of "no change-point") which prevent to determine test critical values through Monte Carlo methods. Here we propose several methods that overcome the later problem and that do not require necessarily a parametric assumption on the underlying distribution.

Let us denote by X_1, ..., X_n the n inter-event durations available at the calendar time t. These random variables are assumed to be independent, but one wants to test whether they are identically distributed or not. The main scheme of the proposed methodology is as follows:

1. split the sample into two subsamples: $(X_1, ..., X_k)$ and $(X_{k+1}, ..., X_n)$ for $k \in \{m, ..., n–m\}$;
2. compute the homogeneity test statistic for each splitting;
3. use all homogeneity test statistics to take a decision.

Decision can be either that no change-point occurs or that a change-point occurs at $k^* \in \{m, ..., n–m\}$.

For the two subsamples $(X_1, ..., X_k)$ and $(X_{k+1}, ..., X_n)$, assume that one can apply a given homogeneity test. We denote by $S_{n,k}$ the corresponding statistic that aims to measure the "distance" between the two subsamples parent distributions. From all these statistics, we suggest three types of global test based on the $n–2\,m + 1$ statistics:

1. maximum-type:

$$M_n = \max_{m \le k \le n-m} \frac{\left|S_{n,k}\right|}{\sqrt{\mathrm{var}\left(S_{n,k}\right)}};$$

2. χ^2-type:

$$\chi_n^2 = \sum_{k=m}^{n-m} \frac{S_{n,k}^2}{\mathrm{var}\left(S_{n,k}\right)};$$

3. quadratic-type:

$$Q_n = \mathbf{S_n}^T \sum^{-1} \mathbf{S_n},$$

where $\mathbf{S_n} = (S_{n,\,m}, ..., S_{n,\,n-M})^T$ and $\sum$ is the covariance matrix of $\mathbf{S_n}$.

For the homogeneity test for comparing two consecutive subsamples, we consider the four following statistics:

1. test based on likelihood ratio;
2. test based on empirical failure rate ratio;
3. test based on Mann-Whitney statistic;
4. test based on precedence statistic.

The two first statistical tests require the assumption that the inter-event durations are exponentially distributed while the two last statistical tests are nonparametric.

Numerical studies were carried out to compare the power of the various proposed tests. These tests are then applied to a real data (typical feedback data from a transportation company).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fine exact methods of safety, security and risk engineering

D. Prochazkova
Institute of Security Technologies and Engineering, Faculty of Transport Sciences, Czech Technical University, Praha

ABSTRACT

The human system safety represents a well-ordered set of human measures and human activities that provides human system security and sustainable development; by analogy it holds for other systems (Prochazkova, 2007 a). Because the human system dynamically behaves, the set of human measures and human activities must be also well proactively and strategically managed. Because a lot of tasks cannot be solved precisely, the engineering disciplines must be applied. The engineering is the wide discipline that solves problems from their insight, over proposal of solution up to realisation under given conditions. It is drawing force of human development because it also solves problems that are heavily exactly soluble. For this it uses the creativity of human individuals and approaches denoted as good practice (good engineering practice). At present it goes from system approach and for ensuring the present aims that are safe utility, safe community, safe region etc. It uses special disciplines that are in the paper briefly described. All engineering disciplines need to know critical items, i.e., items related to real processes and determined by site and time co-ordinates, and are based on negotiation with risks. The risk is for engineering practice well expressed as probable size of losses, damages and harms on followed assets that are caused by a given disaster with specified size and that are rescheduled for certain time unit (usually 1 year) and certain territory unit. At advisement in practice we distinguish whether the risk realisation goes on steadily by same way or variously in dependence on immediate site and time conditions of assets. The principal attributes of each risk are *uncertainty and vagueness*, and therefore, the paper deals with their sources. The classical statistical methods as computation of dependences, time series analyses and cluster analyses do not fulfil the demands necessary for work with data having different accuracies in different time periods, incompleteness and inhomogeneity, and therefore we must apply special methods as fault tree, process models, extreme methods, fuzzy techniques etc. and different approaches from precise deterministic, through probabilistic up to heuristic one. In the professional literature we can find a lot of methods, tools and techniques that are used in practice. The paper summarizes the results of research in which these were systemized according to role, testifying value and demands on data because the author feels that it is necessary for amplification of university education and for practical purposes. The all engineering approaches directed to safety are branches that solve problems, i.e. they use the methods, tools and techniques that indicate how to: texture problem; determine what might be solved; collect and create data set in order that it might give evidence to a given problem; select method for data processing in order that outputs might be relevant to a given problem solution aim; and how to interpret outputs of data processing from the view of human system safety that includes functionality and reliability of a given system. There are dozen methods, tools and techniques that are used in practice. Some of them are broadly known, e.g., methods of arithmetic, algebra, geometry, logic etc. They are followed by methods of mathematic statistics, cluster and factor analysis, application of time series, methods of operating research, network analysis methods, specific methods for decision-making support, and specific methods for safety engineering including those for risk engineering (CHISA, 2002, Prochazkova, 2010 b, 2011 c). According to practical experiences we separated the methods, tools and techniques into categories: general used; specific one; and specially adjusted methods, tools and techniques. For enabling their practical use we described them in (Prochazkova, 2011 c).

ACKNOWLEDGMENT

The research was supported by the Czech Technical University, Faculty of Transport Science, Institute for Security Technologies and Infrastructures and by the EU—project FOCUS.

REFERENCES

CHISA, 2002. *Prevention/Process Safety/Risk Assessment Methodology*. Pratur: CHISA.

Prochazkova, D. 2007 a. *Human System Safety* (in Czech). Ostrava: SPBI, 139 p. ISBN 978-80-86634-97-5.

Prochazkova, D. 2010 b. *Application of SWOT Analysis and of Selected Types of Case Studies at Selection of Model for Strategic Territory Safety Management* (in Czech). Zilina: ENVIRO, STRIX ann. Gillian 2010, ISBN 978-80-89281-56-5, 348–384.

Prochazkova, D. 2011 c. *Methods, Tools and Techniques for Risk Engineering* (in Czech). Praha: CVUT, in print. p. 289.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Importance measures and common-cause failures in network reliability

C. Tanguy
Orange Labs, Carriers and Networks, Issy-les-Moulineaux, France

ABSTRACT

We consider the influence of common-cause failures on a few of the most popular—Birnbaum, Improvement Potential, Risk Achievement Worth, and Fussell-Vesely—importance measures in the context of the reliability of network connections. We first show how the well-known definitions can be simply extended to systems undergoing common-cause failures, and show how calculations can be performed for networks made of identical elements. Different models of common-cause failures are then implemented in order to assess the changes of importance measures. A case study of a simple network architecture constituted by 9 nodes and 14 links allows to infer the expected behavior for larger configurations.

In many network reliability studies, components are usually assumed to fail independently of each other. This is not always realistic. Common-Cause Failures (CCFs) certainly occur, and it is important to assess their influence on the availability of a connection (it can actually increase or decrease). Importance factors such as the Birnbaum, Improvement Potential, Risk Achievement Work, Fussell-Vesely factors are crucial to the system designer since they provide information on the parts of the system that must be updated/improved in order to increase the system's performance. However, their definition relies on the independent behavior of all the elements.

We investigate the possible influence of CCFs on the ranking of the network elements, in comparison with what happens when elements are statistically independent, as is mostly assumed. We first provide generalizations of several well-known importance factors that apply when correlations between elements occur. Then we study the possible ranking changes in a case study (see Figure 1), where the medium-sized meshed network is a reasonable starting point to a better understanding of large systems. The four importance factors mentioned above are calculated exactly for each of the fourteen elements, and ranked for three different models of CCFs, namely the β-factor model, the binomial failure rate model and the degenerate multidimensional normal distribution—a particular case of the Gaussian copula—in order to detect possible general behaviors. An example is given in Figure 2, which displays the Fussell-Vesely importance factor when the common-cause failures are described by the β-factor model. It shows a general increase of this factor for all the elements, when β goes to 1 (the fully correlated configuration). However, the relative ranks of two elements do not necessarily change. This seems to be quite characteristic: adding CCFs to the description of a system does not profoundly change the ranking of the elements, when compared to the standard "independent behavior" result: "important" elements remain so. This study also shows that the ranking offered by the "family" of Birnbaum, Improvement Potential, and Risk Achievement Work factors differs substantially from that offered by the Fussell-Vesely one.

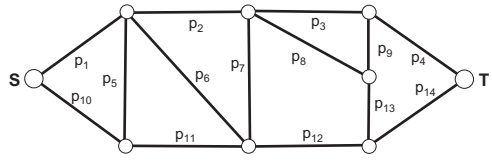


Figure 1. Network configuration of Walter *et al.*

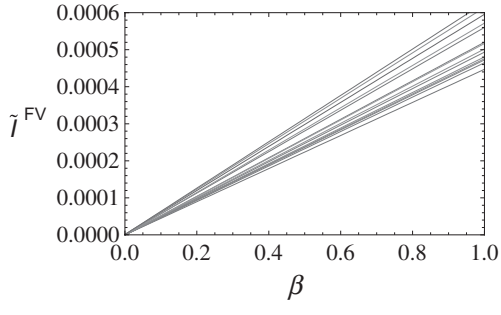


Figure 2. Variation of the numerator of the Fussell-Vesely importance factor as a function of β, for the fourteen links.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Multivariate Gumbel distributions for Reliability Assessment

B.J. Leira & D. Myrhaug
Department of Marine Technology, NTNU, Trondheim, Norway

ABSTRACT

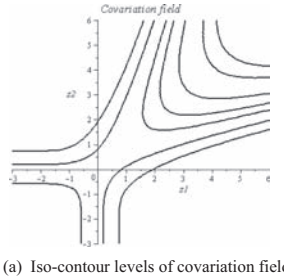
A bivariate Gumbel distribution is established based on transformation of an existing bivariate Rayleigh distribution, see Rice (1944, 1945), Longuet-Higgins (1986), Goda (1976), Kimura (1980), Tayfun (1990), Myrhaug et al. (1995). Application of this distribution in relation to reliability assessment of marine structures is subsequently addressed. An example of a linear combination of the two basic variables which are Gumbel distributed is further considered in connection with a mono-tower structure.

The role of the Gumbel distribution in connection with reliability assessment of marine structures is discussed for the case of multiple "isochromatic" response processes.

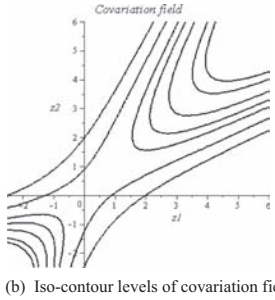
Comparison with another class of bivariate Gumbel distributions (Gumbel Type A, see Gumbel (1958), Johnson and Kotz (1972)) is also made. In general, the properties of the two distributions are found to be quite similar, but with some deviations in the shape of the iso-contour levels.

The so-called "covariation fields" (see Leira (2010), Leira and Myrhaug (2011)) of the two different types of Gumbel distributions are also compared. Iso-contour levels of these to functions for the present model versus that for the Gumbel Type A distribution are shown in Figure 1. For the latter distribution, there is a pronounced peak for negative values of the two variables which is not present for the former distribution.

It is conceived that for linear combinations of the basic variables, the two different probability distributions will give similar results. Differences may occur when they are applied in combination with some categories of non-linear functions of the basic variables.



(a) Iso-contour levels of covariation field for present model. Values are [0.5,1.,2.,3.,5.,10.,15.] from outer to inner contour.



(b) Iso-contour levels of covariation field for Gumbel Type A model. Values are [0.5,1.,2.,3.,5.,10.,15.] from outer to inner contour.

Figure 1. Covariation field for Gumbel type A model.

REFERENCES

Gumbel, E.J. 1958: "Statistics of Extremes", 2nd ed., New York: Columbia University Press.

Goda, Y. 1976. On wave groups. Proc. BOSS'76, Trondheim, Norway, Vol. 1, pp. 115–128.

Johnson, N.L. & Kotz, S. (1972): "Distributions in Statistics: Continuous Multivariate Distributions", John Wiley & sons, New York.

Rice, O.S. 1944, 1945: "Mathematical modelling of random Noise", Bell Syst. Tech. J., 23, 282–332/24, 46–156.

Longuet-Higgins, M.S. 1986: "Wave Group Statistics", *Ocean Whitecaps*, eds. E.C. Manohan, G. Mac Niocaill, D. Reidell Publishing Company, Dordrecht, pp. 15–35.

Leira, B.J. 2010: "Some Multivariate Weibull Distributions with Application to Structural Reliability Assessment", Proc. ESREL Conference, Greece.

Leira, B.J. & Myrhaug, D. 2011 "Some Multivariate Probability Distributions in Marine Technology", CENTEC book, Lsbon, Portugal.

Kimura, A. 1980. Statistical properties of random wave groups. Proc. 17th Int. Conf. on Coastal Engng., Sydney, Australia, pp. 2955–2972.

Tayfun, M.A. 1990. Distribution of large wave heights. J. Water-way, Port, Coastal, Ocean Engng., 116(6), 686–707.

Myrhaug, D., Dahle, E.Aa. & Rue, H. 1995: "A Two-dimensional Weibull Distribution and its Application to Rolling", ASME, Journal of Offshore Mechanics and Arctic Engineering, August, Vol. 117, 178–182.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Nonparametric predictive inference for reliability of a series of subsystems with multiple component types

A.M. Aboalkhair
Department of Mathematical Sciences, Durham University, Durham, UK
Department of Applied Statistics and Insurance, Mansoura University, Mansoura, Egypt

F.P.A. Coolen & I.M. MacPhee
Department of Mathematical Sciences, Durham University, Durham, UK

ABSTRACT

The nonparametric predictive inference (NPI) approach to system reliability explicitly reflects that limited knowledge about reliability of components, resulting from testing, leads to dependence of the reliabilities of components of the same type in a system. Coolen *et al.* (2011) presented NPI for reliability of a single voting system consists of multiple types of components. They are assumed to all play the same role within the system, but with regard to their reliability components of different types are assumed to be independent. The information from tests is also available per type of component. This paper presents the NPI approach for systems with subsystems in a series structure, where all subsystems are voting systems that can have components of the same types. As NPI uses only few modelling assumptions, system reliability is quantified by lower and upper probabilities, reflecting the limited information in the test data. The results are illustrated by examples, which also illustrate important aspects of redundancy and diversity for system reliability. It is particularly logical to focus attention on the NPI lower probability in the examples, as it can be considered to be a conservative inferenc.

EXAMPLE

Two different systems, each having components of $T = 2$ types A and B, are considered. The first is a k-out-of-24 system with $m_a = m_b = 12$. The second consists of $L = 2$ k^i-out-of-12 subsystems in series configuration with $m_a^1 = m_b^1 = m_a^2 = m_b^2 = 6$. The NPI lower probabilities for the event that a system functions successfully are presented in Table 1, for different test data and some different values of k, k^1 and k^2. It is clear that the system reliability, as measured by this NPI lower probability, increases sub-stantially for decreasing k or k^1 and k^2, so if fewer of the 24 components have to function, and also for increasing numbers of tested components if these were all successful. If all components in the system must function the reliability tends to be very small for cases where some components failed in the tests, which is logical as the test information only provides weak support for this event.

Table 1. NPI lower probabilities for two different systems.

n	s	Sys1 $k = 21$	Sys2 $k^1 = 10$ $k^2 = 11$	Sys1 $k = 22$	Sys2 $k^1 = 11$ $k^2 = 11$	Sys1 $k = 24$	Sys2 $k^1 = 12$ $k^2 = 12$
1	1	0.059	0.041	0.036	0.027	0.006	0.006
2	2	0.173	0.123	0.110	0.086	0.020	0.020
3	3	0.294	0.214	0.196	0.155	0.040	0.040
	2	0.023	0.014	0.012	0.007	0.001	0.001
5	5	0.500	0.382	0.360	0.292	0.087	0.087
	4	0.110	0.070	0.057	0.040	0.005	0.005
10	10	0.783	0.650	0.640	0.547	0.207	0.207
	9	0.416	0.292	0.263	0.199	0.038	0.038
	8	0.160	0.099	0.079	0.055	0.006	0.006
20	20	0.944	0.855	0.862	0.783	0.391	0.391
24	24	0.964	0.890	0.900	0.829	0.444	0.444
30	30	0.980	0.923	0.935	0.876	0.510	0.510

For both these systems, the lower probabilities in the two final columns are identical as in these cases the systems only function if all 24 components function. The other cases give different results due to the different system configurations. For example, 22-out-of-24 system functions for more combinations of failing components than two 11-out-of-12 subsystems in a series configuration, for example the former system still functions if there are two failing components both in the same subsystem, in which case the latter system would not function. This explains why the entries related to the first system (Sys1) are greater than those for the corresponding cases, with $k^1 + k^2 = k$, related to the second system (Sys2).

REFERENCE

Coolen, F.P.A, Aboalkhair, A.M. & MacPhee, I.M. 2011. Diversity in system reliability following component testing, *Journal of the Safety and Reliability Society* **30**, pp. 75–93.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Numerical method for the distribution of a service time of a structure subject to corrosion

Adrien Brandejsky, Benoîte de Saporta & François Dufour
INRIA, Team CQFD, France

Charles Elegbede
Astrium, France

ABSTRACT

We propose a numerical method to compute the service time of an aluminum structure subject to corrosion. This example is provided by Astrium. The structure is part of a strategic ballistic missile stored in a nuclear submarine missile launcher and is therefore submitted to strong reliability constraints. We study the loss of thickness by corrosion and more precisely, the distribution of the service time of the structure: the time taken by the thickness loss to reach a critical threshold.

We model the evolution of the thickness loss by a hybrid process belonging to the class of piecewise-deterministic Markov processes (PDMP) introduced by M.H. Davis in (Davis 1993). The service time of the structure is thus an exit time for the PDMP. Our approach is based on the special structure of the PDMP, namely the fact that the only source of randomness of the process is a discrete time Markov chain. We propose a suitable discretization algorithm for this Markov chain based on quantization. For details on the quantization algorithms, the interested reader may consult (Pagès, Pham, and Printems 2004) and the references therein.

The approximation we propose may be easily implemented. Furthermore, and this feature is an important advantage over standard methods such as Monte-Carlo simulations, it is flexible with respect to the threshold we consider. Indeed, in practice, one begins with the preliminary computation of the quantization grids that only depend on the dynamics of the process, in our case the corrosion evolution equation. These grids are stored offline. Next, our method yields, in a very simple way, an approximation of the law of a wide range of service times. This flexibility allows, for instance, to modify the critical threshold and obtain the law of the new exit time with very little further computation. Eventually, we stress the fact that our whole study is rigorous since we provide proofs of convergence of the algorithm in (Brandejsky, de Saporta, and Dufour 2010).

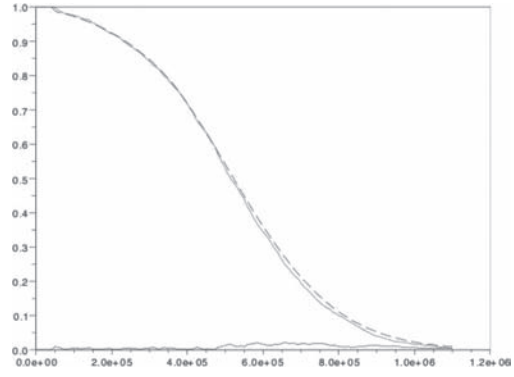


Figure 1. Survival function of the service time obtained through Monte Carlo simulations (dashed black), through our approximation scheme (solid red) and the error between the two functions (solid blue).

REFERENCES

Brandejsky, A., de Saporta, B. & Dufour, F. (2010). Numerical methods for the exit time of a piecewise-deterministic markov process. *Available at http://arxiv.org/abs/1012.2659*

Davis, M.H.A. (1993). *Markov models and optimization, Volume 49 of Monographs on Statistics and Applied Probability*. London: Chapman & Hall.

Pagès, G., Pham, H. & Printems J. (2004). Optimal quantization methods and applications to numerical problems in finance. In *Handbook of computational and numerical methods in finance*, pp. 253–297. Boston, MA: Birkhäuser Boston.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

On generalized shot noise-type stochastic failure model

J.H. Cha
Ewha Womans University, Seoul, Republic of Korea

M. Finkelstein
University of the Free State, Bloemfontein, South Africa

ABSTRACT

We discuss a reliability model that reflects the dynamic dependency between system failure and system stress induced by environmental shock process. Standard assumptions in shock models are that failures of items are related either to the cumulative effect of shocks (cumulative models) or that they are caused by shocks that exceed a certain critical level (extreme shocks models). In this paper, we present useful generalizations of this setting to the case when an item is deteriorating itself, e.g., when the boundary for the fatal shock magnitude is decreasing with time.

Shock models usually consider systems that are subject to shocks of random magnitudes at random times. Traditionally, one distinguishes between two major types: cumulative shock models (systems break down because of a cumulative effect) and extreme shock models (systems break down because of one single large shock). Some references (to name a few) are: Shanthikumar & Sumita (1984), Sumita & Shanthikumar (1985), Gut (1990), Mallor & Santos (2003), Finkelstein (2008), Cha & Finkelstein (2009), Finkelstein & Marais (2010). A combination of these models was investigated by Gut & Hüsler (2005), where the failures were due either to a cumulative effect, or to a single, fatal shock. In this paper, we are somehow in the framework of the latter setting generalizing it to the case when a system itself (apart from the shock process) is deteriorating with time. However, mathematically, our approach is closer to the paper by Lemoine & Wenocur (1986) (see also Lemoine & Wenocur, 1985) and is based on considering the shot noise process-type stochastic intensity as a model for shocks accumulation.

In Lemoine & Wenocur (1986), the system cannot fail directly from a critical shock. However, in many cases, systems can fail due to a shock of a great magnitude. Thus the main goal of our paper is to generalize the model in Lemoine & Wenocur (1986) to the case when a system can also fail due to a fatal shock with the magnitude exceeding the time-dependent bound, which is more realistic in practice. Some illustrative examples are also discussed.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic prognosis of a system: Application to a pneumatic valve

A. Lorton
EADS-Innovation Works, ICD—Université de Technologie de Troyes, UMR STMR—CNRS, France

M. Fouladirad & A. Grall
ICD—Université de Technologie de Troyes, UMR STMR—CNRS, France

ABSTRACT

In the aeronautic industry, the optimisation of the maintenance process is one of the main research goal for economical, ecological and industrial purposes. An interesting approach consists in using Condition-Based Maintenance (CBM) to act on the system based on its current state and before its failure. It requires the computation of the remaining time before this failure occurs, called the Remaining Useful Life (RUL) of the system (see (A. Saxena 2010)). This computation is what we called a prognosis problem. In the present paper, we consider a probabilistic model-based prognosis. The probabilist framework indeed allows to take into account the uncertainties inherent in this problem (unknown degradation process, forecast on some future conditions, complex system, …). The model-based aspect provides a natural way to integrate expert knowledges on the physical behaviour of a system.

We first define our prognosis problem in mathematical terms, and propose a methodology to solve it for specific cases. We consider a stochastic process $Z = (Z_t)_{t \in \mathrm{R}}$, modeling the degradation state of the system through time. The RUL at a prognosis time t, namely RUL_t is then define as the smallest time s after t when the system is considered as useless. Since z is a stochastic process, the RUL_t is a random variable for each t. A first idea is to compute its cumulative distribution function. However, to specify a prognosis for a particular system, it is essential to integrate the information available through monitoring or inspections. A prognosis result adapted to each situation is then the conditional distribution function of RUL_t with respect to the observation process.

We then propose a way to approximate this quantity when the underlying process Z is markovian. Since many traditional models are markovian (pure jump markov processes, Gamma processes, …), this is a reasonable hypothesis. Our methodology consists in a two steps technique. Firstly, the observations are integrated to obtain the conditional probability law of the state of the system at prognosis time. A particle method (see (del Moral 2004)) provides an approximation of this law. Secondly, based on this conditional law, a reliability computation of the system between t and s is required. We propose new reliability estimators when the underlying process is a Piecewise Deterministic Markov Process (see (Davis 1993) or (Cocozza-Thivent 2011), in french).

We illustrate our methodology on an aeronautic example: a pneumatic valve within the BLEED air system. A model of this valve is proposed in (Daigle & Goebel 2010). We adapt this model to compute the RUL of our valve system for a specific degradation process and periodic inspections.

REFERENCES

Cocozza-Thivent, C. (2011). *Processus de Renouvellements Markoviens, Processus de Markov Déterministes par Morceaux*. http://perso-maths.univ-mlv.fr/users/cocozza.christiane/recherche-page-perso/RMetPDMP.pdf

Daigle, M. & K. Goebel (2010). Model-based prognostics under limited sensing. In *Aerospace Conference, 2010 IEEE*, pp. 1–12. IEEE.

Davis, M. (1993). *Markov Models and Optimization*, Volume 49 of *Monographs on statistics and applied probability*. Chapman and Hall.

del Moral, P. (2004). *Feynman-Kac Formulae*. Probability and its Applications. Springer.

Saxena, A. Celaya, J. & B.S.S.S.K.G. (2010). Metrics for offine evaluation of prognostics performance. *International Journal of Prognostics and Health Management*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability of the power electronic components by their dynamical simulation in real working conditions

Jérôme de Reffye
Pi-Ramses Cy, Versailles, France

ABSTRACT

The actual forecast of the reliability of the electronic components is based on methods using analytical formulations established from experimental data. An upgrading processing was operated from the MIL HDBK 217 to the FIDES methodology. But these approaches give only the reliability of components without functional analysis.

Moreover these approaches supply only parameters of reliability that are smoothed by the data processing of the return of experiment and the used empirical formulations. The rates of failure that are supplied suffer a bias between the system in which the components work and the systems that are the origin of the reliability data.

In a same way the variance of the rates of failure is made of the uncertainties of the data of the return of experiment and these data are unknown. If one needs only rough results on parameters of reliability such methods are useful because they are very easy to use. But if we want to analyse the reliability of a real system as control-command system and its real characteristics in operation such methods are inappropriate.

It becomes very important to know the properties of electrical networks and the conditions of work of the power semi-conductors in these networks to estimate really the parameters of reliability of the power electronic systems. This is the reason why we propose an approach of the reliability of the electronic systems based on the physical knowledge of the behaviour of the components of these systems. The electronic cards are analysed according to the thermal mechanical stresses and their reliability is calculated by a strength-stress method.

The behaviour of power semi-conductors is analysed by the variation of the applied voltage, current and their first derivates caused by the fluctuations of charge applied to the electrical net of the electronic system. Their reliability is calculated by a strength-stress method in which the strength parameters are calculated from the quantum mechanics of the physical junctions or supplied by the manufacturer. This approach is a very useful complement of the actual methods to forecast the reliability of the electronic system.

We show in a didactic example how to use in practices this method.

REFERENCES

Alexéev, V. Commande optimale Ed. Mir, 1982.
Feller, W. An Introduction to Probability Theory and its Applications. J. Wiley & Sons, 1980.
Fouillé, A. Electrotechnique à l'usage des ingénieurs. Dunod, 1981.
Internet site. Fides.reliability.org.
Lessons on the mechanics of continuous media of the Ecole Nationale Supérieure des Arts et Métiers (ENSAM).
Procaccia, H. & Suhner, M-C. Démarche bayésienne et applications à la sûreté de fonctionnement. Hermès – Lavoisier, 2003.
Ringler, J. Une extension de l'approche résistance/contrainte appliquée à la modélisation des lois de défaillance des composants électroniques. RSA, tome 31, n°2.
Roïtenberg, S. Théorie du contrôle automatique. Ed. Mir, 1983.
Séguier, G. L'électronique de puissance, Dunod, 1996.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Scenario analysis and PRA: Overview and lessons learned

Diego Mandelli & Tunc Aldemir
Nuclear Engineering Department, The Ohio State University, OH, US

Alper Yilmaz
Photogrammetric Computer Vision Laboratory, The Ohio State University, OH, US

ABSTRACT

The recent trend to use a best estimate plus uncertainty (BEPU) approach to nuclear reactor safety analysis [1] instead of the traditional conservative approach can produce very large amounts of data. Hence, the need for methodologies able to handle high volumes of data in terms of both cardinality (due to the high number of uncertainties included in the analysis) and dimensionality (due to the complexity of systems) arises. Clustering methodologies [2] offer powerful tools that can help the user to identify scenario groups that are representative of the data and, hence, can reduce the effort involved in data analysis. By scenario clustering we mean two actions:

- Identify the scenarios that have a similar behavior (i.e. identify the most evident classes)
- Decide for each event sequence to which class it belongs (i.e., classification)

In the past few years, the Nuclear Engineering Program at The Ohio State University has been involved in the development of such clustering methodologies and algorithms. The specific type data under consideration are those generated using the Dynamic Event Tree (DET) [3] approach for nuclear power reactor transients described by a large set of state variables (i.e., temperature, pressure of specific nodes in the simulator) and information regarding the status of specific components/systems. The purpose of this paper is to present a summary of the research activities regarding the post-processing of scenarios generated by safety analysis codes. Techniques regarding clustering of the raw data, using in particular Mean-Shift Methodology [4], will be overviewed highlighting also lessons learned and possible future research developments. In addition, preprocessing of the raw data and data reduction techniques will be described and compared. Several examples will be presented in order to illustrate the applications of clustering algorithms to data generated by safety analysis codes.

REFERENCES

[1] A. Bucalossi, A. Petruzzi, M. Kristof, & F. D'Auria, 2010. Comparison between Best-Estimate-Plus-Uncertainty Methods and Conservative Tools for Nuclear Power Plant Licensing. Nuclear Technology, 172, 29–47.

[2] K. Dubes, A.K. Jain & C. Richard, 1988. Algorithms for clustering data. Prentice-Hall Inc., Upper Saddle River.

[3] C. Acosta & N. Siu, 1993. Dynamic event trees in accident sequence analysis: application to steam generator tube rupture. Reliability Engineering and System Safety, 41, 135–154.

[4] D. Mandelli, K. Metzroth, A.Yilmaz, R. Denning & T. Aldemir, 2010. Probabilistic Clustering for Scenario Analysis. Proceedings of the American Nuclear Society (ANS), Las Vegas (NV), 103, 371–37.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Small failure probabilities and copula functions: Preliminary studies on structural reliability analysis

E.A. Tamparopoulos, P. Spyridis & K. Bergmeister
BOKU University of Natural Resources and Life Sciences, Vienna, Austria

ABSTRACT

In the present study, the concept of copula functions is used for the construction of multivariate models. Moreover, an evaluation of the structural reliability approach is attempted with respect to the uncertainty owing to assumed correlation coefficient values. Based on a probabilistic analysis of a particular construction system, the problem of evaluating small failure probabilities is discussed in the light of the aforementioned uncertainty.

A stochastic analysis of a single anchor under tension, failing with concrete cone breakout, shown in Figure 1, is considered as a case study. The system's ultimate load can be calculated by means of two correlated concrete parameters, namely the modulus of elasticity E_c and the fracture energy G_f. The effect of various dependence models can be then demonstrated either by calculating the ultimate load value for different predefined failure probabilities, or by calculating the probability of failure for various assumed system loads. In order to evaluate the significance of the underlying dependence structure, three different bivariate models, built upon the theory of copula functions, with Pearson's correlation coefficient $r = 0.5$, and identical marginal distributions, were used in the analysis. Probabilistic expressions regarding the two correlated parameters were adopted by recent relevant studies.

An analysis of the model regarding the involved parameters and their probabilistic expressions discloses that the assumed order of magnitude of failure probability is associated with different demands on accuracy. In fact, the analysis reveals that the effect of the dependence structure induces a significant uncertainty, even for such systems with just two associated parameters. Therefore, using only the Pearson's correlation coefficient value to describe dependence is able to deliver a value for the probability of failure which is valid, at best, as an order of magnitude. The results suggest that attention should be drawn to proper multivariate modeling when high reliability is required. Especially in cases when safety is the main concern and structural design is based on very low target failure probabilities, accurate dependence modeling based on copula functions, becomes vital.

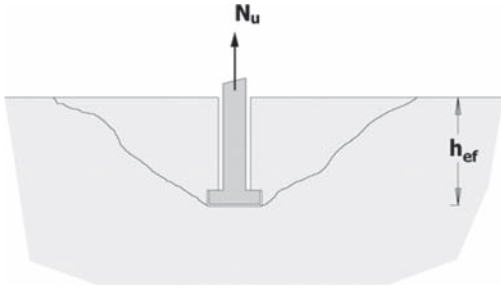


Figure 1. Single concrete anchor failing with concrete cone failure.

REFERENCES

Bergmeister, K., Rieder, A. & Strauss, A. 2004. Bemessung durch Versuche (Assessment through experiments – in German). Department of Civil Engineering and Natural Hazards, University of Natural resources and Applied Life Sciences of Vienna.

Eligehausen, R. & Sawade, G. 1989. A Fracture Mechanics based Description of the Pull–Out Behavior of Headed Studs embedded in Concrete. In L. Elfgren (ed.), Fracture Mechanics of Concrete Structures, RILEM report: 281–299. London: Chapman and Hall.

Nelsen, R.B. 2006. An Introduction to Copulas. Springer Verlag.

Strauss, A. 2003. Stochastische Modellierung und Zuverlässig-keitsanalyse von Betonkonstruktionen (Stochastic modeling and reliability of concrete structures – in German). Dissertation, University of Natural Resources and Life Sciences, Vienna.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Structure decision making for MSS refrigeration system

Ilia Frenkel & Lev Khvatskin
Center for Reliability and Risk Management, SCE—Shamoon College of Engineering, Beer Sheva, Israel

Anatoly Lisnianski
Reliability Department, The Israel Electric Corporation Ltd., Haifa, Israel

ABSTRACT

Supermarkets suffer serious financial losses because of problems with their refrigeration systems. Principal refrigeration system includes 4 basic elements: compressors, evaporators, thermo-expansion valves and roof top condensers with blowers. Due to the system's highly integrated nature, a fault in a single unit can't have detrimental effects on the entire system, only decrease of system cooling capacity. Failure of compressor or axial condenser blower leads to partial system failure (degradation of output cooling capacity) as well as to complete failures of the system. We treat refrigeration system as Multi-State System (MSS), where components and systems have an arbitrary finite number of states. According to the generic MSS model (Lisnianski et al., 2010), the system can have different states corresponding to the system's performance rates, which are discrete-state continuous-time stochastic processes.

In this paper, a generalized approach is applied for decision making for multi-state supermarket refrigeration system structure. The approach is based on the combined Universal Generating Functions (UGF) and stochastic processes method for computation of availability, output performance and performance deficiency for multi-state system.

We consider a typical refrigeration system that is used in one of Israeli supermarkets (Frenkel et al. 2010). The system consists of 2 identical subsystems: main and reserved. Each subsystem consists from 2 elements: block of 4 compressors and block of 2 axial condenser blowers. The way to growth availability of the system is to replace block of 2 axial condenser blowers on the block of 3 axial condenser blowers. One should compute reliability indices for these two possible structures and make the decision—what structure is more appropriate.

Calculation reliability indices (availability, output performance and performance deficiency) for both systems are presented and determine the areas where required reliability measure's level of the refrigeration system can be provided by configuration "Reserved system with 2 blowers" or "Reserved system with 3 blowers". For example, from Figure 1 one can conclude that the configuration "Reserved system with 2 blowers" cannot provide the required average availability, if it must be greater than 0.995.

It was demonstrated that the combined method is well formalized and suitable for practical application in reliability engineering. It supports the engineering decision-making and determines different system structures providing a required reliability/availability level for the multi-state system.

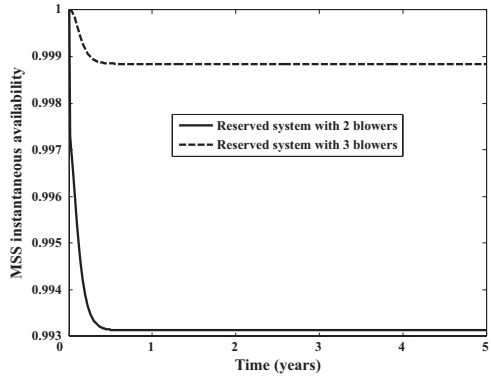


Figure 1. MSS instantaneous availability for different types of systems.

REFERENCES

Frenkel, I., Khvatskin, L. & Lisnianski, A. 2010. Management Decision Making based on Markov Reward Models for Refrigeration System. J Polish Safety and Reliab Ass, 1: 89–98.

Lisnianski, A., Frenkel, I. & Ding, Y. 2010. Multi-state System Reliability Analysis and Optimization for Engineers and Industrial Managers. London: Springer.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

The Inverse Gamma process for modeling state-dependent deterioration processes

M. Guida
Department of Electronic and Computer Engineering, University of Salerno, Fisciano, Italy

G. Pulcini
Istituto Motori, CNR, Naples, Italy

ABSTRACT

The Gamma process model is widely used for describing non-decreasing deterioration processes over time mainly due to its mathematical tractability (see, e.g., Bagdonavičius & Nikulin (2000)). The property of "independence of increments", however, confines the use of this model to deterioration mechanisms where the probability distribution of deterioration increments depends on the current time t and not on the current state of the unit at time t.

Although the description in terms of the degradation level as a function of time, say $\{W(t), t \geq 0\}$, is the usual "direct" way of modeling a deterioration mechanism, it makes also sense (e.g., for reliability evaluations) to consider the "inverse" process $\{T(w), w \geq 0\}$, i.e., the process of the first time for reaching the degradation level w. It is worth noting that, when the "direct" process $\{W(t), t \geq 0\}$ is a purely state-dependent process (i.e., a process where the distribution of degradation increments depends only on the current state w of the item at the time t and not on the current age t), the "inverse" process $\{T(w), w \geq 0\}$ has "independent time increments". Then, the Gamma process model could be appropriately used to describe the process $\{T(w), w \geq 0\}$ and, in such a case, the deterioration process $\{W(t), t \geq 0\}$ is an Inverse Gamma process where the distribution of degradation increments only depends on the current state of the unit (Harlamov, 2006).

This paper proposes non-stationary Inverse Gamma processes for modeling state-dependent deterioration processes with non linear trend. The (conditional) distribution of the deterioration growth ΔW over a generic time interval $(t_0, t_0 + \delta_T)$, given the current state w_0 at the time t_0 is derived in a closed form. The distribution of the time for reaching a given deterioration limit w_{max}, as well the residual lifetime and the residual reliability of the unit, given the current state, are also provided. Maximum likelihood estimates of the parameters which index the Inverse Gamma process are also discussed.

The main advantage provided by the Inverse Gamma process with respect to the existing state-dependent models (Giorgio et al., 2010, and Giorgio et al., 2011) is that, unlike the previous models, the Inverse Gamma process is a time-continuous and state-continuous model, so that its mathematical treatment is much easier. In particular, within the Inverse Gamma process, the (conditional) distribution of the deterioration growth ΔW over a generic time interval, given the current state, is in closed form and hence does not require the time—and state-discretization of the previously proposed models, with the subsequent evaluation of transition probability matrices and onerous calculations.

Finally, the proposed model is applied to a real dataset consisting in the wear process of the liners of some Diesel engines equipping three identical ships of the Grimaldi group. This dataset was previously analyzed in Giorgio et al. (2010) and in Giorgio et al. (2011) and was proved to be a pure state-dependent process. A comparison of the inferential results obtained within the proposed Inverse Gamma process with the results obtained within the previous models shows the ability of the Inverse Gamma process to adequately model the observed state-dependent wear process.

REFERENCES

Bagdonavičius, V. & Nikulin, M.S. 2000. Estimation in degradation models with explanatory variables. Lifetime Data Analysis 7(1): 85–103.

Harlamov, B.P. 2006. On statistics of inverse gamma process as a model of wear. In M. Nikulin, D. Commenges & C. Huber (eds), Probability, Statistics and Modelling in Public Health: 187–201. Springer, New York.

Giorgio, M., Guida, M. & Pulcini, G. 2010. A state-dependent wear model with an application to marine engine cylinder liners. Technometrics 52(2): 172–187.

Giorgio, M., Guida, M. & Pulcini, G. 2011. An age-and state-dependent Markov model for degradation processes. IIE Transactions 43(9), in press.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The method of safe 4D flight trajectory prediction in controlled airspace

M. Piatek
Polish Air Navigation Services Agency, Warsaw, Poland

A. Stelmach
Warsaw University of Technology, Faculty of Transport, Warsaw, Poland

ABSTRACT

A number of trajectory modeling methods have been proposed to automate air traffic conflict detection and resolution (Kuchar, Yung 2000), several of which had been in use or under operational evaluation. Most of described modeling methods have been built from a foundation of structured routes and evolved procedures. The proposed model aims the issues of modeling a safe 4D flight trajectory of aircraft in a future controlled airspace where the structured routes will be used only in high density traffic areas and the airspace free of predetermined routes will be used to manage traffic flows.

The elaborated method of planning the 4D trajectory allows to:

- verify the separation of the aircrafts,
- check the separation of the trajectory from the elements of the airspace,
- set a different flight trajectory in order to avoid a potential midair collision or in case there is no possibility for take-off or landing with given flight parameters,
- set all trajectories in such a way that the aircrafts landing in the same airports would enter the controlled airport area keeping appropriate separations,
- set all trajectories with minimum total fuel consumption and with the smallest number of changes in the flight parameters (direction, altitude and speed).

The proposed model of controlled airspace (Piatek M., 2010) includes randomly planned air routes as well as criteria of choosing safe and separated flight trajectories. Modified Dijkstra algorithm (Dijkstra, 1959) has been used for model implementation.

The elaborated concept aims at increasing the capacity of the sectors responsible for operational planning in future and current structures of the controlled airspace, maintaining the safe and separated realization of air operations.

Table 1. The calculation results for the air-carriers benefiting from the greatest profit in the fuel consumption.

N	Carrier	ΔL [%]	ΔL [kg]	ΣL [kg]
230	LOT	10.88	19,665.65	180,820.18
57	RYR	9.84	5479.26	55,699.71
76	CLW	6.45	5461.67	84,659.63
49	ESK	11.12	3782.84	34,018.81
34	WZZ	8.94	3636.28	40,686.24
235	DLH	0.46	2242.00	488,103.64
43	BAW	1.24	2200.67	177,224.44
28	EZY	6.26	1761.15	28,111.92
62	AFL	0.98	1330.70	135,488.68
20	GWI	6.60	131908	19,983.16

The proposed method of determining the non-collision trajectory of a 4D flight in a controlled space allows the decrease of the aircraft operators' costs. This aim has been reached while providing the required separation of relative flights' trajectories and the trajectories relative to separated airspace elements at the medium-range planning.

The simulation research, utilizing real air traffic and airspace description data, proved the applicability of the proposed method to the real world air traffic planning software. Table 1 presents the calculation results for the top 10 air-carriers that experienced the greatest absolute fuel consumption decrease (ΔL) during the simulation research.

REFERENCES

Dijkstra, E.W. 1959. A note on two problems in connexion with graphs. *Numerische Mathematik*, 1: 269–271.

Kuchar, J.K. & Yang L.C. 2000. A Review of Conflict Detection and Resolution Modeling Methods. *IEEE Transactions on Intelligent Transportation Systems*, Volume 1, No. 4.

Piatek, M. 2010. The metod of safe free flight trajectory modeling and prediction in controlled airspace. *PhD Thesis*, Warsaw University of Technology.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Process oriented simulation framework for Common-Cause Failure assessment

E. Bejdakic, M. Krauß & H.-P. Berg
Bundesamt für Strahlenschutz (BfS), Germany

ABSTRACT

Dependent failures, in particular so-called Common Cause Failure (CCF), are extremely important in reliability and safety analysis due to their potential to lead to a simultaneously loss of several redundant systems or components. Therefore, consequences of common-cause failures are one of the major issues in probabilistic safety assessment, not only of nuclear power plants, and must be adequately treated to minimize an underestimation of reliability. Experience from numerous probabilistic safety assessments has shown that, especially for highly redundant systems in nuclear power plants, common cause failures can dominate the results of these assessments such as the core damage frequency or large early release frequency. Depending on the studies considered and especially the design of the respective nuclear power plant analysed, failure of several components can contribute between twenty and more than eighty percent to the system unavailability which is correlated to the calculated value of the core damage frequency in case of nuclear power plants. Due to the small number of observed events resulting from identified common cause failures, it is difficult to assess this issue in the short run. It is therefore necessary to gather data over an extended period of time and test various models against that data.

Process Oriented Simulation framework (POS) (**?**) is an approach for quantification of component unavailability caused by common-cause failures. It can be seen as an extension of the Binomial Failure Rate model (BFR) (**?**, **?**) and was introduced in the 1990s. POS model uses Monte Carlo simulation technique to compute the unavailability of components. The POS model distinguishes explicitly between immediate and delayed failures and it does not assume that all components are affected by the Common Cause (CC). Instead, it treats the number of components affected by CC as a stochastic variable. Further, the POS model has the ability to model various relevant stages of the CCF process, hence the name of the model. In this paper, we use the standard Maximum Likelihood Estimation (MLE) method and apply it on accumulated isolating slide valve data from German nuclear power plants. The data needed for the process oriented simulation model are given in Table 1, the r is the redundancy and m is the number of components affected by common cause, both damaged and actually failed. We compare the results with parameter values obtained using estimation method described in previous publications. The resulting unavailability is presented in Figure 1.

Table 1. Data needed for the parameter estimation of POS model.

r	4	4	2	3	4	4	3	2	4
m	4	2	2	2	4	4	2	2	4

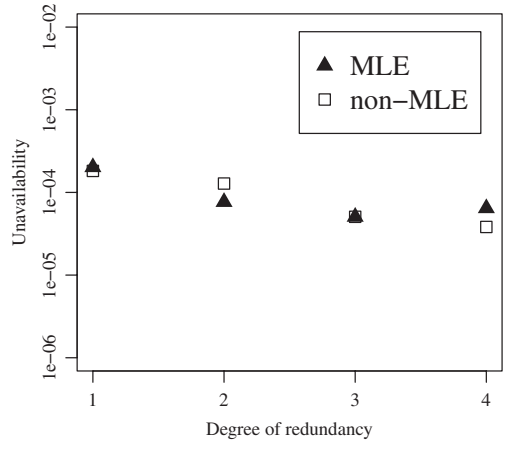


Figure 1. Unavailability from two parameter estimation methods.

REFERENCES

Atwood, C. (1986). The binomial failure rate common cause model. *Technometrics 28*, 139–148.

Berg, H.-P., Görtz, R., Mahlke, J., Reckers, J., Scheib, P. & Weil, L. (2008). The POS model for common cause failures quantification. BfS-SK 10/08, Bundesamt für Strahlenschutz (BfS).

Vesely, W. (1977). Estimating common cause failure probabilities in reliability and risk analyses: Marshall-Olkin specializations. *Fussell and Burdick, eds., Nuclear systems reliability engineering and risk assessment. Soc. Ind. Appl. Math.*, 314–341.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The unique signal applied to weapon system safety design

L.Y. Xiao, J. Li, B. Suo & S. Li
Institute of Electronic Engineering, China Academy of Engineering Physics, China

ABSTRACT

Because of the safety of weapons is very important, many safety design methods have been produced. The fuze safety system pays an important part in the weapon safety design. In general design method, multiple environmental signal and safety switch are used to achieve safety goal. This will lead to complex of the system, and the quantization of the safety failure rate is made difficult. Then, there is an integrated concept to approach the above mentioned problems: an arming signal, which can not be generated in normal or abnormal environment, should be found, the probability of whose accidental occurrence is low and the quantization of which is easy. And this can be called the "unique signal". The UQS methodology provides resistance to various threats that might be present in abnormal environments, in particular significantly reducing vulnerability to non-random threats, while optimizing resistance to random threats.

The unique signal is a binary sequence the elements of which are all taken from the set I = (A, B), marked C_k, having a length marked n. And this is a pseudorandom sequence. If the accidental occurrence probability of C_k is P (C_k) and ε is a small enough positive number, C_k is a unique codes whose occurrence probability is smaller than ε and ε is the maximum occurrence probability.

The UQS codes consist of three elements: event, pattern and length. The UQS pattern refers to the particular sequence, where lies the core of the uniqueness of the UQS codes. And an UQS pattern is supposed to meet the following selection criteria:

a. the number in the event As and event Bs are equal or seem to be equal to each other;
b. the number of the event pairs (AA, AB, BA, BB) are equal or seem to be equal to each other;
c. the recurring event string (run-length) should be as short as possible, where the length of the maximum run cannot exceed 4 and the inversed UQS codes and the complementary codes are tested with the maximum run-length;
d. it must not be periodic;
e. it must be asymmetrical;
f. the occurrence probability of event As with various run-lengths must be different from that of event Bs.

The UQS length refers to the number of the events, which makes sure that the safety failure rate of the system has a theoretical upper bound that is 2^{-n} (n is the number of the UQS codes). The above listed criteria have all been mathematically strictly justified, ensuring that the maximum occurrence probability of this pattern is smaller than that of any other pattern with the same length.

Different from the design of the ordinary switches, the switch for UQS codes is Strong Link, which must decodes all the UQS codes on the one-per-cycle basis and will be locked in case of any wrong codes, that is, to be kept in a safe place.

Furthermore, Strong Link is strong in that its mechanical construction can resist abnormal environment. And the decoding process of SL can be well expressed in the following binary labyrinth. In this paper, the fuze safety system based on UQS is provided.

Adopting the UQS, the constitution of the system can be simplified, with safety ensured. Meanwhile, the designing criteria of UQS make it possible to quantize its accidental occurrence probability, which is supposed to provide the basic data for the calculation of the safety failure rate of the system.

REFERENCES

Arlin Cooper, J. 2002. Mathematical Aspects of Unique Signal Assessment. New Mexico: Albuquerque.

Curt Mueller & Stan Spray. 1992. The unique signal concept for detonation safety in nuclear weapons. New Mexico: Albuquerque.

Ekman, M.E., Werner, P.W. et al. 1997. *A thematic approach to system safety.* New Mexico: Albuquerque.

Gary T. Randall. 1994. High Consequence System Surety Process Description. New Mexico: Albuquerque.

MIL-HDBK-272A(OS). 1993. *Nuclear weapons systems, safety design and evaluation criteria for*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty analysis via failure domain characterization: Polynomial requirement functions

L.G. Crespo
National Institute of Aerospace, VA, US

C.A. Muñoz, A.J. Narkawicz, S.P. Kenny & D.P. Giesy
NASA Langley Research Center, Hampton, VA, US

ABSTRACT

This paper studies the reliability of a system for which a parametric mathematical model is available. The acceptability of the system depends upon its ability to satisfy several design requirements. These requirements, which are represented by a set of inequality constraints on selected output metrics, depend on the uncertain parameter vector $\boldsymbol{p}$. The system is deemed acceptable if all inequalities are satisfied. The constraints partition the uncertain parameter space into two sets, the failure domain, where at least one of them is violated, and the safe domain, where all of them are satisfied. The reliability analysis of a system consists of assessing its ability to satisfy the requirements when $\boldsymbol{p}$ can take on any value from a prescribed set. The most common practice in reliability analysis is to assume a probabilistic *uncertainty model* of $\boldsymbol{p}$ and estimate the corresponding probability of failure. Sampling-based approaches (Niederreiter 1992, Kalland Wallace 1994) and methods based on asymptotic approximations (Rackwitz 2001) are the engines of most of the techniques used to estimate this probability.

Reliability assessments whose figure of merit is the probability of failure are strongly dependent on the uncertainty model assumed. Quite often this model is created using engineering judgment, expert opinion, and/or limited observations. The persistent incertitude in the model resulting from this process makes the soundness of the reliability analyses based on failure probabilities questionable. Furthermore, the failure probability fails to describe practically significant features of the geometry of the failure event. Some of these features are the separation between any given point and the failure domain, the location of worst-case uncertainty combinations, and the geometry of the failure domain boundary.

This paper proposes an uncertainty analysis framework based on the characterization of the uncertain parameter space. This characterization enables the evaluation of the features listed above, the approximation of the failure and safe domains and the calculation of arbitrarily tight bounds to the failure probability. A significant thrust of this research is the generation of sequences of inner approximations to the safe and failure domains by subsets of readily computable probability. These sequences are chosen such that they almost surely fill up the region of interest. The strategies proposed, which are only applicable to requirement functions having an explicitly known polynomial dependency on the uncertainty, are based on Bernstein expansions and sum of squares programming. Some of the most prominent features of the methodology are the substantial desensitization of the calculations from the uncertainty model assumed as well as the accommodation for changes in such a model with a practically insignificant amount of computational effort. The companion paper (Crespo et al., 2011) proposes strategies with the same goal but applicable to unrestricted requirement functions.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty assessment in semi Markov methods for Weibull functions distributions

M. Zajac & A. Kierzkowski
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Dependability indices like reliability and related measures, as availability, maintainability, failure rate, mean times, etc., are very important in design, development and lifetime analysis of real systems.

It is worth to point out that there is an assumption that during the calculation of the dependability contributors for technical objects that are under investigation, probabilities of transition between states or sojourn times' probabilities are exponential. Many causes, for example, lack of information, small sample sizes, or inaccurate assessment of data may result in the model assumptions being violated. In some cases, when exponential distribution is assumed, there is also possibility to assess factors according to different distributions, like Weibull, Erlang, etc.

Probabilities of transition between states and availability belong to the fundamental characteristic of reliability. The discrete-time case can be obtained from the continuous one, by considering counting measure for discrete time points. However we consider that important is to make it separately for this case, since an increasing interest is observed in practice for the discrete case. There are attempts to calculate factors with continuous-time in literature, however calculations are prepared using exponential functions distributions. In engineering practice it very important to obtain accurate results without using strong simplifications.

The paper consists of discussions about the possibility and about the reason of carrying out these calculations, which is made by the application of simple models of the Markov and Semi-Markov processes, where there are attempts of use of continuous time in these calculations. Discussion is based on hypothetical exponential and non-exponential sojourn times' probabilities. Valuation of these methods is based on the comparison of availability and probabilities of transition values when using exponential and Weibull functions distributions. Previous experience presented in gave a reason to estimate uncertainty of calculation method, when Weibull functions distributions and Semi-Markov solution and also continuous time are applied.

The paper consist discussion on possibility and reasonability of carrying out calculation using Markov and semi-Markov methods on simple example with attempts to use continuous time in calculations. Discussion is based on prepared exponential and non-exponential sojourn times' probabilities. Valuation of methods is based on comparison availability and probabilities of transition values.

For needs of particular example two states set-up is prepared, which is mathematically described by semi Markov process. Prepared data includes information on sojourn times during 100 points of time. Collected data didn't allow for verify probabilities distribution. However the data allow to asses main parameters characterizing sample according to exponential, Weibul and Erlangl functions distributions.

In "macro scale" implementation of different functions distributions doesn't give serious differences in values of availability and transient probabilities. However in "micro scale" some disparities can be visible.

REFERENCES

Barbu, V. & Limnios, N. (2008). Semi-Markov chains and hidden Semi-Markov models. Toward applications. Lecture notes in statistics, vol. 191, Springer.

Chryssaphinou, O., Limnios, N. & Malefaki, S. (2010). Multi-state reliability systems under discrete time Semi-Markovian hypothesis. IEEE TR.

Grabski, F. (2002). Semi Markov models of reliability and maintenance (in polish). Polish Academy of Sciences, System Research Institute.

Lisnianski, A. & Levitin, G. (2003). Multi-state system reliability. World Scientific.

Zajac, M. & Budny, T. (2009). On determination of some characteristics of Semi-Markov process for different distributions of transient probabilities. R&RATA #2(13), (Vol. 2).

This page intentionally left blank

Occupational safety

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An engineering and psycho-social integrated approach for Work-Related Stress (WRS) assessment and management

P. Citti
Università degli Studi "G. Marconi" di Roma, Rome, Italy

M. Delogu, A. Meneghin & F. Pagliai
Università degli Studi di Firenze, Florence, Italy

ABSTRACT

According to the Framework Directive 89/391/EEC, all employers have the duty of protecting the occupational safety and health of all workers. As suggested by the ECJ interpretation, that also concretely refers to the WHO definition of "health" ("a state of complete physical, mental and social well-being"), this duty also applies to work-related stress problems. The Framework Agreement on work-related stress of 8 October 2004, and the EU Council Resolution of 25 june 2007 confirmed and clarified the strong EU commitment to ensure health and safety at work, effectively facing work-related stress. Work-related stress problems may be handled within an overall process of risk assessment, through a methodological approach fitted for specific work-related stress risk features.

Although traditionally associated to engineering, the risk assessment and process optimization methods increasingly find their application in very different contexts. Since each set of objects and people interacting with each other can be considered a system and that any sequence of activities aimed at achieving a goal can be regarded as a process, it follows that the theories and techniques developed for quality systems can become effective in very diverse fields of expertise. Furthermore, the more complex the systems become and the more processes affect the human sphere, the more it is necessary to overcome the anachronistic disciplinary boundaries.

Therefore the challenge was to look at the work-related stress as a process whose variables, once identified, could be measured, analyzed, evaluated and optimized using the correct sequence of process analysis traditional tools.

This contribution pertains to the development and the outcome of an analysis and optimization approach performed to assess the risks of work-related stress inside the University of Florence, Italy. The activities have been led by a cross-curricular committee (quality engineering, work psychologists, University safety managers, technical staff and Equal Opportunity Committee members).

The University Scientific and Technological (UST) Campus was chosen as the survey domain, mainly because of its high level of activity diversification; the stress-related issues in Departments and Offices have been evaluated and associated with a set of potential improvement actions. All the steps were planned and carried out collectively by the investigation Board, involving in the entire process both the teaching and the administrative/technical staff.

The use of a logical flow of risk assessment and process optimization methods (based on Fishbone diagram, Pareto and the use of correlation matrices), tailored and integrated with psycho-social communication and decision making techniques, (based on questionnaire, brainstorming, focus group), has allowed the team to describe the context in which it was operating and the expectations of stakeholders, to define the critical processes, to identify priorities for action, to build a set of possible improvement solutions and finally to select the key actions to be implemented in agreement with the University management.

REFERENCES

Harry, M. & Schroeder, R. 2000. *Six sigma: the breakthrough management strategy revolutionizing the world's top corporations*. New York: Currency.

Health and Safety Executive (HSE) 2007. Managing the causes of work-related stress - A step-by-step approach using the Management Standards. UK: HSE Books.

Leka, S. & Cox, T. 2008. The European Framework for Psychosocial Risk Management: PRIMA-EF. UK, Nottingham: I-WHO Publications.

Montgomery, D.C. 2009. *Introduction to Statistical Quality Control, 6th Edition*. Arizona: John Wiley & Sons.

National Institute for Occupational Safety and Health (NIOSH) 2002. *The changing organisation of work and the safety and health of working people*. Report No. 2002–116. USA, Cincinnati: NIOSH.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Applying the safe place, safe person, safe systems framework to the healthcare industry

O. Lasaki, A.-M. Makin & C. Winder
The University of New South Wales, Sydney, Australia

ABSTRACT

Makin's original Safe Place, Safe Persons, Safe Systems approach provided a strategic OHS management tool, derived from the literature and underpinned by the creation of a comprehensive hazard profile of the organisation in question (Makin and Winder, 2008; 2009). The original framework, consisting of sixty elements was transformed into an assessment tool, trialed and validated by peer review, then applied to eight case studies, spanning different industries ranging from construction to manufacturing. It was suggested that this approach could be used universally across these industries.

Historically, the healthcare industry at the turn of the twentieth century had adopted the safety management model of high-risk profile industries such as aviation and the nuclear industry at a time when injuries due to negligent behaviour and procedural errors were high. However, at the time of this transition, many authors had argued that the direct adaptation of safety initiatives from high reliability organisations in high risk industries to healthcare would be deficient owing to the difference in culture between industries. The subsequent framework that emerged has been referred to as being "fragmented," as a higher priority is given to patient safety than worker safety.

The focus of the present study was to conduct a literature review of safety management within the healthcare industry in order to provide a comprehensive hazard profile, identify and assess the current trends, the prevailing culture, and barriers to improvement interventions. It also sought to clarify if there was a fragmented framework and to find out what fed this pattern. The study uses the Safe Place, Safe Persons, Safe Systems assessment tool as a guide for reviewing the literature systematically, to perform a gap analysis of the current management strategies and to examine the characterisation of the hazard profile attributed to the healthcare industry in Makin's original work and the efficacy of the assessment tool in its use in the healthcare industry. This review highlights the safety climate within the industry and the challenges the industry faces in developing a holistic safety management approach.

The study details the differences in culture between the high reliability organisations, which historically the healthcare industry had tried to mirror in its approach to safety management and how these differences affect implementation and eventually the outcomes of safety management in the healthcare industry. It also emphasises the need for a more integrated approach to safety management in the industry through cross-specialty collaboration, and other strategies such as modification of the educational curriculum, which are all aimed at changing the current culture. In all, a total of 135 articles were analysed and sorted into groups relating to "Safe Person, Safe Place and Safe Systems."

This review also allows for an assessment of the applicability of the Safe Place, Safe Persons and Safe Systems assessment tool in the healthcare industry. At the end of the review it is suggested that there is a need for customisation of the current framework by the adoption of one new element—dynamic risk management and modification of some existing elements so that the assessment tool becomes explicitly suited to the needs of the healthcare industry. The study concludes that the approach brings a practicality to the assessment of safety management systems and affords practitioners a systematic and strategic solution within the healthcare industry, to dealing with a "fragmented" safety management culture.

REFERENCES

Makin, A.M. & Winder, C. (2008). A new conceptual framework to improve the application of occupational health and safety management systems. *Safety Science* 46: 935–948.

Makin, A.-M. & Winder, C. (2009). Managing hazards in the workplace using organisational management systems – a safe place, safe person, safe systems approach. *Journal of Risk Research*, 12: 329–343.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Applying the safe place, safe person, safe systems framework to the management of biohazards

A. Bamford, A.-M. Makin & C. Winder
The University of New South Wales, Sydney, Australia

ABSTRACT

Biological hazards (biohazards) are present from exposure to infectious micro-organisms, toxic substances of biological origin, and plants and animals. Animals are among the few animate objects with which workers interact, placing them in a special class of workplace hazards. Working with, or in the presence of, animal(s) requires special attention to the unique hazards they pose.

This study describes the application and evaluation of the Safe Place, Safe Person, Safe Systems framework (Makin and Winder, 2008; 2009) to the management of biohazards encountered when working with animals, with a purpose of examining the efficacy and suitability of the framework. This study consisted of a review of the literature on biohazards in animal-related professions, typically in the context of veterinary practices and zoos, and their management in the workplace. This is a new area where the model has not been previously applied.

Risks associated with working with animals were found to be divided into three categories: direct physical risks, infectious diseases from animals (zoonoses); and hypersensitivity risks.

The framework brings together the merits of the three main control strategies that have emerged for dealing with workplace hazards (namely safe place, safe person and safe systems) to ensure that an OHS MS has been carefully constructed and customised to the individual organisation.

For Safe Place elements, aspects that were considered important were: (i) workplace design and function, including access/egress, plant and equipment, ergonomic evaluation, maintenance; (ii) common workplace hazards, such as hazardous chemicals, manual handling, noise and of course, biohazards; and (iii) systems for non-routine situations and adverse events, such as security and emergency planning.

For Safe Person elements, aspects that were considered important were: (i) obtaining good personnel, job descriptions, selection criteria, health surveillance, performance appraisals, training and further education; (ii) work design, such as job demands, workloads and stress awareness and its management, and (iii) aspects of risk controls relying on worker behaviour, such as personal protective equipment and first aid/reporting.

For Safe System elements, aspects that were considered important included OHS policy, infection control systems, competent supervision, incident management and overall system review.

However, this analysis also identified many elements that were not well established in this industry sector, such as goal setting, accountabilities, due diligence review, communication, consultation, safe working procedures, contractor management. While many of these were poorly covered, their importance is well established. Identification of systems critical for organisational OHS management that were absent is an important benefit of this type of review.

A key finding in this study was that the Safe Place, Safe Person, Safe Systems framework was versatile and could be successfully applied to animal-related professions to promote OHS improvements and to provide a systematic, planned approach to fulfilling OHS responsibilities. It was apparent that a customised OHS MS will allow sufficient freedom to enable workers to exercise their experience, education, judgement and skills as required and the size of the organisation it is being applied to will influence the degree of formality with which it the elements of the framework are applied.

REFERENCES

Makin, A.M. & Winder, C. (2008). A new conceptual framework to improve the application of occupational health and safety management systems. *Safety Science* 46: 935–948.

Makin, A.-M. & Winder, C. (2009). Managing hazards in the workplace using organisational management systems – a safe place, safe person, safe systems approach. *Journal of Risk Research*, 12: 329–343.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Cognitive, affective and behaviour outcomes of a safety training program

L.O. Duarte
Santa Casa da Misericórdia de Lisboa, Lisbon, Portugal

S.A. Olea
Universidad León, León, Spain

S.A. Silva
ISCTE-IUL Instituto Universitário de Lisboa, Lisbon, Portugal

ABSTRACT

Safety training is a key intervention strategy for developing systems, methods and actions that allow more and better safety performance and contributes for changing or developing organizations safety culture.

Moreover, training is well recognized as essential for improving and supporting people safety competencies and actions (e.g., KSAO—knowledge; skills; attitudes and others). For instance, it is expected that training increase safety knowledge (e.g., learning about risks), perceptions (e.g., safety climate), attitudes (e.g., satisfaction with safety), and behaviours (e.g., compliance and participative behaviour). Therefore, it should contribute for individuals cognitive, affective and behaviour change.

Although there is already a consistent body of research showing safety training positive effects and important issues for improving its efficacy (e.g., Colligan & Cohen, 2004; Burke et al., 2006) only very few studies assessed multiple and across time effects for a specific safety program. The present study intends to fulfil this gap.

Departing from Kirkpatrick seminal work (e.g., Kirkpatrick & Kirkpatrick 2006) and most update knowledge about training (e.g., Aguinis, 2009; Ford, Kraiger, Merritt, 2009) and safety training (e.g., Burke et al., 2006) a pre-post test design study was used to assess the outcomes of a safety program.

The study was conducted in four phases which include: 1) initial assessment conducted 15 days prior to training (covering safety perceptions, attitudes and behaviours); 2) evaluation of safety knowledge one hour before the start of training; 3) assessment of safety knowledge 1 hour after training; 4) final evaluation of safety perceptions, attitudes and behaviours, six months after training.

The data was all collected through a self-report questionnaire and the variables were operationalized using scales already validated and subjected to reliability and factor analysis. Internal consistency analysis showed adequate values (Cronbach's alpha between 0.68 and 0.89).

A total of 330 workers from a non-profit institution participated in this study pre and pos test phases.

The training program covered a wide range of topics such as, safety, fire fighting, classes of fire risk, safety signs, emergency lighting and emergency planning including the construction of the prevention plans of action and evacuation.

The safety training method included expository presentations and more engaging strategies as active feedback and behavioural modelling and hands-on training as recommended by Burke et al., (2006).

Results of paired T-test analysis show statistical significant differences for all variables in this study revealing an increase after training (for example, more safety behaviours).

REFERENCES

Burke, M.J., Sarpy, S.A., Smith-Crowe, K., Chan-Serafin, S., Salvador, R.O. & Islam, G. (2006). Relative Effectiveness of Worker Safety and Health Training Methods. American Journal of Public Health n.º2, pp. 315–324.

Kirkpatrick, D.L. & Kirkpatrick, J.D. (2006). Evaluating Training Programs. Berrett-Koehler Publishers, Inc. San Francisco.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Manual handling operations risk assessment

A.R. Burcíaga-Ortega & J.R. Santos-Reyes
Safety, Accident, Risk & Reliability Analysis (SARACS) Research Group, SEPI-ESIME, IPN, Mexico

ABSTRACT

It is believed that every year more than 2 million people die from occupational accidents or work-related diseases. Moreover, there are 270 million occupational accidents and 160 million cases of occupational disease (ILO, 2010). On the other hand, these figures vary enormously between countries, economic sectors and social groups. Furthermore, deaths and injuries take a particularly heavy toll in developing nations, where large numbers of people are engaged in hazardous activities such as agriculture, construction, logging, fishing and mining, etc. (ILO, 2010). Musculoskeletal Disorders (MSD) constitute the largest category of work-related illness in developed and developing countries, and are a major source of pain, disability, restricted activity, lost work days, reduced productivity, and costs to industry and the public service (Dampsey & Hashemi, 1999). For example, the authors found that manual materials handling represented the largest source of claims. These results were compared with those reported by some authors who found that manual materials handling accounted for between 24% and 35% of all injuries.

Given the above, it is clear that manual handling operations may be regarded as a major cause of injury and ill-health in the work place. In order to address these issues, some countries have introduced regulations aiming at preventing MSD related illness. For example, the Manual Handling Operations Regulations 1992 (MHOR) were introduced from 1 January 1993 in the UK (HSE, 1998). Some similar steps have been implemented in the USA. In view of the individual distress, occupational limitations, and economic costs associated with MSD, the topic has attracted much research attention in the fields of epidemiology, medicine, physiology, and psychology. However, there is no evidence of studies associated with MSD being conducted in Mexico.

This paper presents the results of a study conducted on the risks associated with manual handling operations in the retailer and manufacturing sectors (Fig. 1). The approach has been the application of the Manual Handling Assessment Charts (MAC) developed by (HSE, 2002). The MAC tool is intended to help to assess the most common risk factors in lifting, carrying and team handling operations. It is hoped that by conducting studies such as the present case studies, illnesses related to MSDs may be prevented.

Figure 1. Manual handling-Carrying operations.

REFERENCES

Dampsey, P. & Hashemi, L. 1999. Analysis of workers' compensation claims associated with manual materials handling, *Ergonomics*, Vol. 42, 1.

HSE. 1998. *Manual Handling. Manual Handling Operations Regulations 1992*. Guidance on Regulations, (Sudbury, Suffolk: HSE Books), L23, Second Edition. UK.

HSE. 2002. *Manual Handling Assessment Charts*. (Bootle, Health and Safety Executive), MISC 480. UK.

ILO. International Labour organization (ILO). http://www.ilo.org/global/Themes/Safety_and_Health_at_Work/lang--en/index.htm. (15/02/2010).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Measurement of safety social norms at organizations: Construct validation of a safety social norms survey

C.S. Fugas & S.A. Silva
Lisbon University Institute, Portugal

J.L. Meliá
University of Valencia, Spain

ABSTRACT

Attempts to minimize errors and reduce accidents have been predominantly purely reactive, after the occurrence of accidents. The measurement and analysis of safety social norms can be a way to manage safety on a proactive basis in order to improve the safety of individuals in the workplace.

Extending recent findings that social processes underlying safety at work are multidimensional and can impact safety behaviors differently (Fugas, Meliá & Silva, 2009), the present study was designed to test the reliability and construct validity of a questionnaire devoted to the measurement of social influences on safety behavior. This instrument can be useful as a diagnostic tool for intervention aimed at improving safety of the organizations in different industrial sectors.

Following Cialdini and Trost (1998) assumptions, in this paper, safety group norms are considered as informal safety internalized rules emanating from relevant group figures that work groups adopt to regulate group member's behavior and that are used to infer acceptable behavior. Norms include not only a prescriptive element, but also a descriptive element. Descriptive norms refer to perceptions of others' safety behavior, based on observations of how supervisors and coworkers participate in and comply with safety practices and injunctive norms refer to the perceived approval of proactive and compliance safety practices (Fugas, Meliá & Silva, 2011). In contrast to the descriptive norms, which specify what is done, injunctive norms specify what should be done.

The results of this study confirmed the reliability and validity of constructs of the Safety Social Norms Survey. The CFA has played an important role in assessing the dimensionality of the constructs proposed in this study. Results showed the factor structure proposed for 4-factors related to safety social norms. Supervisors and coworkers' descriptive and injunctive norms are not isomorphic constructs, but refer to different dimensions of social influence on safety. The CFA also allowed confirming the convergent and discriminant validity of the safety social norms scales.

The convergent analysis showed that the supervisors' descriptive safety norms scale was strongly correlated with the scale of the organizational safety climate, showing a good convergence between the two constructs. The remaining three scales also had high correlations with the construct of organizational safety climate indicating convergence.

The results of discriminant validity showed that the four constructs of safety social norms and perceived behavioral control are conceptually independent (although correlated) and have a good validity.

These findings can be promising for practice. Norm-based interventions can successfully contribute to correct worker's misperceptions about the safety practices of their peers and supervisors.

REFERENCES

Cialdini, R.B. & Trost, M.R. 1998. Social influence: Social norms, conformity and compliance. In D.T. Gilbert, S.T. Fiske, & G. Lindzey (Eds.), The Handbook of Social Psychology (4th ed., Vol. 2, pp. 151–192). New York: McGraw-Hill.

Conner, M. & McMillan, B. 1999. Interaction effects in the theory of planned behavior: Studying cannabis use. British Journal of Social Psychology, 38, 195–222.

Fugas, C., Meliá, J.L. & Silva, S. 2009. Exploratory and confirmatory analysis of the relationship between social norms and safety behavior. In S. Martorell, C. Guedes Soares & J. Barnett (Eds.), Safety, Reliability and Risk Analysis: Theory, Methods and Applications (vol. 1, pp. 243–248). London: Taylor & Francis Group.

Fugas, C.S., Meliá, J.L. & Silva, S.A. 2011. The "is" and the "ought": How perceived social norms influence safety behaviors at work? Journal of Occupational Health Psychology, 16(1), 67–79.

Zohar, D. & Luria, G. 2005. Multilevel model of safety climate: Cross-level Relationships between organization and group-level climates. Journal of Applied Psychology, 9(4), 616–628.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Organizing for quality and safety in health care—the Norwegian case

S. Wiig
University of Stavanger, Norway

J. Quartz
Erasmus University, Rotterdam, The Netherlands

C.v. Plessen
University of Stavanger, Norway & Hillerød Hospital, Denmark

S. Harthug
Haukeland University Hospital & University of Bergen, Norway

ABSTRACT

Quality and patient safety can be considered as complex processes in socio-technical systems depending on structures, process and information flow between different institutions, organizations and stakeholders. In order to map vital institutions and their relationships and activities to improve quality and patient safety one should approach them from a multi-level perspective (e.g., Wiig, 2008; Rasmussen, 1997) incorporating the macro (national health care system), meso (hospital) and micro (frontline clinical teams) levels. Despite growing awareness of quality and patient safety risks, and significant effort to improve, progress is hard to measure (Goeschel et al., 2010).

In the Norwegian context the patient safety research and efforts related to organizing for patient safety in external and local governance systems is in its infancy. The aim of this paper is to describe the organization of the Norwegian system for patient safety and quality improvement.

The paper reports results from a pilot study of the Norwegian health care system (van de Bovenkamp et al., 2011). Data collection has been conducted through a triangulation of semi-structured interviews and document analysis. We have performed 20 interviews with informants representing organizations and institutions on macro, meso, and micro level.

Organizing for quality and safety in the Norwegian context strongly relies on state institutions and self-regulation as part of the external governance system. In the local governance system internal control is the main mechanism in organizing for quality and safety. At the macro level a national health plan and a national strategy for quality improvement has played a vital role in increasing attention to quality improvement at different system levels. At the meso and micro level effort is still needed to increase the status of the quality and patient safety initiatives. The informants at the meso and micro level argue for the importance of bottom-up approaches in the Norwegian context. Informants at the micro level rely on their professional international communities and argue for a higher trust in guides and guidelines developed by the professional communities compared to guides and guidelines established and distributed by Norwegian state organizations.

The specialized health care sector has been exposed to major structural changes such as hospital mergers and health care reforms the past years. Presently, changes in the legal framework are on public hearing. Several of the suggested changes are related to organizing for quality and patient safety such as the organizing of the error reporting system; the role of the regulator; and new legal requirements related to quality improvement and patient safety.

The effort to improve organization of quality and safety is increasing at different system levels in the Norwegian case. However the meso and micro level still lack resources resulting in improvement efforts prone to priority issues and lack of enthusiasm.

ACKNOWLEDGEMENTS

The study is part of the EU-project *Quality and Safety in European Union Hospitals. A research-based guide for implementing best practices and a framework for assessing performance* (QUASER). The authors wish to thank the European Commission for funding this research.

REFERENCES

Goeschel, C.A., Wachter, R.M. & Pronovost, P.J. (2010). Responsibility for Quality Improvement and Patient Safety. CHEST, Vol. 138, No. 1, pp. 171–179.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science*, Vol. 27, No. (2–3), pp. 183–213.

van de Bovenkamp, H., Quartz, J., Weggelaar-Jansen, A.M. & Bal, R. On behalf of the QUASER research team (2011). *Guiding quality work in European hospitals*. (Paper F).

Wiig, S. (2008). *Contributions to Risk Management in the Public Sector.* PhD Thesis UiS no. 48- February 2008. University of Stavanger.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Safety design of high consequence systems based on first principles

S. Li, J. Li, B. Suo & L.Y. Xiao
Institute of Electronic Engineering, CAEP, Sichuan, China

ABSTRACT

High Consequence Systems (HCSs) are those which would bring on some potential catastrophes when accidents occur. For example, nuclear weapons, manned spaceships, nuclear power stations fall into this category. It is crucial but extremely difficult to design assured and quantified safety consequence systems to avoid political storm, social instability or economic loss. Fortunately, lots of problems are solved by safety design approach based on first principles, which makes use of the fundamental characteristics inherent in the physics and/or chemistry of a material in order to provide a predictable response of a component when subjected to specific environmental stimuli. An example of a first principles design approach is the use of a material having a well-defined melting point in the design of a component that is required to fail safe if a certain undesired threshold temperature is exceeded. Rather than utilizing an active heat sensor in order to detect and then send a signal to some safing circuit, the material will instead inherently melt and fail safe. In this paper, the authors present their work on safety design of HCSs based on first principles about how to analyze system precondition and get the safety critical component. The detailed design approach of safety critical components, which utilizes the intrinsical physical/chemical characteristic of material to eliminate the hazard after identification, is proposed to guide the safety design of other HCSs. Then the most successful use of first principles technology, which induce the invention of ENDS (Enhanced Nuclear Detonation Safety) presented in Arming & Fuzing (A&F) system of nuclear weapons, is particularly specified in this paper about how to achieve its safety design goal. A&F system, the primary function of which is outputting detonating signal to detonator after receiving a series of arm command, must prevent from giving detonating signal by accident and unauthorized access under both abnormal and normal environments. The ENDS system contains four parts: Exclusion region, a barrier which is protected, or isolated from sources of electrical power; Strong link, a warhead component that precludes energy transfer to an exclusion region under normal and abnormal environmental conditions unless it receives a unique signal indicating intent to arm; Weak link, that becomes predictably and irreversibly inoperable at threshold environmental levels lower than those at which the associated strong links will remain operable and barriers will maintain integrity; Unique signal, a specific, nonchangeable sequence of bits of a pseudo-random nature. Safety design approach based first principles, which utilizes the above four parts together, improves system intrinsic safety effectively, reduces the cost of system used to assure safety in normal and abnormal environments, and also simplifies the evaluation of system safety. The safety design approach based on first principles introduced in this paper can be widely used in other similar one-off consequence systems.

REFERENCES

Authors unknown. *Narrative summaries of accidents involving US. Nuclear weapons, 1950~1980*.

Dvorack, M.A., Jones, T.R. et al. 1998. *System safety assessment combining first principles and model based safety assessment methodologies*. New Mexico: Albuqureque.

Ekman, M.E., Werner, P.W. et al. 1997. *A thematic approach to system safety.* New Mexico: Albuqureque.

MIL-HDBK-272A(OS). 1993. *Nuclear weapons systems, safety design and evaluation criteria for*.

Stanley, D. Spray & Cooper, J.A. 1995. *Passive safety concepts applied to critical functions*. New Mexico: Albuqureque.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The contribution of balanced scorecards to the management of occupational health and safety

F. Juglaret
Preventeo and Mines-ParisTech, Sophia-Antipolis, France

J.M. Rallo
Preventeo, Le Cannet, France

R. Textoris
L'Oreal, Aulnay sous bois, France

F. Guarnieri & E. Garbolino
Mines-ParisTech, Sophia-Antipolis, France

ABSTRACT

While it has been established for many years that the management of Occupational Safety and Health (OSH) is carried out by means of Management Systems, the question of how to measure the performance and the control of these systems is still current. This article addresses this problem, and discusses the contribution of the use of Balanced Scorecards.

Management Systems are the combination of many interacting processes, which are usually the result of standards implementation (OHSAS 18001, ILO, etc.). These processes are generally organized along the same lines; the logic being one of continuous improvement. Traditionally, performance indicators have been used to measure the performance of Management Systems: the frequency and severity of absences due to sickness, and work-related diseases. These traditional, retrospective indicators have several constraints and limitations. First, they are based on historical results and cannot be used to handle anomalous situations that have not arisen before. In addition, benchmarking is made difficult because the indicators, by their very nature, are heterogeneous.

If the primary purpose of a Management System is considered to be the reduction of absences due to sickness and work-related illness (in terms of severity and frequency), its functioning can be evaluated and assessed in detail, by looking at the constituent interacting processes.

Balanced Scorecards are a tool designed to fill some of the gaps identified when traditional OHS indicators are used. They bring together synthetic indicators. This enables both the measurement of the outcome of actions (lagging indicators), and also the correct functioning of internal sub-processes (leading indicators) (Figure 1).

This article is in three parts. The first part addresses the issue of the traditional indicators identified in the literature. Once defined, their contribution and limitations are discussed. Next,

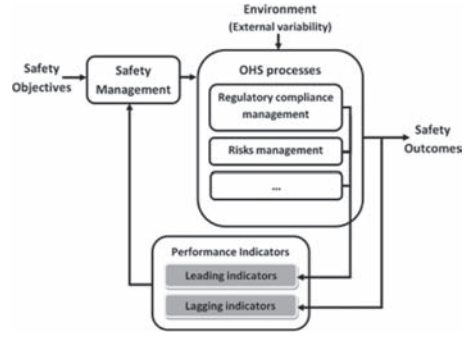


Figure 1. Regulatory and risk activities integrated into an OHS management model.

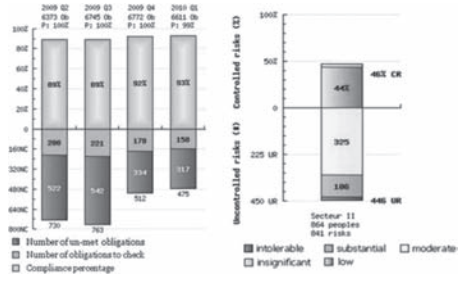


Figure 2. Regulatory compliance and risk control indicators.

the general concept of Balanced Scorecards is described, along with a survey of the work that has been carried out in the OHS domain. Finally, an example from the aeronautic and aerospace industry is used to illustrate the prospective Balanced Scorecards model. It integrates leading management indicators for two particularly interesting sub-processes of a Management System; namely, the supervision of regulatory compliance and risk management (Figure 2).

REFERENCES

Cambon, J. 2007. *Vers une nouvelle méthodologie de mesure de la performance des systèmes de management de la sante-sécurité au travail*. Doctoral Thesis. Mines ParisTech.

Hollnagel, E., Leveson, N. & Woods, D. 2006. *Resilience Engineering: Concepts and Precepts*.

Kaplan, R. & Norton, D. 1996-02. *The Balanced Scorecard - Measures that Drive Performance*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The impact of framework conditions on HSE in subcontracting/ outsourcing

K. Skarholt, U. Forseth, M. Hermundsgård & R. Rosness
SINTEF Technology and Society, Trondheim, Norway

ABSTRACT

The purpose of this paper is to investigate how various framework conditions affect issues related to Health Safety and Environment (HSE) in a contractor hierarchy within the Norwegian petroleum industry, both positively and negatively. By framework conditions for HSE work, we refer to conditions that influence the opportunities an organisation, organisational unit, group or individual has to ensure good HSE conditions (Rosness et al., 2009, Rosness et al., 2010). The term thus covers a broad range of conditions, such as market conditions (e.g., oil prices), terms of contract, physical layout of installations, management style and ideology.

In recent years it has become increasingly common to outsource tasks which were previously seen as core activities (Marchington et al., 2005). The petroleum industry was one of the first industries to make use of extensive outsourcing and is probably among the most specialized industries in the Norwegian economy. This sector is organised in contractor hierarchies, where operators buy services from several contractors which in turn hire subcontractors. In this setting, actors at one level (e.g., operators) may have a strong impact on the framework conditions facing other actors (e.g. contractors).

In this paper we investigate how HSE is negotiated between different actors in a contractor hierarchy. Using different power perspectives, we analyze two stories/examples identifying strategies and tactics employed by the actors involved in the contractor hierarchy, and how collaborations and networks are mobilized to improve HSE.

According to our interviewees, there has been a positive development towards more integration of personnel from contractors and subcontractors offshore. Operators and subcontractors alike consider it a goal to promote collaboration and shared understandings of safe operations. This analysis, however, has also illustrated that the different actors in a contractor hierarchy have different power bases, and they employ various power strategies and tactics in order to strengthen their arguments, resist action or formulate a new discourse in times of disagreement. Indeed, in the two examples/narratives that we analyzed, we found that almost all of our listed tactics were employed by either persons from the operator or the contractor. Thus, we can conclude that actors use all available resources in order to strengthen their viewpoints and increase their power base.

It seems, however, that it is easier to influence decisions and change outcomes for the operator company compared to contractors and sub-contractors. Furthermore, the analysis shows that non-human actors such as the safety barriers on board, the management system and a campaign for compliance to the management system, were enrolled and became important as framework conditions influencing the outcomes of the negotiation (or power struggles) regarding HSE challenges. Our analysis thus shed light on the functioning of the Norwegian regulatory regime, and the importance of formal power bases supported by law, a rich repertoire of power tactics in negotiations and how enrolling human and non-human actors can help increase one's powerbase.

REFERENCES

Marchington, M., Grimshaw, D. Rubery, J. & Willmott, H. (2005). *Fragmenting work – blurring organizational boundaries and disordering hierarchies*. Oxford: Oxford University Press.

Rosness, R., Blakstad, H.C. & Forseth, U. (2010): Exploring Power Perspectives on Robust Regulation. SINTEF report.

Rosness, R., Blakstad, H.C., Forseth, U., Wiig, S. & Dahle, I.B. (2010). *Environmental conditions for safety work - Theoretical foundations.* Working on Safety, Røros, 7.–10. September.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The impact of human and organisational factors on risk perception on Danish production platforms

H.B. Rasmussen
Centre of Maritime Health and Safety, University of Southern Denmark, Esbjerg, Denmark

ABSTRACT

The study explores the impact of human and organizational factors on subjective risk perception of personal injuries and process accidents on Danish production platforms. The present study applies models used in several studies conducted in the UK and Norwegian offshore industry (Fleming et al., 1998; Mearns et al., 2001; Rundmo, 1995; Rundmo, 1996). These studies have shown that organisational factors like priority of production versus safety and satisfaction with safety measures had an influence on risk perceptions among offshore employees in the UK and Norwegian sectors.

The definition of risk perception varies dependent on the research area and who is defining. There are two general ways of looking at risk perception: an objective and a subjective. The objective risk has been defined by experts as the probability of the unwanted dangerous event that can happen and its consequences (Rundmo, 1996). The subjective risk perception is the way the individuals perceive risk and behave in response to it (Fleming et al., 1998). The subjective risk perception is socially constructed and depends on the social context (Bye & Lamvik, 2007).

Danish data were collected through a questionnaire survey sent to all productions platform in the Danish sector in 2010. Principal component analysis (with Varimax rotation) was used to identify underlying dimensions. All dimensions were tested in both SPSS and in the LISREL program. LISREL analysis of structural relationships by the method of maximum likelihood was used. Statistical significance of the goodness of fit of the model was tested with Root Mean Square Error of Approximation (RMSEA), Comparative Fit Index (CFI) Goodness of Fit Index (GFI). The reliability of the scales was measured by Cronbach's Alpha.

The expectations to the results were that experience of accidents, less working experience and bad working conditions would have an impact on the risk perception of occupational hazards. The expectations were also that higher satisfaction with safety measurements and better safety culture would give lower risk perception of process incidents.

The study shows that more individual factors like behaviour, work experience and experience of injury have an influence on the risk perception of occupational hazards. Dimension safety versus production is a good predicate for risk perception of process incidents.

However, the study shows that the risk perception of offshore employees appears to be influenced by organisational factors such as satisfaction with safety (detection systems) and working condition for both kinds of risk perception.

REFERENCES

Bye, R. & Lamvik, G.M. 2007. Professional culture and risk perception: Coping with danger on board small fishing boats and offshore service vessels. *Reliability Engineering & System Safety*, *92*(12), 1756–1763.

Fleming, M., Flin, R., Mearns, K. & Gordon, R. 1998. Risk perceptions of offshore workers on UK oil and gas platforms. *Risk Analysis*, *18*(1), 103–110.

Mearns, K., Flin, R., Gordon, R. & Fleming, M. 2001. Human and organizational factors in offshore safety. *Work and Stress*, *15*(2), 144–160.

Rundmo, T. 1995. Perceived Risk, Safety Status, and Job Stress Among Injured and Noninjured Employees on Offshore Petroleum Installations. *Journal of Safety Research*, *26*(2), 87–97.

Rundmo, T. 1996. Associations between risk perception and safety. *Safety Science*, *24*(3), 197–209.

This page intentionally left blank

Quantitative risk assessment

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A BBN risk model of maintenance work on major process equipment on offshore petroleum installations

B.A. Gran, O.M. Nyheim & J. Seljelid
Safetec Nordic AS, Trondheim, Norway

J.E. Vinnem
University of Stavanger, Norway

ABSTRACT

Operational safety is receiving more and more attention in the Norwegian offshore industry. Almost 2/3 of all hydrocarbon leaks on offshore installations in the period 2001–2005 according to the Risk Level Project by Petroleum Safety Authority in Norway (Vinnem et al., 2006), resulted from manual operations and interventions, as well as shut-down and start-up, confirming what is considered common knowledge; that incidents and accidents often are caused by failure of operational barriers. Investigations of major accidents show that technical, human, operational, as well as organizational factors influence the leakages. In spite of these facts, quantitative risk analyses of offshore oil and gas production platforms have focused on technical safety systems.

The intention with the Risk OMT (Risk Modelling—Integration of Organisational, Human and Technical factors) program was to develop more representative models for calculation of leak frequencies as a function of the volume of manual operations and interventions. The Risk OMT program represents a further development of the work in the Barrier and Operational Risk Analysis (BORA, Vinnem et al., 2003) and Operational Condition Safety (OTS, Sklet et al., 2010) projects. The basic approach is the same, but the emphasis is on a more comprehensive modeling of Risk Influencing Factors (RIFs) and how these affect the performance of operational barriers. In the Risk OMT project a generic risk model has been developed and is adapted to use for specific failure scenarios (Nyheim et al., 2010; Vinnem et al., 2010). The model considers the operational barriers in event trees and fault trees, as well as RIFs that determine the basic event probabilities in the fault trees. The generic risk model applies Bayesian Belief Networks (BBNs) in its modeling. The model has been evaluated through case studies and has been applied to evaluate the effect of different proposed strategies to reduce the leakage rates (Gran et al., 2011).

This paper presents the BBN model step by step from two viewpoints: the data and expert judgment needed, and how the model uses the provided data and judgments. The procedure contains two main parts: step 1–4 representing the establishment of a model, and step 5–9 representing the application of the model.

Step 1: The scenarios
Step 2: Fault trees
Step 3: The basic events
Step 4: The RIFs
Step 5: Calculating a priori values
Step 6: Including observations
Step 7: Scoring of RIFs
Step 8: Proposing measures
Step 9: Calculate the effect of a measures

REFERENCES

Gran, B.A., Bye, R., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J., Sklet, S., Vatn, J. & Vinnem, J.E. 2011. Evaluation of the risk model of maintenance work on major process equipment on offshore petroleum installations. Submitted to *Reliability Engineering and System Safety*.

Nyheim, O.M., Gran, B.A., Pedersen, L.M., Seljelid, J., Vatn, J. & Vinnem, J.E. 2010. Use of Bayesian network for modeling Risk Influencing Factors. presented at *ESREL 2010*, Rhodos.

Sklet, S., Ringstad, A.J., Steen, S.A., Tronstad, L., Haugen, S., Seljelid, J., Kongsvik, T. & Wærø, I. 2010. Monitoring of Human and Organizational Factors Influencing Risk of Major Accidents. Presented at *SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production*, Rio de Janeiro.

Vinnem, J.E. et al. 2003. Risk assessment for offshore installations in the operational phase, presented at the *ESREL 2003*, Maastrict.

Vinnem, J.E., Aven, T., Husebø, T., Seljelid, J. & Tveit, O. 2006. Major hazard risk indicators for monitoring of trends in the Norwegian offshore petroleum sector. *Reliability Engineering & Systems Safety*, 91(7): 778–791.

Vinnem, J.E., Bye, R., Gran, B.A., Kongsvik, T., Laumann, K., Nyheim, O.M., Okstad, E.H., Seljelid, J. & Vatn, J. 2010. Risk modeling of maintenance work on major process equipment on offshore petroleum installations. Submitted to *Reliability Engineering and System Safety*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A methodology to quantitative ecological risk assessment for industrial accidents

O.H. Duarte & E.A. Droguett
Federal University of Pernambuco (UFPE), Recife, Pernambuco, Brazil

ABSTRACT

Recent industrial accidents such as toxic spills have caused catastrophic damage to the ecological environment and consequently great economic losses to the responsible company, as the British Petroleum painfully learned after the oil spill in the Gulf of Mexico, causing one of the most severe ecological disasters in history and a loss to the company estimated at U$37 billion to be spent with cleanup, fines, damages and repairs. However, this leak could have been avoided with the purchase of an equipment of U$500,000, able to seal the well in case of accident. The savings were therefore miscalculated under the risk-taking, which means that risk estimates were inaccurate. Such accidents as well as the high number of smaller accidents that happen every year has demanded an effective method to assess ecological risks. In fact, establishments with very hazardous installations or activities require quantitative values to the risks related to accidents with potential to cause human injury, ecological damage or economic loss, in order to objectively decide the necessary amount of resources to be invested in preventive measures, and this is the greatest contribution of Quantitative Risk Assessment (QRA). On the one hand, most studies in QRA for industrial accidents only consider risks to human health, disregarding the quantification of ecological risks. On the other hand, in the context of ecological QRA (i.e., QERA), although some methodologies have been able of quantifying ecological risks, they focus on risks caused by almost surely events (e.g., chronic pollution) of an industrial establishment, i.e., events that happen with probability one; because they do not include the event frequency in the composition of the risk, they are not capable of contemplating accidents, i.e., (rare) events with low probability of occurrence but that may cause catastrophic damage. Therefore, this work aims at proposing a methodology capable of quantifying ecological risks originating from rare events such as accidents. We use population modeling (Pastorok *et al.,* 2002) to simulate future changes in the population abundance of key species at risk and therefore estimate the probability of extinction or decline, time to extinction and other measures, for each accidental scenario. Thus, it was possible to develop an approach that links the ecological damage (predicted via ecological modeling) with the frequency of occurrence of the accidental scenario (estimated via historical data and reliability analysis). Similar to the societal risk in a human quantitative risk assessment (CPR18E 2005), the result is a FN risk curve, where N is the average population decline number and F the cumulative frequency of accidents with N or greater abundance decline. The Figure 1 shows an example.

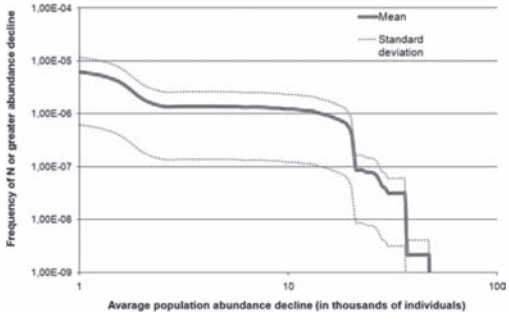


Figure 1. FN curve for representation of the accidents' ecological risks in an establishment.

REFERENCES

Akçakaya, H.R. *et al.* 1999. *Applied Population Ecology*. Sunderland, Massachussets: Sinauer Associates.

CPR18E 2005. *Guideline for quantitative risk assessment (the "Purple book")*.

Pastorok, R.A. *et al.* 2002. *Ecological modeling in risk assessment: chemical effects on populations, ecosystems and landscapes*. CRC Press LLC.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A predicting method of system safety risk state transition time based on Markov process

H.T. Li, X.M. Liu, J.L. Zhou & G. Jin
System Engineering Department, College of Information System and Management, National University of Defense Technology, PR China

ABSTRACT

Safety risk which can be described by the probability and severity level of consequence is an important measure of system safety. Nowadays, most of the classical methods used to evaluate the safety risk are probability safety assessment methods, which rely on the system safety model including event tree and fault tree to assess the probability and severity level of various consequences based on the analysis of the reliability of component. Marseguerra gives a Monte Carlo approach to PSA for dynamic process systems (Marseguerra, M. et al., 1996). Aneziris presents a method for evaluating the probability of catastrophic failures in process systems (Aneziris, O.N. et al., 2004.) and another for calculating the dynamic reliability of safety systems and its application to a refrigerated liquid cryogenic ammonia storage tank (Aneziris, O.N. et al., 2000). Dynamic safety assessment: Scenario identification via a probability clustering approach is researched by Podofillini (Podofillini, L. et al., 2010). Zhu gives a framework to integrate software behavior into dynamic probabilistic risk assessment (Zhu, D.F. et al., 2007). To ensure the safety of a process system, Kalantarnia puts up Dynamic risk assessment using failure assessment and Bayesian theory (Kalantarnia, M. et al., 2009). Probability risk assessment methods listed above are only some typical examples, and the similar methods are so many that we cannot enumerate all.

These methods are very effective for the safety assessment of certain system and have solved a lot of safety assessment problems including static system and dynamic system. However, they also have some limitations. In these classical methods, the safety risk is only represented by probability and no system state evolving process of the safety is presented. So, it can't clearly describe the safety using the method of dynamic evolvement of the system state. Actually, most catastrophic accidents of complex system occur as a result of a series evolvement of system states over a time interval after the abnormal event has happened. Therefore, a problem that how do we model the evolving process of the accident through the system state evolvement and how do we predict the evolving time between various safety risk states of the system is put up. To cope with these issues, a method to describe the dynamic evolvement of safety risk and predict the transition time of safety risk state is presented.

It is very important to prevent the occurrence of accident through predicting the transition time of system's safety risk state. Given the definition of system safety risk state, the method applied in this paper can simulate dynamic phenomena of safety through the evolvement of system state. It is based on the markov method which is a classical method to model the dynamic process. And then, the transition time of safety risk state is calculated based on the simulation outcomes. Various systems have their requirement on the transition time in order to ensure the safety. Therefore, whether the system safety is appropriate can be got according to the requirement. To evaluate the confidence of the prediction of the transition time of safety risk state, the paper introduces a bootstrap method. At last, an ethyl benzene process is taken as an example To demonstrate the predicting method of safety risk state transition time.

REFERENCES

Aneziris, O.N. & Papazoglou, I.A. 2004. Fast Markovian method for dynamic safety analysis of process plants. *Journal of Loss Prevention in the Process Industries* 17: 1–8.

Aneziris, O.N., Papazoglou, I.A. & Lygerou, V. 2000. Dynamic safety analysis of process systems with an application to a cryogenic ammonia storage tank. *Journal of Loss Prevention in the Process Industries* 13: 153–165.

Bucci, P., Kirschenbaum, J., Mangan, L.A. (et al.). 2008. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. *Reliability Engineering and System Safety* 93: 1616–1627.

Kalantarnia, M., Khan, F. & Hawboldt, K. 2009. Dynamic risk assessment using failure assessment and Bayesian theory. *Journal of Loss Prevention in the Process Industries* 22: 600–606.

Marseguerra, M. & Zio, E. 1996. Monte Carlo approach to PSA for dynamic process systems. *Reliability Engineering and System Safety* 52: 227–241.

Zhu, D.F., Mosleh, A. & Smidts, C. 2007. A framework to integrate software behavior into dynamic probabilistic risk assessment. *Reliability Engineering and System Safety* 92: 1733–1755.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A research on simulation methods for system risk assessment

X.M. Liu, H.T. Li, J.L. Zhou & P.C. Luo
College of Information System and Management, National University of Defense Technology, Changsha, China

ABSTRACT

In the areas of system safety, it is difficult but important to perform safety risk assessment. The accurate assessment is significant to risk management and control. Many of researches have promoted the safety risk assessment. Nevertheless, few papers are devoted to simulation methods of system risk assessment. The aim of this work is just to make researches on the simulation methods.

Safety risk is a characteristic for measuring safety level, which is the combination of the probability of occurrence of accident and the severity of that accident. Risk can be divided into low-medium-high risk sets. Suppose that system state risk is the risk when the system in the state $X(t)$, denotes $R(X(t))$. And we can partition the system state space into low risk state set E_{LR}, medium risk state set E_{MR} and high risk state set E_{HR}. It's known that the probability of system state $X(t)$ at time t belonging to E_{LR}, E_{MR} and E_{HR} is $P_1(t)$, $P_2(t)$, $P_3(t)$ respectively.

The simulation methods for safety risk assessment based on system initial perfect state can be carried out as follows:

Step 1 Determine the time t for risk analysis;

Step 2 Calculate the probability of picking state from state sets for the component i at time t, and sample a state $x_i(t)$ randomly with the probability. Sequentially, the system state $X_1(t)$ can be obtained by sampling of all the components;

Step 3 Repeat step 2 by N times, and get N system states $X_1(t)$, $X_2(t)$, … , $X_N(t)$ at time t;

Step 4 Classify these N system states by risk as E_{LR}, E_{MR}, E_{HR}, then compute $P_1(t)$, $P_2(t)$, $P_3(t)$.

Let the time t increases gradually from zero, the system safety risk in the future period beginning from initial perfect state can be gained.

The simulation methods based on system current state are similar to above steps, but we must get failure rate $\lambda(t)$ firstly.

According to the proposed methods, the risk change from system initial and current states (including known runtime and unknown runtime) can be obtained. To demonstrate the performance gains of our model, a chemical reactor involving urgency-cooling system is analyzed as an example. The results show that the methods can assess the system risk state in the future time effectively. Furthermore, the conclusion can be used to guide the risk control and improve system safety.

REFERENCES

Charvet, C. et al. 2010. Learning from the application of nuclear probabilistic safety assessment to the chemical industry, *Journal of Loss Prevention in the Process Industries*.

Goble, W.M. 1998. *Control Systems Safety Evaluation & Reliability* (second ed.): ISA.

Ibáñez-Llano, C. et al. 2010. A reduction approach to improve the quantification of linked fault trees through binary decision diagrams. *Reliability Engineering and System Safety*, 95, 1314–1323.

Jung, W.S. 2009. ZBDD algorithm features for an efficient Probabilistic Safety Assessment. *Nuclear Engineering and Design* 239, 2085–2092.

Kančev, D. et al. 2011. Optimization of test interval for ageing equipment:A multi-objective genetic algorithm approach, *Journal of Loss Prevention in the Process Industries*.

Kang, D.I. et al. 2011. Estimation of common cause failure parameters for essential service water system pump using the CAFE-PSA. *Progress in Nuclear Energy*, 53, 24–31.

Kim, M.C. & Seong, P.H. 2006. A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. *Reliability Engineering and System Safety*, 91, 580–593.

Kritzinger, D. 2006. *Aircraft system safety*. Cambridge: Woodhead Publishing Limited.

Rao, K.D. et al. 2009. Dynamic fault tree analysis using Monte Carlo simulation in probabilistic safety assessment. *Reliability Engineering and System Safety*, 94, 872–883.

Veeramany, A. & Pandey, M.D. 2011. Reliability analysis of nuclear component cooling water system using semi-Markov process model, *Nuclear Engineering and Design*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Assessment of common cause failures and defensive measures for the representation of I&C in probabilistic models

G. Deleuze, N. Thuy, R. Quatrain & F. Jouanet
EDF R&D, France

ABSTRACT

Digital equipment and systems have an important role in the operation and control of Nuclear Power Plants (NPP) and their main components. Digital equipment and systems may have beneficial effects, for example due to advanced capabilities or improved hardware reliability. They may also have detrimental effects. In particular, although digital equipment is usually more reliable than analog equipment it replaces, its use raises specific technical and modeling issues, especially on digital Common Cause Failures (CCF) due to design or software faults.

As many products are available, and many architectures are possible for a given project, it is important for designers to be able to assess without excessive conservatism the impacts of the proposed solutions on plant safety, in new builds or through upgrades. Even if software related failures are systematic, it is important to note that many systematic failures are non-software related. A recent analysis (EPRI, 2008) has highlighted the dominance of non-software failure mechanisms such as pre-accidental human factors. For example, human errors due to difficulty in the analysis of complicated logic, whatever the I&C technology (relays, FPGA, microprocessor), may be significant.

This article presents an approach to improve the representation of digital I&C, while keeping the models simple and usable in probabilistic models of an installation, the so called SPINOSA approach. It relies on the combined use of a particular representation of I&C effects, the "Compact Model", and a sensitivity analysis based on "Beta Factors" representing potential dependencies due to hardware, software, human actions or interactions. It considers random mechanisms and systematic mechanisms, assessed by a combination of probabilistic and deterministic approaches. The framework used to assess the systematic failures due to hardware, software and human actions is partly presented here, i.e. the taxonomy of software related failure mechanisms and associated defence measures necessary to assess associated factors. The taxonomy is based on a general system failure model and an identification of faults, effects, activating events, common cause contexts. We expect from this framework an analytical approach representing a significant improvement compared to holistic assessment approaches such as IEC 61508 and its declinations. It will also be the starting point of effective FMEA dedicated to digital systems.

After the description of the practice of I&C modelling for probabilistic safety assessment of nuclear installations within EDF, we present the limitations of state of the art standards like IEC 61508 to assess with a sufficient relevance and accuracy the CCF risks in large protection systems. We presented in chapter 3 the SPINOSA approach, a concept method currently being experimented with within EDF R&D, to improve the representation of I&C effects in probabilistic safety assessments, that addresses in particular such limitations on CCF risk assessment. After a brief general presentation, we detailed in chapter 3 the assessment of common cause failures and defensive measures for the representation of I&C in probabilistic models. We expect from such an analytical approach, based on system failure models, fault and context taxonomies, a significant improvement compared to holistic assessment approaches such as IEC 61508 and its declinations. It will also be the starting point for effective FMEAs dedicated to digital systems.

REFERENCES

Deleuze, G., Thuy, N., Quatrain, R. & Jouanet, F. 2010. Experimentation of sensitivity study based on Beta Factors to assess the impact of I&C in PSA. PSAM 2010, Seattle, June 2010.

EPRI, 1996. TR-106439 – Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, October 1996.

EPRI, 2003. TR-1007997 - Guideline for performing Defense in Depth and diversity assessments for digital I&C upgrades, December 2003.

EPRI, 2008. Report 1016731. Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems". Draft, November 4, 2008.

NUREG, 2009. NUREG/CR-7007 ORNL/TM-2009/302, "Diversity Strategies for Nuclear Power Plants and Instrumentation and Control Systems".

Thuy, N. 2010. EPRI Report Estimating Failure Rates in Highly Reliable Digital Systems, Draft November 2010.

Thuy, N. & Deleuze, G. 2009. A Mixed Approach to Assess the Impact of I&C in PSA. Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC &HMIT 2009, Knoxville, Tennessee.

Torok, R. & Thuy, N. 2010. EPRI Report 1019182 Protecting Against Digital Common-Cause Failure - Combining Defensive Measures and Diversity Attributes, December 2010.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Combining FMECA and fault trees for declining safety requirements of complex systems

R. Guillerm & H. Demmou
CNRS; LAAS—University of Toulouse, Toulouse, France

N. Sadou
SUPELEC / IETR, Cesson-Sevigne, France

ABSTRACT

Modern systems are increasingly complex. Indeed, they integrate more and more different technologies, offering more functions, but with a complex components in interaction. The process and the design methods must evolve to reflect this growing complexity. In particular, for our purposes, the dealing with properties such as security and reliability must evolve accordingly, to ensure and enable the necessary level of confidence. For an effective consideration of safety in the design process, it is necessary to consider safety in overall studies by the engineering system process. For this purpose it is necessary to define safety system (global) requirements and then to decline then into sub-systems requirements. Indeed, safety is defined as a non functional requirement and is related to emergent system properties. These non-functional properties cannot be attributed to single system components, they emerge as a result of integrating system components. So safety requirements must be formulated in the large (system level) and then declined in the small (sub-system level).

REFERENCES

Avizienis, A., Laprie, J.-C., Randell, B. & Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, vol. 1, pp. 11–33, 2004.

Buzzatto, J.L. Failure mode, effects and criticality analysis (FMECA) use in the Federal Aviation Administration (FAA) reusable launch vehicle (RLV) licensing process. Digital Avionics Systems Conference, 1999. Proceedings 18th. vol. 2 10/24-29/1999. Location: St Louis, MO, USA.

CEI 60812: Techniques d'analyse de la fiabilité des systèmes, 1995.

Chavalarias, D., Bourgine, P., Perrier, E., Amblard, F., Arlabosse, F., Auger, P., Baillon, J.-B., Barreteau, O., Baudot, P. & Bouchaud, E. et al, French Roadmap for complex Systems 2008–2009, French National Network for Complex Systems (RNSC), Paris Ile-de-France Complex Systems Institute (ISC-PIF) and IXXI, "Entretiens de Cargèse 2008", 2008.

ED-79/ARP 4754: Certification considerations for Highly-Integrated or Complex Aircrafts Systems, SAE 1996–11, 1996.

EIA-632: *Processes for engineering systems*, Electronic Industries Alliance standard, January 7, 1999.

Goguen, J. & Linde, C. Techniques for requirements elicitation. In 1st IEEE International Symposium on Requirements Engineering, pages 152–164, San Diego, 4–6th January 1993.

Gotel. O.C.Z. & Finkelstein, C.W. "An analysis of the requirements traceability problem," in International Conference on Requirements Engineering, 1994, pp. 94–101.

Guillerm, R., Demmou, H. & Sadou, N. System engineering approach for safety management of complex systems. Proceedings of European Modeling and simulation (ESM'2009). October 26–28, 2009, Leicester, United Kingdom.

Juristo, N., Moreno, A.M. & Silva, A. "Is the European Industry Moving Toward Solving Requirements Engineering Problems?" IEEE Software, vol. 19, no. 6, pp. 70–77, 2002.

Komi-Sirvio, S. & Tihinen, M. "Great Challenges and Opportunities of Distributed Software Development – An Industrial Survey." in Proceedings of the Fifteenth International Conference on Software Engineering & Knowledge Engineering (SEKE'2003), 2003, pp. 489–496.

Rasmussen, J. Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, vol. 27, No. 2/3, Elsevier Science Ltd., 1997, pp. 183213.

Sahraoui, A.-E.-K. "Requirements Traceability Issues: Generic Model, Methodology and Formal Basis." International Journal of Information Technology and Decision Making, vol. 4, no. 1, pp. 59–80, 2005.

Sahraoui, A.-E.-K., Buede, D. & Sage, A. "issues in systems engineering research," INCOSE congress, Toulouse, 2004.

Sommerville, I. Software Engineering: (Update) (8th Edition) (International Computer Science). Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2006.

Lee, W.S., Grosh, D.L., Tillman, F.A. & Lie, C.H. "Fault tree analysis, methods, and applications - A review", IEEE Transactions on Reliability, August 1, 1985; ISSN 0018-9529; r-34, page 194–203.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Discussion of a mathematical model to simulate a fire ball from gaseous explosion (BLEVE)

A.N. Haddad
Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

E.B.F. Galante
Exército Brasileiro, Brazil

ABSTRACT

This work presents (mathematically) the phenomenon of explosion of a cylinder of LPG—Liquefied Petroleum Gas, mixing with air and the subsequent fireball.

Currently, the mathematical tools used to model this kind of events relies upon the equations of state. Furthermore, it relies upon the Navier-Stokes equations to model the flow, the energy equation for the temperature. Usually this kind of models are calculated by the use of finite elements technique, having the continuity equation (density variation equal to zero) as convergence criteria.

Using a computational platform some algorithms can be implemented to calculate expected the effects a Bleve (having gas as fuel). These algorithims used different hypothesis, wich allowed comparison. Among the hypothesis list, it ought to be enumerated:

- Absence of external influences on the flow (wind and topography)
- Linear correlation between enthalpy and specific heat source for the term of the energy equation
- Incompressible Fluid
- The cylinder of LPG will be reduced to a point

The importance of this work is justified by the need to quantify the risk of such event by the used of computational tools that can be simple, fast and accurate. These three qualities are a trade-off. Increase one imposed a loss on another. Even more, the tools a designer has to deal to chance these qualities are the hypothesis used at implementation stage, The same hypothesis discussed on this work.

REFERENCES

Akhavan, J. The Chemistry of Explosives - 2nd Edition. Royal Military College of Science, Swindow.

Castellan, G. Fisicoquimica. Edited by Pearson Prentice Hall. 1987. ISBN 9684443161.

Crippa, C., Fiorentini, L., Rossini, V., Stefanelli, R., Tafaro, S. & Marchi, M. 2009. Fire risk management system for safe operation of large atmospheric storage tanks. Web of science. Journal of Loss Prevention in the Process Industries.

Ellis, T.M., Philips, R., Ivor, Lahey, R. & Thomas, M. 2004. Programming Fortran 90. England. Addison-Wesley (ISBN 0-201-54446 6).

Emilio Chuvieco, Inmaculada Aguado, Marta Yebra, Héctor Nieto, Javier Salas, M. Pilar Martín, Lara Vilar, Javier Martínez, Susana Martín, Paloma Ibarra, Juan de la Riva, Jaime Baeza, Francisco Rodríguez, Juan R. Molina, Miguel A. Herrera & Ricardo Zamora. 2009. Development of a framework for fire risk assessment using remote sensing and geographic information system technologies. Web of science.

Fogler, H.S. Elements of Chemical Reaction Engineering. Prentice-Hall International Series in the Physical and Chemical Engineering Sciences. IBSN 0-13-53708-8.

Kuo & Kenneth Kuan-Yun. Principles of Combustion, Singapore, John Wiley and Son Publishers. 1986. ISBN 85-22627.

Meyer, R. Explosives. Gebr. Diesbach. Germany. 1977.

Pula, R., Khan, F.I., Veitch, B. & Amyotte, P.R. 2008. A Grid Based Approach for Fire and Explosion Consequence Analysis. Web of science.

SFPE Handbook of Fire Protection Engineering. National Fire Protection Association, - 3rd Edition. Quincy, Massachusetts. 2002. ISBN 087765-451-4.

Tannehill, John, C., Anderson, Dale, A. e Pletcher & Richard, H., 2nd Edition. Computational Fluid Mechanics and Heat Transfer, USA. Taylor & Francis Publisher. (ISBN 1-56032-046-X).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Enabling quantitative risk assessment of the real world transport system

M. Kowalski & J. Magott
Wrocław University of Technology, Wybrzeże Wyspiańskiego, Wrocław, Poland

ABSTRACT

Fault Trees do not have great power of expressing the real systems. Factors that increased applicability of Fault Trees were the following papers: (Dugan et al., 1992), where dynamic fault trees have been introduced and (Bobbio & Codetta 2004), where repair boxes have been defined. However, descriptive power of the above extensions when such time dependencies like a sequence of time consuming activities or time redundancy have to be expressed is strictly limited.

These extensions failed when challenged with timing dependencies of a tram-based public transport system (Werbińska-Wojciechowska, S. 2008). In this system a failed tram is replaced in some time by a spare one. When the failed tram is repaired and delivered, it is put into action releasing the spare one. However, the failed tram has to be either replaced or delivered after repair within a time resource. If not, an undesirable event called hazard starts occurring.

Although we finally managed to express the tram system using a stochastic Petri net (Kowalski et al., 2011), the model was deemed obscure by domain experts. Hence, driven by the necessity to increase modeling power of fault trees and their applicability we blend them with Petri nets, thereby coming up with Fault Graphs with Time Dependencies (FGTDs) (Kowalski & Magott 2011), which are capable of expressing not only the system in question, but also a number of formerly devised fault tree extensions. In (Kowalski & Magott 2011), three repair policies applied to computer system failure/repair process have been analyzed. FGTDs contain probabilistic fault tree with time dependencies (Babczyński et al., 2010) based elements and Petri net based elements. In the research we strive to retain the genuine intuitiveness of fault trees, which is the main reason for their popularity and acceptance among safety engineers.

The hazard probability of the tram system and simulation time metrics are examined using a dedicated simulator. The values are computed depending on a number of redundant trams. Additionally, analytical estimations of these values are found and their accuracy is verified. Finally, we come up with following hazard probability evaluation techniques:

- Optimistic bound
- Pessimistic bound
- Queuing model estimation
- Queuing model with repair estimation
- Simulation (Fig. 1)

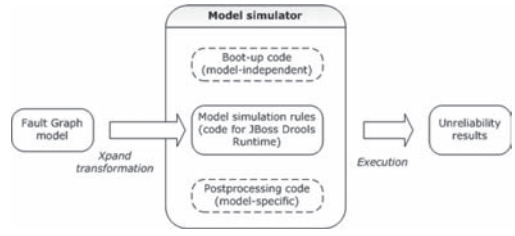


Figure 1. The simulator's architecture.

REFERENCES

Babczyński, T., Łukowicz, M. & Magott, J. 2010. Time coordination of distance protections using probabilistic fault trees with time dependencies. *IEEE Transaction on Power Delivery*, July, Vol. 25, No. 3, 1402–1409.

Bobbio, A. & Codetta, D. 2004. Parametric fault trees with dynamic gates and repair boxes. In *Proc. Annual Symposium on Reliability and Maintainability:* 459–465.

Dugan, J.B., Bavuso, S.J. & Boyd, M.A. 1992. Dynamic fault-tree models for fault-tolerant computer systems. *IEEE Trans. Reliab*., Vol. 41, No. 3, 363–367.

Kowalski, M. & Magott, J. 2011. Conjoining fault trees with Petri nets to model repair policies, accepted for publication in *Advances in Artificial Intelligence and Soft Computing*, Springer.

Kowalski, M., Magott, J., Nowakowski, T. & Werbińska-Wojciechowska, S. 2011. Analysis of transportation system with the use of Petri nets. *Eksploatacja i Niezawodność, Maintenance and Reliability*, No. 1, 117–128.

Werbińska-Wojciechowska, S. 2008. Model of logistic support for exploitation system of means of transport. *PhD. Thesis, Wroclaw University of Technology*, Poland, report: PRE. 3/2008.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fault tree analysis of substations

M. Čepin
Faculty of Electrical Engineering, Ljubljana, Slovenia

ABSTRACT

Substation reliability is defined as the inability of the substation to support the delivery of electrical power supply to any of its related loads.

The objective of this paper is to investigate the ways how to assess reliability of substations in order to avoid complex dynamic methods and at the same time include in the analysis the features of different system configurations and conditions.

The goal is to develop a method, which would enable preparation of substation models, which are useful for their integration into the models of power system reliability. The integration of substation models and model of the power system is important for realistic assessment of power systems.

The method consists of the following steps:

- definition of the conditions of the systems under investigation,
- the model of the substation structure,
- transformation of the model of substation structure into the model, which is suitable for the fault tree analysis,
- the fault tree analysis,
- the interpretation of the results and direction of possible improvements.

Different conditions can represent the system in a different configuration or in different operating conditions. Each set of conditions related to specific configuration or operating conditions can in theory require changed models in the other steps of the method. The model of substation structure is defined with the help of the matrix of connections. Substation structure is transformed into the model, which is suitable for the fault tree analysis. The results of the fault tree analysis give system reliability. Several fault trees are developed for one system.

The method upgrades the static reliability calculation of the systems by introduction of several configurations and conditions of the system, which are evaluated separately under different sets of conditions.

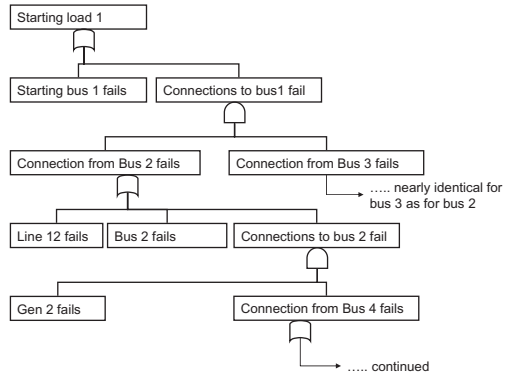


Figure 1. Example fault tree.

Those different sets of conditions cause consideration of different failure probabilities of components of the systems. Different input data may change the results significantly and the weighted average of sets of conditions gives a better representation of system reliability in reality.

REFERENCES

Čepin, M. 2010. Application of Common Cause Analysis for Assessment of Reliability of Power Systems, PMAPS2010, Singapore, IEEE Proceedings.

Čepin, M. 2010. Assessment of switchyard reliability with the fault tree analysis, PSAM2010, Seattle.

Čepin, M. & Mavko, B. 2002. A Dynamic Fault Tree, Reliability Engineering and System Safety, Vol. 75, No. 1, pp. 83–91.

IEEE-Std-500. 1983. IEEE guide to the collection and presentation of electrical, electronic, sensing component and mechanical equipment reliability data for nuclear power generating stations, IEEE, New York.

Volkanovski, A., Čepin, M. & Mavko, B. 2009. Application of the fault tree analysis for assessment of power system reliability, Reliability Engineering & System Safety, Vol. 94 (6), pp. 1116–1127.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Formalization of a quantitative risk analysis methodology for static explosive events

R.G. Salhab, I. Häring & F.K.F. Radtke
Fraunhofer Ernst-Mach-Institute (EMI), Efringen-Kirchen, Germany

ABSTRACT

The paper presents the methodology of a quantitative risk analysis implemented in an interactive 3D expert software-tool for high explosive events of static sources, e.g. terrorist bombing threats in urban environments, which is being developed since more than 10 years (Dörr & Gürke 2006). The methodology is described in a formal way covering the following steps: analysis of scenario, hazard, damage, event frequency, exposure and finally risk assessment.

For each step we give the input and output, the engineering and physical models as well as the algorithms. The effects of fragment and blast are considered. We show that the formalization describes the methodology in a short and concise way and discuss possible generalizations and further improvements of the methodology and the formalization.

Risk assessment tools have been developed, amongst others, in the US (SAFER (Tatom 2008)) or the Netherlands (Dongen 2000). A formalization of a quantitative risk analysis for fragments of high-explosive shells in air has been presented in (Häring & Schönherr 2009).

The presented risk analysis follows the scheme illustrated in Figure 1. In the scenario analysis step the geographical conditions, properties of hazard sources, exposed sites and counter measures are defined by the user. Implicitly standard conditions for the atmospheric conditions are assumed. Physical consequences of the detonation are computed in the hazard analysis step, like specific impulse and peak overpressure of the blast and fragment densities on the ground. The exposure of the personnel is defined by the user. The event frequency is predefined in a probability of event table that has been adapted to German conditions. In the damage analysis step the damage due to fragments, blast and a combination of both are calculated using probit distributions and probabilistic considerations. In the final risk analysis step individual, local and group risk are specified.

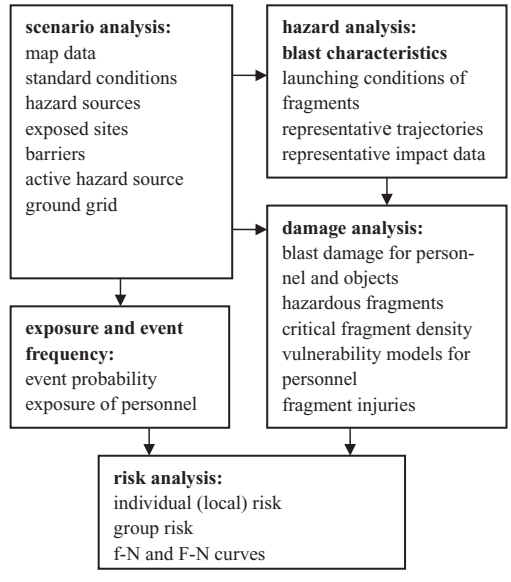


Figure 1. Scheme of the analysis steps.

With the help of the calculated individual local risk, finally formulas for f-N and F-N curves are extracted which can be compared with acceptance criteria of different countries.

REFERENCES

Dongen, P. v. 2000. RISK-NL. *29th DoD Explosives Safety Seminar*, New Orleans, Louisiana.

Dörr, A., Gürke, G. & Ruebarsch, D. 2006. The German Explosive Safety Code ESQRA-GE. *32nd DoD Explosives Safety Seminar*, Philadelphia, Pa., USA.

Häring, I., Schönherr, M. & Richter, C. 2009. "Quantitative hazard and risk analysis for fragments of high-explosive shells in air." *Reliability Engineering and System Safety*.

Tatom, J.W. 2008. The Science of Safer 3.03. *33rd DoD Explosives Safety Seminar*, Palm Springs, California.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

High-pressure pipeline break risk assessment

T. Saska, J. Novak & F. Kratochvil
Technical University of Liberec, Liberec, Czech Republic

R. Sousek
University of Pardubice, Pardubice, Czech Republic

ABSTRACT

The risk quantification represents complex multidisciplinary problem, requiring pipeline disturbance probability evaluation, escaping gas quantity assessment, physical effects of caused fire or explosion under different technical and meteorological conditions, individual risk evaluation and vulnerability assessment of exposed people or objects.

This work represents trying to criteria formulation for development licence with the usage of individual and social risk assessment. It is affected by estimation uncertainty of probability of major pipeline break. In the worldwide scale it is concerned about unique cases, so it is not possible to consider available statistic data as adequately reliable for accident frequency determination.

The physical effect calculations are more accurate. Here the uncertainties arise from large number of available conditions, from which it is possible to take into account only limited number. It is necessary to notify, that the reach of negative effects (in case of major accident, such as e.g. pipeline total rupture) may affect to the distance which several fold exceeds the bandwidth.

Vulnerability assessment of objects and people results both from methodics recommended by Ministry of the Environment of the Czech Republic and from recherche to principles of landscape planning and to risk acceptability in foreign countries. The social risk calculation is not aimed at concrete existing objects, but at typical objects category, which are under consideration in the term of acceptability assessment of their localization inside safety zone.

Risk is defined as a product of unwanted event rise probability and its consequences. The event probability is contingent both on equipment technical parameters (gas pressure, pipeline diameter, material, number of components), their reliability and random outside effects resistance. The consequences may be related to detriment of people health and lives, also economic losses and environmental damages. We know two different risk types:

– individual,
– social.

Individual risk represents probability of specific quantified consequence for person or object which inheres in given location against potential risk source (eventually more risk sources). Individual risk for one person in specific place near the accident source (e.g. individual fatality, individual risk of injury) depends not on population density round about the source, generally not even on the fact, whether in the area some people are. Similarly the individual risk for object is possible to determine no matter if some object is situated in the given point. Individual risk value sinks with the distance from the accident source. According to its area distribution it is possible to specify areas of enhanced risk.

Social risk is relevant to the number of threatened people, to the number, value and significance of objects, eventually also to the quality of threatened environment. So, it depends on population density (also on its distribution in area and time) and on concrete objects existence in threatened area. Social risk is defined as a product of number of threatened people or value of affected resources and relevant individual risk. That is why the social risk value may be (and often is) higher in farther points from the accident source, than in near points. According its level the risk acceptability for industry objects is evaluated.

The continuous economic growth, country industrialization and the development area expanding is connected with finding an acceptable balance between risk from energetic infrastructure and its need for every people because of power supply. In our case we will concern with VTL pipelines. Present legislature in the Czech Republic and the technical regulations and rules solve these problems. We have to claim, that the concrete conditions specification is different in most of European countries. We could say that it is less strict and simpler than in the Czech Republic. For finding acceptable level for above mentioned balance we can successfully use risk assessment methods.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Integrated risk assessment for LNG terminals

O.N. Aneziris, I.A. Papazoglou & Myrto Konstantinidou
National Centre for Scientific Research "DEMOKRITOS", Terma Patriarchou Grigoriou, Aghia Paraskevi, Greece

ABSTRACT

This paper presents the methodological and procedural steps for quantified risk assessment of LNG and its application to two LNG terminals an onshore and an offshore. The onshore consists of two storage tanks with total capacity 100000 m^3 and the offshore of four double containment spherical tanks, each with capacity 34672 m^3. This analysis was performed in the framework of the iNTeg-RISK project, coordinated by Jovanovic (2010).

Over the last years risk assessment methodology has been widely used for estimating risk of chemical plants storing flammable and toxic substances, such as ammonia, LPG and fuels, by Papazoglou et al. (1992) and Taveau (2010). Nevertheless quantified risk assessment of LNG installations appears in few cases in the literature.

Extensive research has been performed in the area of consequence analysis. The behaviour of LNG has been extensively studied if released in the atmosphere, on ground or on water. Results of experiments and modelling concerning LNG outflow, dispersion, pool fires and vapour explosions have been presented by Cleaver et al. (2007), Hanlin (2006) and the Sandia report (2004) presents methods of LNG spills on water.

The basic steps for risk assessment followed in both cases are the following: a) Hazard Identification, where the main sources of LNG release are identified and the initiating events that can cause accidents are determined b) Accident Sequence Modeling, where logic models for the installations are developed. c) Data Acquisition and Parameter Estimation; parameters which were estimated with generic values include the frequencies of the initiating events, component unavailability and probabilities of human actions. d) Accident Sequence Quantification; the frequency of occurrence of all accident sequences identified in the second step is assessed by using the laws of Boolean algebra and required data e) Consequence Assessment; calculation of release and evaporation rate, radiation levels and overpressure owing to immediate or delayed ignition of LNG is performed f) Integration of Results; integration of models and associated results developed in steps a) to e) results in estimation of individual risk as a function of distance from the installation, for both LNG terminals.

Twenty one event trees have been developed and quantified for twenty one initiating events identified for both LNG plants, contributing to the risk of twelve plant damage states, such as tank rupture owing to overpressure, overfilling, underpressure and pipe rupture in loading, unloading and outlet sections. For the on shore plant, total individual risk is equal to 10^{-5}, 10^{-6}, 10^{-7}, 10^{-8}/yr at distance of 50, 100, 600, 820 meters from the centre of the plant respectively, while for the off shore plant the same values of total individual risk are encountered at distances of 80, 560, 790, 1000 meters from the centre of the plant respectively, under the assumptions and uncertainties of each terminal. These results are valuable for land use planning around the LNG terminal sites.

REFERENCES

Cleaver P., Johnson M., & Ho, B. 2007. A summary of some experimental data on LNG safety, *Journal of Hazardous Materials*, 140, 3, 429–438.

Hanlin, A.L. 2006. A review of large-scale LNG spills: Experiments and modeling, *Journal of Hazardous Materials*, 132, 2–3, 119–140.

Jovanovic, A. 2010. iNTeg-Risk Project: Concept and first results, *Proceedings of the 2nd iNTeg-Risk Conference: New Technologies and Emerging Risks - Dealing with multiple and interconnected emerging risks*, Steinbeis Editon, Stuttgart (Germany), ISBN 978-3-938062-33-3.

Papazoglou, I.A., Nivolianitou, Z., Aneziris, O. & Christou, M. 1992. Probabilistic safety analysis in chemical installations, *J. Loss Prevention in Process Industries*, Vol. 5, No. 3, 1992, 181–191.

Sandia Report 2004. Guidance on Risk Analysis and Safety Implications of a Large Liquefied Natural Gas (LNG) Spill over water, *SAND 2004-6258*.

Taveau, J. 2010. Risk assessment and land-use planning regulations in France following the AZF disaster, *Journal of Loss Prevention in the Process Industries*, In Press, Corrected Proof, Available online 21 April 2010.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

ITRA: GUST—The Guttman scaling tool for supporting IT risk assessment audits

R. Mock & Ph. Aeschlimann
University of Technology Zurich, Zurich, Switzerland

ABSTRACT

There is not a chance for something like Fault Tree Analyses of IT at Small and Medium Enterprises (SME): At any rate, practitioners regard a check list approach as a resource-conserving method of choice. However, the seemingly simplicity of check list compilation and application often leave aside its heuristic procedures and biased results.

Optimising the way of questioning in check lists offers great potential to improve the quality of risk assessment surveys of IT infrastructures at enterprises. For this, staggered lists of IT security measurements are constructed (Guttman scales) whereas the Code of Practice ISO/IEC 27002 [1] provides the objectives and recommendations relating to information security management in this regard. The FMEA approach finally structures the overall risk analysis process. A questionnaire/ survey design using this "Best Practice FMEA" enables the analyst to represent the results in the form of matrices of measurements with regard to the Code's Objectives improving statistical analysis and validity. The respondents' answers are displayed as rectangular array **X** of j; $j = 1, 2, \ldots, n$ rows and $k = 1, 2, \ldots, 5$ columns. The statistical evaluation of **X** mainly sorts Objectives, e.g. in ascending order from total non-implementation $O_{j;non} = \{0\ 0\ 0\ 0\ 0\}$ to full implementation of measurements $O_{j;full} = \{1\ 1\ 1\ 1\ 1\}$.

Three types of scales are developed: Pure and near Guttman scaling as well as an FMEA scaling of frequencies of expected interferences or failures. However, the drift from pure Guttman to other scales requires sophisticated statistics to group the Objectives.

The statistical evaluation process uses k-means which is a nonhierachical clustering method. Hierarchical clustering methods are only outlined as already presented at the previous ESREL conference. Both clustering methods are equivalent as they group the Objectives in the same way. With regard to applicability, the k-means approach is found easier to implement at (small and medium-sized) enterprises. The interpretation of k-means results is eased by the usage of shilhouette plots.

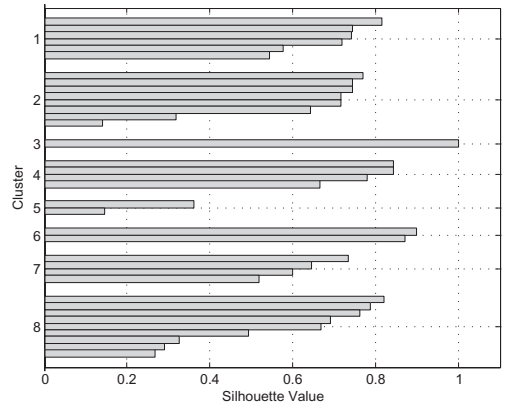


Figure 1. Silhouette plot of clusters according to case study data (Value ≥ 0.6: Objective is well located in its cluster).

The results of a literature research show the placement of Best Practice FMEA among other IT risk assessment approaches, e.g. CRAMM and OCTAVES. It becomes apparent that Best Practice FMEA is most applicable at small-scale enterprises which are not fully covered by the other approaches.

The paper also shows the transfer of the previous paper-based approach into the web based tool ITRA: GUST. The concepts of tool design and software architecture are presented. The closing remarks summarise and reason the method development of Best Practice FMEA and ITRA: GUST.

REFERENCE

[1] ISO/IEC, 2005. Information Technology – Security Techniques – Code of Practice for Information Security Management (ISO/IEC 27002:2005).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Literate PSA modeling for a modular PSA

M. Hibti
Departement Management des Risques industriels, EDF R&D Clamart, France

The very act of communicating one's work clearly to other people will improve the work itself.

D.E. Knuth

ABSTRACT

Now that PSAs are widely used to check and improve the design of many complex industrial systems, and as a key tool for maintenance planning and many Risk Informed Decision processes, it is time to take a look at the complexity of the tool and have a discussion on the way models are built and documented.

For Nuclear Power Plants, for example, many PSA models were developed and are used for maintenance and operational tasks. These models have been extended in many directions to meet licensees needs and safety authority requirements. The models nowadays deal not only with internal events, for shut-down and power states, but also with fire, flooding, and all external events in addition to other considerations with respect to different PSA applications.

These developments depend on the softwares that are used to develop the models. Moreover, the modeling was mostly performed regarding a set of needs, requirements, extensions that may not have necessarily been planned initially. This generally leads to huge models with the following characteristics:

- The models are developed by many PSA developers, with different methodologies, and with different objectives (e.g. a model for internal events is not developed in the same way as one dedicated to technical specifications needs),
- Different tricky modeling (due the lack of expressiveness of the Boolean Algebra) may be used without necessarily being documented since it seems "at least for the moment" obvious for the user.
- The different changes are reported on the basis of "reference" model documentation and may be limited to what the user thinks it is relevant.
- The lack of modern version control tools makes the model changes sometimes derivating and a important amount of time may be needed to recover from such situation or just to merge two different developpement versions.

In this paper, we propose to pursue an idea of Donald Knuth (*Literate Programming*) to propose a Literate PSA Modeling. The idea is to implement PSA modeling in such a way that "the presentation of the model", its clarity and its accurate use shall be considered as an objective of a good PSA modeling. A prototype is proposed to give an idea of what could be a tool of literate PSA modeling. We discuss the benefits of such approach in a context of modular PSA, the reasons for which such an approach, initially introduced as Literate Programming was not successful in the computer science community and why it should be in the community of PSA modeling/programming.

REFERENCES

[1] Bezroukov, N. 2006. Portarits of Open Source Pioneers. http://www.softpanorama.org-/People/Knuth/literate programming.shtml
[2] Hibti M. 2010. Vers une eps modulaire. In Actes du congr lambda/mu, La Rochelle.
[3] Knuth, D.E. 1983. Literate programming. Technical report STAN-CS-83-981, Stanford University, Department of Computer Science.
[4] Schulte, E. et al., To appear. A multi-language computing environment for literate programming and reproducible research. Journal of Statistical Software.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Managing the risks to personnel within occupied buildings

N.J. Cavanagh
DNV, London, UK

ABSTRACT

Accidents like Buncefield and Texas City have put the risk to people in occupied buildings high on the agenda of both regulators and operators. Regulatory regimes for assessing the safety of those in occupied buildings are becoming more demanding and the need for accuracy and transparency has increased. For example, regulatory guidelines like API RP752 and RP 753 provide guidance on the design and location of permanent and portable buildings to minimise risks to occupants. This paper focuses on advances in software models for assessing risks to people in buildings from releases of flammable materials.

When deciding on the location and construction of occupied buildings in the vicinity of hazardous installations, a number of factors must be considered during the design and operational phases. Key to the process of deciding where to locate buildings and what level of protection they should offer their occupants are the level of risk to which it is acceptable to expose those occupants. Traditional QRA tends to use "generic" vulnerability for people indoors where their probability of death when particular levels of different types of hazardous effects are exceeded, such as explosion overpressure, radiation from fires, flame impingement or toxicity, is treated as being independent of the type of building within which they reside, This is obviously a significant limitation to using the results of traditional QRA in selecting appropriate building types in different situations or to locate buildings in the safest place from the standpoint of risk to occupants.

Risk to building occupants is a function of both building location and construction. In order to minimise risks to personnel in the most cost effective way, plant designers and safety managers need to be able to compare and assess different options with ease.

This paper describes recent advances in the capabilities of the Phast Risk QRA tool (Cavanagh et al., 2009, Cavanagh 2010) which allow analysts to assess the relative benefits of using different building types to reduce risks to their occupants. These new features enable individual definition of building types and associated occupant vulnerability. In addition, GIS facilities allowing analysts to locate buildings of a particular type in various locations help ensure overall risks can be minimised, or location specific risks for particular buildings can be assessed. A case study is used to illustrate the application of the new vulnerability modelling to selecting suitable building types, and locating them in the most appropriate position to minimise risks to occupants. In addition, techniques are described for using these methods to help locate and design buildings to withstand the possible explosion, radiation and flammable effects to which they may be subjected.

REFERENCES

Cavanagh, N.J. 2010. Recent advances in software for modelling the risks associated with gas explosions in congested spaces using the Multi Energy Method, 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industry, June 6th–9th, Bruges, Belgium.

Cavanagh, N.J., Xu, Y. & Worthington, D.R.E. 2009. A Software Model for Assessing Fatality Risk from Explosion Hazards using the Multi Energy Method and Baker Strehlow Tang Approach, Hazards XXI Symposium, November 10th–12th, Manchester, UK.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Method for quantitative assessment of domino effect caused by overpressure

F. Kadri, E. Châtelet & G. Chen
UMR STMR—CNRS, Institut Charles Delaunay, Université de Technologie de Troyes, Troyes, France

ABSTRACT

In the field of risks analysis, the domino effect or chain of accidents has been documented in technical literature since 1947. The accidents caused by the domino effect are those that cause the most catastrophic damage. The consequences of the damage caused are at various levels and may not only affect the industrial sites (activities, importance …), but also people, environment and economy. The probability of the domino effect is increasingly high due to the development in industrial plants, their proximity to such establishments, and their inventory of dangerous substances, the transportation networks and the population growth.

The potential risk of the domino effect is widely recognized in legislation since the first "Seveso-I" Directive (82/501/EEC), which required the assessment of domino effects in the safety analysis of industrial sites whose activities are subject to this directive. Furthermore, the "Seveso-II" (Directive 96/82/EC 1997) extended these requirements to the assessment of domino effects not only within the site under consideration, but also to nearby plants.

Recently, in an inventory of the past domino accidents (Abdolhamidzadeh, Abbasi, Rashtchian & Abbasi 2010), authors have recorded 224 domino accidents occurred over the period 1917 to 2009 with 30% of these domino accidents recorded between (2000 to 2009). This study reveals that explosion are the most frequent cause of domino effect (57%), followed by fires (43%).

An industrial site and/or storage areas contains many storage equipments that may be subjected to an external and/or internal incident like overpressure. The escalation vectors or physical affects (overpressure, heat radiation, and toxic release) generated after a vessel rupture (explosion), may affect the surrounding equipment / facilities. If the affected targets are damaged, these latter, may also explode and generate another threats to other surrounding equipments / facilities and so on. This accident chain is a domino effect and may lead to catastrophic consequences in an industrial plant.

A review of methodologies and software tools used in the literature to the study of the cascading events, (Kadri & Châtelet & Elegbede 2011) shows that, in the last decade, the available methodologies for the assessment of domino effects caused by overpressure waves to process equipment in the framework of domino effect analysis are based on the probit models.

The objective of this paper is to present a methodology for the quantitative assessment of domino effect caused by overpressure to industrial equipments and to compute the individual risk in the framework of domino effect analysis. In the introduction, the second sub-section is devoted to the definition of the domino effect and some major accidents involving chain of accidents identified in the literature. In the next section, a brief analysis of previous works is presented. In the third section, a methodology for quantitative assessment of domino accidents in industrial sites is presented. The fourth section uses a case study to illustrate the proposed model and to present typical results. The last section concludes this paper.

REFERENCES

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D. & Abbasi, S.A. 2010. Domino effect in process-industry—An inventory of past events and identification of some patterns. *Journal of loss Prevention in the Process Industries*, 1–19, Article in Press.

Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances, *Official Journal of the European Communities*, L 10/13 of 14 January 1997.

European Community Directive (82/501/ EEC).

Kadri, F., Châtelet, E. & Elegbede, C. 2011. Domino Effect Analysis and Assessment of Industrial Sites: A Review of Methodologies and Software Tools. *Reliability Engineering & System Safety*, Under review.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Organizational interface failures: A historical perspective and risk analysis framework

T.T. Pires & A. Mosleh
University of Maryland at College Park, MD, US

ABSTRACT

This article argues that it is crucial to extend our understanding on how weaknesses in Organizational Interfaces (OI) can contribute to significant losses. The bases of the argument are detailed analysis of various accidents and incidents that have occurred in the past, with an emphasis on identifying evidence that organization interface flaws played important role in such accidents and incidents. The analysis presents accidents and incidents in assorted fields including commercial nuclear power generation, air and rail transportation, health care, defense, space exploration, and the entertainment industry. The objective of the analysis is to provide building blocks for a generic OI failure classification scheme and an approach to quantify OI failure probability based on a model of organizational interface. The accidents and incidents analysis has revealed that poor communication channels, lack or weak collaboration mechanisms and poor coordination were important factors in the initiation, development, and/or mitigation/prevention of the accidents and incidents analyzed. Therefore, communication, coordination and collaboration interface failure are defined as top level OI failure categories.

Communication Interfaces (CmI) are important because it is through them that information is exchanged between the elements at the ends of the interface. Some CmI failures identified in the accident/incident analysis include wrong information content being transmitted, information transmitted or received at the wrong time or location, etc. Coordination Interfaces (CrI) are important because it is though them that the information that is communicated is used for a purpose. Some CrI failures identified include poor organizational rules and common grounding, causing the inability to identify one's intent, comprehension of the situation, and poor feedback. Collaboration Interfaces (CoI) are important because it applies to the interactions among the elements at the interfaces, which must have trust, has to be beneficial, and lead to joint value creation. Some CrI failures identified include lack of confidence or predictability in one's expectation and lack of confidence in the other's goodwill.

The paper will summarize these insights and provide the evidence gathered to support the classicization of interface failures. Having identified these three OI failure categories, the paper outlines an approach to incorporate OI failures in risk models of complex socio-technical systems. The risk model can then be used in aiding organizations identifying and eliminating interface weaknesses, and comparing different interface design alternatives. The quantification approach proposed is a Bayesian belief network model that accounts for a set of factors assumed to influence communication, coordination and collaboration interfaces failure probability. An illustrative example is presented, using one of the accidents analyzed as subject.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic risk analysis procedure for aircraft overruns

M.G. Gratton, M. De Ambroggi & P. Trucco
Department of Management, Economics and Industrial Engineering, Politecnico di Milano—Milan, Italy

ABSTRACT

According to the World Aircraft Accident Summary, during the 14-year period from 1995 through 2008, commercial transport aircrafts were involved in a total of 1,429 accidents resulting in major or substantial damage. Considering the 431 runway-related accidents (30% of the total), the 97% (or 417 accidents) were runway excursions (FSF, 2009). Mitigations approaches for these kinds of accident mainly consist in the enlargement of the runway safety area up to standards set by international or national agencies. This procedure is however very expensive and in many cases of no easy accomplishment. There is therefore the need for a probabilistic risk-based approach to analyze the portion of space lying beyond the runway end to understand if case-specific solutions, alternative to standard requirements, are available.

Based on a literature review of available models, we assumed the ACRP hazard probability model (Hall et al., 2008) as a basis for the development of a Probabilistic Risk Analysis procedure specific for aircraft overruns. Input variables (e.g. aircraft characteristics, runway characteristics, weather conditions) were described by way of statistical distributions derived from historical data of the airport under analysis. The resulting probability distribution of accident probability was then calculated by means of Monte Carlo simulation and used, along with longitudinal and lateral location models, to generate a two-dimensional grid reporting the probability of each area to be the end location of an overrun accident. This result is particularly original and useful as it can be reported superimposed to an airport map to provide immediate visual information on the probability of interactions between overrunning aircrafts and infrastructures beyond the runway end.

Further a stocastic indication of the kinetic energy was also introduced on the location models, so as to provide a a quick and "easy to use" index of the potential crash severity. The characterization of the probability distributions of possible aircraft weight and speed, in fact allowed to generate a topological representation of the mean aircraft kinetic energy in each area of the grid.

From the union of kinetic energy probability distributions and the grid of accident probabilities, an Iso Kinetic Energy Area grid was assembled, once again thanks to the adoption of Monte Carlo simulation. This final result is able to summarize the probability and consequences of an accident into a single risk-related index with an associated topological map (Figure 1). The results of the proposed PRA procedure can be used in many ways: once an acceptable risk threshold is defined, critical locations and infrastructures may be located at a glance; acting on the probability distributions of input variables "what if" analyses and accident rate forecasts can be easily performed.

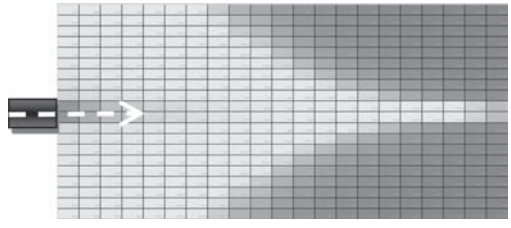


Figure 1. Expected aircraft kinetic energy [kJ/movement] in different points beyond runway end.

REFERENCES

Flight Safety Foundation. 2009. *Reducing the Risk of Runway Excursions.* Flight Safety Foundation.

Hall, J., Wong, D. & Ayres, M. 2008. *Analysis of Aircraft Overruns and Undershoots for Runway Safety Areas.* Airport Cooperative Research Program. Washington DC: Transportation Research Board.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic Safety Assessment of a UF_6 production process

Behrooz Ebrahimi
Department of Energy Engineering of Sharif University of Technology, Tehran, Iran

ABSTRACT

Application of Probabilistic Safety Assessment (PSA) to a Uranium Hexafluoride (UF_6) production process in this paper is presented. The process is constituted from three main units, UF_4 conversion to UF_6, condensation of produced UF_6 gas and tail gas treatment. UF_4 powder reacts with F_2 and N_2 gas mixture in a vertical fluorination reactor. Produced gas goes to condensation unit and is condensed in two stages. Gaseous waste from condensation process goes to tail gas treatment unit for F_2 and HF removal. Radioactive gas is present in all parts of the process and occurrence of high pressure or temperature in process equipments may lead to radioactive release to workplace and environment. The work is mainly based on PSA experience in nuclear power plants. Accordingly for the process, major Initiating Events (IE) leading to UF_6 gas release have been identified using HAZOP study. Eight different groups of IEs after HAZOP study have been identified. These IEs are events leading to high pressure or temperature in Fluorination Furnace or two condensers, which eventually will lead to UF_6 gas release. For each IE, based on related safety systems and functions, accident sequence analysis is performed with Event Tree Analysis (ETA). First step in ETA is identification of safety systems and functions which act against IEs. After identification of safety systems, they are entered as top events of event trees and based on engineering judgments final states of different accident sequences in ETA has been defined.

For frequency estimation of IEs which require failure of more than one component to occur FTA is used, for other IEs since data from similar plants are unavailable simply expert judgment has been applied. Due to greater reliance placed on operator in nuclear fuel cycle facilities compared to NPPs, special consideration is taken into account for Human Reliability Analysis (HRA). HRA is performed according to Swain and Guttman method (THERP) described in NUREG/CR-1278. For human error analysis and quantification, five Performance Shaping Factors (PSF) are considered: Time margin, Effect of scenario (Stress level), complexity of decision making, Man-Machine Interface (MMI) and quality of procedures.

Results of the study show frequency of 3.77E-04 (1/year) for radioactive release in the process. Considering worst possible condition for radioactive source term released in the workplace, maximum dose exposure for operator is 1 mSv. According to internationally accepted Probabilistic Safety Criteria (PSC) for Non-Reactor Nuclear Facilities (NRNF) the plant risk is acceptable. However using two importance measures namely Fussel-Vesely and Birnbaum importance, suggestions for safety improvement of plant are provided. Fussel-Vesely measure shows great contribution of human errors in plant risk which could be reduced by further training. Birnbaum measure on the other hand shows importance of CCFs which could be improved by using defense in depth.

REFERENCES

EPRI (2006). Reliability and Risk Significance for maintenance and reliability professionals at nuclear power plants.

IAEA (2002). Procedures for conducting Probabilistic Safety Assessment for non-reactor nuclear facilities, IAEA-TECDOC-1267, Austria, IAEA.

Kirchsteiger C. On the use of probabilistic and deterministic methods in the risk analysis, Journal of Loss Prevention in the Process Industries, 1999.

Mosleh A. & Rasmausen D.M. Common cause failure parameter estimation, 1998, NUREG/CR-5497.

Mosleh A. & Rasmausen D.M. Guidelines on modelling common cause failures in probabilistic risk assessment, 1998, NUREG/CR-5485.

Swain, A.D. & Guttmann, H.E. Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, 1983, NUREG/CR-1278, USNRC.

van der Borst M. & Schoonakker H. An overview of PSA importance measures, Reliability Engineering and System Safety, 2001.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Safety factors in fire safety engineering

H. Bjelland & O. Njå
University of Stavanger, Stavanger, Norway

ABSTRACT

During the 1980s and 1990s there was a major regulation regime shift in many countries, going from a regulation based on prescriptive solutions to performance-based design. Many authors were involved in the process of developing appropriate performance goals and engineering tools (Hadjisophocleous, Benichou et al., 1998).

In this paper we discuss the current practice of fire safety design, i.e. a prescriptive approach with deviations and a deterministic approach. We also take a look at the probabilistic approach. Based on our experience with the fire safety engineering industry we claim that a probabilistic approach introduces serious fundamental challenges. These challenges are related to a) a lack of holistic understanding of the sociotechnical relationships between buildings, fires and occupants and b) the lack of relevant probabilistic data.

Consequently, we argue that a development of the current practice based on deterministic approaches and the use of safety factors is more promising. Our perspective is the abilities of buildings to provide life safety for occupants during a fire. This leads to a discussion of safety factors related to Required Safe Egress Time (RSET) versus Available Safe Egress Time (ASET) (Babrauskas, Fleming et al., 2010).

The concept of safety margin between load and capacity is challenging in engineering of occupant fire safety. If the safety margin is related to an extreme event, an even more extreme event could always be specified. The concept of safety margin appears to be important to regulators; hence there is a need to address its contents. In structural engineering the safety margin reflects variability with respect to loads deviating from "normal conditions" and variability in material characteristics and erecting performance. It is clearly defined within the load code framework which events should be considered to act simultaneously (Moe 1971; Blockley 1992).

In fire safety engineering the safety margin must reflect something else than the traditional safety factor. This paper discusses safety margins from the Norwegian fire safety regulation. There appears to be a dramatic gap between the fire safety engineering environment's competencies to adopt probabilistic approaches and the intentions behind the functional fire safety regulations. The question is therefore what enhances good engineering practice and what does not? Fire safety engineers search for deterministic scenario-based designs, thus the safety margins must encompass relevant uncertainty factors.

We conclude that practical fire safety engineering should utilize a deterministic approach and focus on safety factors. This is due to engineers' lack of a fundamental understanding of phenomena and correlations, lack of relevant data, inability to become researchers in their own construction projects, and because academic inspired risk assessments is often performed at the expense of making engineering knowledge explicit.

REFERENCES

Babrauskas, V., Fleming, J.M., et al. (2010). "RSET/ASET, a flawed concept for fire safety assessment." *Fire and Materials* **34**(7): 341–355.

Blockley, D.I. (1992). *Engineering safety*. London, McGraw-Hill.

Hadjisophocleous, G.V., Benichou, N., et al. (1998). "Literature review of performance-based fire codes and design environment." *Journal of Fire Protection Engineering* **9**(1): 12–40.

Moe, A.J. (1971). *The factor of safety in technical structures. Copenhagen*, Dansk Ingeniørforening.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Setting rational safety goals for human spaceflight

Joseph R. Fragola
Vice President M&S / Risk Analysis at Valador, Inc., Rockville Center, US

Elisabeth L. Morse
Systems Engineer at Valador, Inc., Broadlands, US

ABSTRACT

NASA is embarking on a new era of human spaceflight, one in which commercial service providers will sell astronaut transportation services to NASA. Thus NASA will have limited insight into the design and manufacturing processes of space transportation vehicles. In this new paradigm, setting appropriate safety requirements and goals, for the service providers to meet, and a standard process for evaluating the safety of commercial rides, will be of paramount importance to ensuring the safety of the astronauts.

Good systems engineering practice emphasizes the importance of having valid and verifiable requirements (NASA 2007). While challenging requirements can serve as incentive for the industry to innovate, requirements that are too high could be ignored altogether. In the case of safety, carrying an unrealistically high, and thus unverifiable requirement can actually reduce the safety of vehicles under development because it can lead to focus on quantification of known failure modes rather than on a search for the unknowns, focus on process rather than experience, false sense of security, and tendency to game the analysis to meet the requirement (Gleick 1993, Jenkins 1992).

A probability of Loss Of Crew (LOC) requirement cannot be strictly verified, as there will be too few flights for statistics and probability forecasts are only "opinions" of the forecaster. But the reliability and safety that were actually achieved by previous vehicles, with reasonable expectations of growth, inform the range of LOC probabilities that can be credibly achieved by new systems. This paper shows how this process can inform the development of rational requirements with the example of launch vehicle safety.

Flight history shows that launch risk has been driven by the unknowns and the under-estimated, meaning that the actual safety risk faced by astronauts on operational missions is typically much higher than suggested by bottom-up analyses of system reliability "at maturity". The building of knowledge with time has led to both particular vehicle reliability growth and intergenerational reliability growth, but the second type of growth has diminished between launch vehicle generations (Morse 2010). Even accounting for further growth beyond historical results, the range of safety credibly achievable by new launch vehicles at maturity falls short of the 1 in 1000 requirement currently set by NASA; and on an operational flight even after ten successful test flights, the credible safety range is more than an order of magnitude worse than that goal.

The paper concludes that unless a new paradigm for launch vehicle design, manufacturing and operations can be developed that promises more than order-of-magnitude improvements over the natural generational growth, the ascent requirement for LOC should not be better than 1 in 50 to 1 in 200. Furthermore, the requirement has no meaning without a clear definition of verification method. In particular, verification will need to recognize the actual immaturity of most vehicles and to focus on evaluating how well the available analysis, flight and test data combine to eliminate the unknown and underestimated failure modes from the system.

REFERENCES

Gleick & James (1993). *Genius*. Knopf Double Day Publishing Group, NY.

Jenkins & Dennis (1992). S*pace Shuttle The History of the National Space Transportation System: The First 100 Missions*, World Print Ltd.

Morse, E.L., Fragola, J.R. & Putney, B. (2010). Modeling Launch Vehicle Reliability Growth as Defect Elimination II, AIAA Space 2010 Conference and Exhibition, (AIAA-2010-8836).

NASA Systems Engineering Handbook NASA/SP-2007-6105 Rev. 1, 33.

Reliability and safety data collection and analysis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A discussion on expert judgments in national risk analyses

K. Russell Vastveit & O. Njå
University of Stavanger, Norway

G.S. Braut
Stord/Haugesund University College, Norway

M. Ruge Holte
Directorate for Civil Protection and Emergency Planning, Norway

ABSTRACT

Risk and vulnerability analyses are widely used by national, regional and municipal authorities as well as many business sectors in Norway. In 2009 the Ministry of Justice and the Police asked the Directorate for Civil Protection and Emergency Planning (DSB) to develop a National Risk Picture (NRP) by conducting a National Risk Assessment. The end goal of the NRP was support of policy making. The project was conducted in three phases; methodology development; hazard identification; and scenario development and analysis. The analysis of ten scenarios was completed by the end of 2010 and the first National Risk Picture report was published in March 2011.The aim of the directorate is to continue the project by adding new scenarios to the National Risk Picture every year.

The work described in this paper deals with the core of risk analysis—the interpretation and understanding of risk, uncertainties and performance. It examines the use of experts in the context of the scenario development and analysis phase of the National Risk Assessment. It discusses the structure of expert judgment with regard to knowledge contributions to the analysis, the elicitation techniques that were used and associations with different types of judgment biases. Experts took part in the process by developing scenarios, providing consequence judgments and assigning probabilities to events described in the scenarios. They represented core organizations with responsibilities related to the specific scenarios. In addition they also held expert knowledge related to risk areas and the expected outcomes of events.

We found that there were several challenges associated with the expert opinion elicitation process during the scenario meetings.

Among there were a lack of scientific and professional knowledge; lack of and variation (local, regional, national or international) in personal experience; personal agendas (politics) and variation in preparations for the meetings. We observed the use of several heuristics, such as availability, anchoring and representativeness during the expert scenario analysis.

We conclude that the risk analysis process provided spin-off effects beyond policy making support, such as multidisciplinary learning and collaboration across institutional borders. The national risk analysis processes can therefore become the starting point for a significant shift in the national major hazard and accident prevention and emergency management concept. It is clear that experts are important participants when discussing consequences and uncertainties related to major disasters and incidents with serious impacts on society. We did however find that the scenario analysis meetings showed substantial weaknesses in the methodology used for expert judgment in National Risk Assessments. There is a lack of standardized and evaluated methods for expert participation in complex risk analyses at the societal level. Such methods would ensure that inputs from expert participation were made explicit and thereby open to criticism.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A simple polynomial regression to estimate the parameters of the Weibull distribution with $\gamma > 0$

I.B. Sidibé
Université Paul Verlaine, Laboratoire de génie industriel et de production de Metz, Metz, France

K.H. Adjallah
Ecole nationale d'ingénieur de Metz, Laboratoire de génie industriel et de production de Metz, Metz, France

ABSTRACT

The life of industrial mechanical equipment is in general a continuous random variable, difficult to be accurately predicted, in spite of progresses in reliability engineering. These random variables have statistical distributions that can be modelled using probabilistic distribution function such as exponential, gamma, Weibull, lognormal, etc. These laws must accurately describe the equipment degradation behaviour in operation.

The Weibull model is an important distribution widely used in mechanical reliability under those properties to describe the equipment behaviour (degradation process) throughout their lifespan (youth, maturity, old age). This distribution is defined by three positive parameters characterizing explicitly the model: β models the shape of the distribution, η models the scale and γ models the time origin of the failure events.

Field experience data should allow estimating these parameters but in practice this is difficult due to the complexity of the calculations requirements. There are three approaches for the parameters estimation: 1) the Allen Plait technique based on functional paper graphic; 2) analytical identification based on statistical inferences; 3) combines the two above techniques to estimating the coefficients of a regression line by the least square method.

In this paper, without any hypothesis, we introduce an approach for identifying the 3-parameters-based Weibull distribution function, conversely to the practice. We propose to implement a simpler, practical, robust and effective approach for estimating the Weibull 3-parameters distributions. Our method is based on polynomial regression whose purpose is to build an explicit expression of the parameters without recurrent use of optimization tools.

The approach uses analytical and graphical methods for estimating the parameters of a distribution for $\gamma > 0$. The first uses an analytical logic, i.e., mathematical tricks and Taylor series of sufficient order, to estimate the parameters. The latter uses posterior information on β to determine the most probable distribution. Combining both methods allows us relaxing the constraint on the parameters and show that they are as effective as the method of David (1975). We explicitly show that under the issued conditions our estimators are efficient.

The proposed approach is effective and robust, but its performance is skewed by the size and nature of the data. Its effectiveness depends on the data quality through the convergence of the estimators of the cumulative function.

REFERENCES

Al-Fawzan, M. (2000). Methods for estimating the parameters of the Weibull distribution. InterStat, 10(1).

Jukic, D. & Markovic, D. 2010. On nonlinear weighted errors-in-variables parameter estimation problem in the three-parameter Weibull model. Applied Mathematics and Computation, 215(10), pp. 3599–3609.

Markovic, D., Jukic, D. & Bensic, M. 2009. Non-linear weighted least squares estimation of a three-parameter Weibull density with a non-parametric start. Journal of Computational and Applied Mathematics, 228(1), 304–312.

McCool & John I. 1970. Inference on Weibull Percentiles and Shape Parameter from Maximum Likelihood Estimates. IEEE trans reliability.

Palisson, F. (1989). Détermination des paramètres du modèle de Weibull à partir de la méthode de l'actuariat. Revue, de statistique appliquée, 37, n° 4, pp. 5–39.

Qiao, H. & Tsokos, C.P. 1995. Estimation of the three parameter Weibull probability distribution. Mathematics and Computers in Simulation, 39(1–2), pp. 173–185.

Sidibe, I. & Adjallah, K. 2011. Analysis of the residual lifetimes of an equipment and deferred maintenance: case of the Weibull distribution.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Accelerated test model in fatigue life reliability evaluation of stub axle

E.A. Azrulhisham
Malaysia France Institute, Universiti Kuala Lumpur, Malaysia

Y.M. Asri
Universiti Teknikal Malaysia Melaka, Malaysia

A.W. Dzuraidah
Universiti Kebangsaan Malaysia, Malaysia

A.H. Hairul Fahmi
Engineering Division, Perusahaan Otomobil Nasional (PROTON), Malaysia

ABSTRACT

In view of increasing pressures of shortened development cycles and desire to save costs, accelerated life testing method has been devised to force products to fail quickly. In case where the scatter in fatigue life was neglected it is sufficient to know the relationship between load and the accelerated life using typical stress-life (SN) relationship. However, in terms of mass production, fatigue properties of material used in the fabrication of components cannot be exactly consistent in quality due to uncertainties associated with the size effect, machining and manufacturing conditions (Schijve 2005). These uncertainties factors should be considered as random variables that results in variation of the fatigue life curves (Azrulhisham et al., 2010).

In this study, fatigue life of an automotive stub axle was calculated by the linear damage rule stress-life method using stress range intercept and slope of a Probabilistic SN (PSN) curve along with Belgian pave load patterns. In this approach, the PSN curve was illustrated by the reliability function of Inverse Power Law–lognormal (IPL-lognormal) parametric model of accelerated cyclic load test. The IPL-lognormal parametric model was derived from incorporation of IPL stress-life model with lognormal life distribution. The parameters of the model were then estimated using Maximum Likelihood Estimation (MLE).

In view of the fact that that the material property represented by the PSN plot has been obtained by a set of accelerated cyclic tension test, the experimental data have the standard deviation and it is difficult to ensure that the actual material used in the fabrication is closely matched to the known mean value. In this study, the degree of reliability of the estimated fatigue life of the component was evaluated by developing a Pearson statistical model considering stress range intercept and slope of the PSN curve as random variables. Based on the first through fourth statistical moments, the type of the Pearson system was determined as Type I. Probability Density Function (PDF) of the fatigue life estimates shown in Figure 1 was obtained using Pearson curve of Type I relationship and the fatigue life reliability is then evaluated from the PDF.

Considering normal distribution of fatigue strength, it is found that the fatigue life of the stub axle to have the highest reliability between 4000–5000 cycles. Taking into account the variation of material properties associated with the size effect, machining and manufacturing conditions, the method described in this study can be effectively

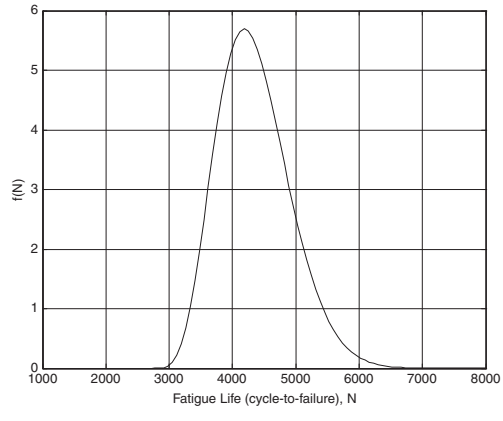


Figure 1. PDF of the fatigue life estimates.

applied in determination of probability of failure of mass-produced parts.

REFERENCES

Azrulhisham, E.A., Asri, Y.M., Dzuraidah, A.W., Nik Abdullah, N.M., Shahrum, A. & Che Hassan, C.H. 2010. Evaluation of Fatigue Life Reliability of Steering Knuckle Using Pearson Parametric Distribution Model. *International Journal of Quality, Statistics and Reliability.* vol. 2010, Article ID 816407, doi:10.1155/2010/816407.

Schijve, J. 2005. Statistical distribution functions and fatigue of structures. *International Journal of Fatigue* 9(7): 1031–1039.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Analysis of wave energy parameters based on copula functions

C. Ejoh & S. Sriramula
School of Engineering, University of Aberdeen, Aberdeen, UK

ABSTRACT

The amount of available wave energy at a particular location is one of the most significant variables influencing the installation choice of these turbine facilities. It is widely accepted that the available wave energy is highly uncertain and depends on the significant wave height and the zero-crossing period variations, which in turn are randomly varying. Probabilistic methods provide a rational framework to represent the randomness in reliable system performance. By simulating the variations in significant wave height and the zero-crossing period in terms of appropriate probability distribution models with accurate dependency considerations, it is possible to study the randomness in the corresponding wave energy output. This requires the formulation of the corresponding multivariate distribution model. Conventional approaches of simulation with multivariate probability distribution models require the univariate marginals to be from the same class or impose a restriction on the statistical dependence by the distribution parameters. The widely used Pearson's correlation coefficient for dependence modelling cannot capture the dependence structure accurately and may be misleading in case of non-elliptical distributions and is sensitive to outliers.

The desire to get the best and most reliable method for modelling data led to the research on copula functions. Although rather new to the engineering world, copula functions have been widely used in the financial and actuarial risk management strategies. These functions work by separating the dependence structure of the marginal distributions from the multivariate model. One very important fact about copula functions is that the marginal distributions can be chosen arbitrarily. This paper will show why copula based simulation is a better alternative than the traditional linear correlation based simulation by analysing wave energy parameters. Environmental field data on the significant wave height and the zero-crossing period is obtained from a potential turbine location and the dependency of these data is being utilised. Copula functions are then used to simulate the parameters and the dependence structure of the simulated data is compared to that of the actual data. The scatter plots for the elliptical copulas and for the traditional linear correlation method are shown in Figure 1. It can be seen that there exists a tail dependency in the observed data; both the Gaussian and the t-student copula simulate this tail dependency well but this is not the case for the traditional linear correlation method of simulation. All three Archimedean copulas are also found to be better representations of the observed data. By doing this, it is seen that the copula based simulation provides a better model than the traditional linear correlation method which is generally an acceptable engineering method. Its unique advantages and the flexibility could make it a preferred simulation option than the traditional linear correlation method.

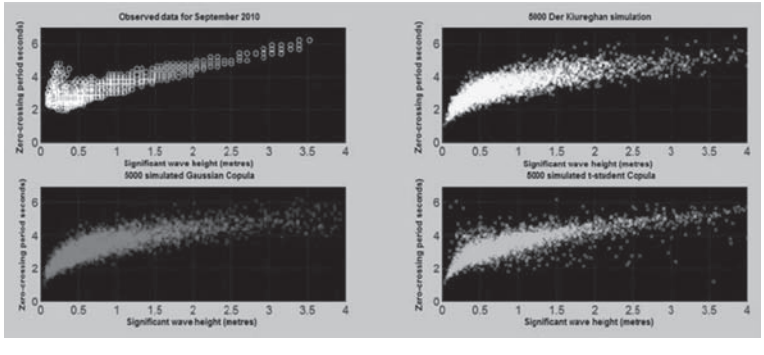


Figure 1. Scatter plots for the elliptical copulas and for the traditional linear correlation method.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Database concept in early stage of operation

I. Dziaduch & M. Mlynczak
Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Evaluation and management of new established systems is difficult and loaded with uncertainty because of lack of information concerning its behavior and possible disturbances. If common operation process is properly designed due to usage and maintenance, then expected effect and profit should be achieved. But usually random disturbances influence negatively process efficiency (human error, failures, environmental hazards). The role of operator and staff responsible for the operation process is carrying on the process and meets the threat preferably with sufficient advance. Operating manager usually expects positive feedback from the operation system to be informed how efficiency indexes vary due to undertaken actions.

It is described in the paper assumptions and formal model of database supporting the regional rail transportation system operating new rail-buses. The operational system is at present in build-up phase i.e., new rail vehicles are to be bought, new railway connections are opened and operating staff is growing. New elements of the system and expanding offer of services introduce much information and unexpected events. It is almost obvious that informative database and operation aid system have to be designed and introduced to real system. The computer aided system is directed on managing current operation and maintenance, especially preventive maintenance and scheduled preventive maintenance of single object in the group of objects. Proposed database, based on similar idea shown in Computerized Maintenance Management System (CMMS) has been improved by segment of cost analysis helpful in LCC methodology especially important for the owner of regional transportation system.

The crucial point underlies in selecting, collecting and processing operating data. Data acquisition is a spread computerized and based on formal written forms system. Database collecting segment involves operators, maintenance staff and dispatcher. The operating system has been identified and elements classified due to its role fulfilled in the system. Data are classified as a parameters of system components and parameters of process states. There are distinguished sources of data such as: people (operational staff, maintenance staff, passengers, third parties members), rail vehicle, transportation system support structure (rail road, control systems, passenger transfer points, concomitant infrastructure), natural environment (weather, season).

Database creates multilayer morphology space enabling analysis of statistic parameters and function and cross regression between important factors covering system performance, availability, safety and costs.

Making use of analysis results is expected in management of transportation system. Long-lasting observation will create database suitable for RAMSC (C- costs) analysis supporting design, operation, maintenance and safety as well as life cycle cost analysis in further investments.

REFERENCES

Barringer, H.P. 1996. *Life Cycle Cost Tutorial*. Fifth International Conference on Process Plant Reliability. Huston.

Beynon-Davies, P. 2003. *Database Systems.* transl. Szadkowska-Rucińska, M. WNT, Warszawa.

Golabek, A. ed. 2003. *Reliability of Buses.* Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław.

Inmon, W.H. 2005. *Building the Data Warehouse*. Wiley Publishing, Inc., Indianapolis.

Misra, K.B. ed. 2008. *Handbook of Performability Engineering*. Springer-Verlag London.

Mobley, R.K. ed. 2008. *Maintenance Engineering Handbook*. Mc Graw Hill. New York.

Nagabhushana, S. 2006. *Data Warehousing. OLAP and Data Mining*. New Age International Ltd. Publisher. New Delhi.

Taniar, D. 2008. *Data Mining and Knowledge Discovery Technologies*. IGI Publishing, Hershey, New York.

Thomsen, E. 2002. *OLAP Solutions. Building Multidimensional Information Systems*. Wiley Computer Publishing. John Wiley&Son. New York.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Estimation of an aging failure process taking into account change in trend and local perturbation

E. Idée, P. Briand & C. Labart
University of Savoie, LAMA—UMR 5127 CNRS, Le Bourget-du-Lac, France

V. Verrier & P. Bertrand
EDF R&D—Industrial Risk Management Department, Chatou, France

ABSTRACT

Power companies have entered a far more competitive market and industrial assets management is now a major issue. That is why EDF, the major French utility, must find strategies to detect ageing phenomenon, have robust estimation of component reliability or maintenance efficiency in order to reduce damages and to control costs.

When historical data are collected to model failure process of a component, different trends can sometimes be observed: at first, constant failure rate with a law intensity and then an increase in the number of failures. When change in trends occurs, classical non homogeneous Poisson process are not well adapted to describe these different periods.

The purpose of this paper is to propose a general threshold loglinear process adapted to describe:

- a break in the failure process (for example change in trend, which are usually observed when failure come from fatigue mechanism),
- some locally sudden increase in the number of failures.

This model is based on a classical loglinear process. The intensity of the threshold loginear process we studied is given by:

$$\lambda(t) = e^{a+bt+c_1 z(t)+c_2 z(t)} \quad \text{with}$$

$$z_1(t) = 1_{\{N(t^-)>0\}} 1_{\left\{t-t_{N(t^-)}\le s\right\}} 1_{\{t<t_1\}} \quad \text{and}$$

$$z_2(t) = 1_{\{N(t^-)>0\}} 1_{\left\{t-t_{N(t^-)}\le s\right\}} 1_{\{t_1\le t<\tau\}}$$

with $t \ge 0$, $s > 0$ and a, b, c_1, c_2 real.

The observation time is divided in 2 periods $[0,t_1]$ and $[t_1,\tau]$, where c_1 describes the first trend and c_2 describes the second one. The threshold S traduces the fact that the probability of failure grows temporarily faster after a failure than with the classical loglinear process. With this model, it is possible to calculate the relative difference of failure intensities between the two period, which gives an idea of the acceleration of the failure process. Parameters are estimated by maximum likelihood. Confidence interval can be given for b, c_1, c_2 considering asymptotic normality.

This model will be applied on a real data set corresponding to failures of some components of a fossil fired power plant. These components are subjected to thermal fatigue phenomenon: a long incubation time period is observed before the acceleration in the number of failure.

For these components, some sudden increase in the number of failures occur because of some hydraulic tests that are made to ensure repairs. When these tests are made, groups of failure can be observed on a short period of time in the historical data collection, that's why the threshold model is used to model this sudden increase.

The choice of the threshold s will be discussed on the ground of the example. The performance of the model is compared to the classical loglinear process.

REFERENCES

Cook, R.J. & Lawless, J.F. 2007. The statistical Analysis of Recurrent Events, Statistics for Biology, Springer.

Lindqvist, B.H. 2006. On the statistical modeling and analysis of repairable system, Statistical Science, 21 532–551.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Gamma process classification according to relevant variables: Problem statement and first study

Xuan Zhou Wang, Edith Grall-Maës & Pierre Beauseroy
Institut Charles Delaunay-LM2S, UMR STMR CNRS Université de Technologie de Troyes, Troyes, France

ABSTRACT

With the rapid development of engineering industry, the importance of system reliability and maintenance management has grown (Dekker & Scarf 1998). In order to analyze the reliability or to make a maintenance decision of the system, we could look into a number of sample data that characterize the deterioration level. However, the sample data often come from different system classes, and for each class the deterioration level is supposed to be modeled by a statistical process that depends on certain parameters. It is also assumed that the deterioration model depends on some covariates. Take the corrosion of pipeline for example, we could probably measure the thickness in certain parts of the pipeline as sample data that represent the deterioration level. Besides, as the deterioration process might be changing in different positions of the pipeline, we could refer to the positions as covariates. Since the values of thickness might be described by some mathematical process, we need to know which process they fit best and make a proper decision to carry out the maintenance based on such kind of information. In a word, the aim is to design a decision rule depending on the covariates to determine the deterioration model that applies to the observed system. For achieving that aim, a partition of the covariate space needs to be learned and the parameters of the stochastic process have to be estimated simultaneously using the data.

In this paper, we consider the deterioration processes as the homogeneous Gamma processes. According to (Van Noortwijk 2009), the Gamma process is appropriate for stochastic modeling of monotonic and gradual deterioration, as it can be well adapted to data in a lot of cases such as creep of concrete, fatigue crack growth and corroded steel gates etc. The property of 'homogeneity' represents that the transition probability between two given state values at any two times depends only on the difference between those times. A brief summary of Gamma process is given including its definition and several important statistical and mathematical properties.

Some assumptions have been made in the paper. We suppose that the observations belong to two classes, and all the realizations of process originating from one class share the same parameters. In other words, There are two parameter vectors that characterize the realizations of the homogeneous Gamma process. Also, the covariate vector for each observation is assumed to be mono-dimensional, i.e., the covariates could be interpreted by scalar. A more complex situation with multi-classes and multidimensional covariates will be studied in the future work.

We propose a method *Maximum Likelihood Classification* for classifying the observations. The basic idea is to compute the sum value of maximum likelihood for each possible partition of classes in terms of covariates, and the best partition is supposed to be the one with the maximum value. Once the partition of classes is known, we are able to compute the estimated parameters for each class.

For the numerical study, we test two estimators of the Gamma process parameters: the maximum likelihood estimator and the moments one (Cinlar, Bazant & Osman 1977). Besides, several analysis have been made in different aspects such as the influence of the observation number and the effect of dissimilarity between the two considered classes. The numerical result shows that the algorithm is well adapted when there exists a significant dissimilarity between the two classes, which is the most interesting case in our study.

REFERENCES

Cinlar, E., Bazant, Z. & Osman, E. (1977). Stochastic process for extrapolating concrete creep. *Journal of Engineering Mechanics 103*(ASCE 13447 Proceeding).

Dekker, R. & Scarf, P. (1998). On the impact of optimisation models in maintenance decision making: the state of the art. *Reliability Engineering & System Safety 60*(2), 111–119.

Van Noortwijk, J. (2009). A survey of the application of gamma processes in maintenance. *Reliability Engineering & System Safety 94*(1), 2–21.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Improved estimation of failure frequencies for offshore pipelines and risers

Pavel Praks
VŠB-Technical University of Ostrava, Ostrava, Czech Republic

Sava Medonos
Petrellus Engineering Ltd, UK

ABSTRACT

Statistical failure frequencies of offshore pipelines and risers are relatively low, which would indicate good reliability. However, if a gas or oil leak occurs and it is ignited, the resulting consequences in the form of explosions and fires, harm to personnel, environmental damage, impairment of assets and financial losses may be very severe due to the high volume of leaking fluid. The relatively low number of observed failures causes uncertainties in statistical estimations of failure frequencies. This Paper deals with a probabilistic approach for analyzing data based on counts of events (failures) during the fixed time period of monitoring (pipelines-years and risers-years). There is a problem with uncertainties of data resulting from observed failures because of i) limited number of observed failures and ii) restricted time-monitoring limitations. As point estimations of failure rates for pipelines and risers can underestimate or overestimate the computed risk, this Paper gives probabilistic estimates of lower and upper bounds of failure characteristics. Advantages of using these probabilistic estimations for practical risk analyses in the offshore oil & gas production are also discussed.

In this Paper we present typical leak scenarios of hydrocarbons from pipelines and risers on a piled offshore production and risers platform, and analyze uncertainties in failure rates of selected components from the offshore industry. The Poisson model is used for computing confidence limits of the failure rates. Our test case indicates that especially the short exposure times of flexible pipelines risers and steel wells risers cause substantial uncertainties of failure rates, i.e., large confidence intervals. Direct computations and the simulation approach show how these input uncertainties influence a risk model. For example, with 90% confidence, direct computations indicate that IRPA (Individual Risk Per Annum) is somewhere between 3.32E-05 and 7.51E-04. The ratio between these numbers is approximately 22.6, which represents a significant uncertainty of risk predictions even when ageing is not modeled. When simulations are used, the far too rare extreme events are not fully detected. As a result, the total IRPA risk based on simulations is estimated between 2.8E-04 and 5.1E-04, which indicates a much more conservative ratio of 5.1E-04 / 2.8E-04 = 1.82. In the future, when ageing data will be available, it would be interesting to add a degradation model. An alternative approach based on genetic programming has been presented relatively recently in (Xu et al., 2011).

REFERENCES

Buchan, I. (2004). *Calculating Poisson confidence Intervals in Excel*. Public Health Informatics at the University of Manchester.

Engelhardt, M.E. (1994). *Events in time: Basic analysis of Poisson data*. Department of Energy (DOE), http://dx.doi.org/10.2172/10191309

Fleiss, J.L., Levin, B. & Paik, M.C. (2003). *Statistical Methods for Rates & Proportions*. Wiley.

PARLOC 2001. (2003). *The Update of Loss of Containment Data for Offshore Pipelines*, prepared by Mott MacDonald Ltd for the UK Health and Safety Executive, 5th Edition. Energy Institute.

Praks, P. & Medonos, S. (2010). Confidence Limits with Improved Accuracy for Time Dependent Ignition Probabilities of Blowouts in the Oil & Gas Industry. In Ale, Papazoglou & Zio (eds), *Reliability, Risk and Safety:* 1182–1185. Taylor & Francis Group, London.

Praks, P., Medonos, S. & Raman, R. (2010). Fire loads for realistic risk assessment applications in petrochemical industry. In: R. Briš, C. Guedes Soares, S. Martorell (eds.), *Reliability, Risk, and Safety: Theory and Applications*: 2199–2207. Taylor & Francis Group, London.

The UK HSE Hydrocarbon Releases System (covering 1 April 1992 to 31 March 2008).

Xu, Q., Chen, Q., Li, W. & Ma, J. (2011). Pipe break prediction based on evolutionary data-driven methods with brief recorded data. *Reliability Engineering and System Safety*, http://dx.doi.org/10.1016/j.ress.2011.03.010

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Links between reliability Cox model for MV electrical component and the reliability target defined for the global MV electrical network

P. Carer, R. Lattes, L. Guerineau & B. Puluhen
EDF R&D (« Clamart » and « Les Renardières ») France

L. Pierrat
L.&P Consulting Grenoble, University of Grenoble, France

ABSTRACT

In the context of the deregulation of the electricity market in Europe, the French regulator defines reliability and availability target for the electrical power supply. For example one of the target is:

- 95% of the customer at less than 6 outages per year ("outage": long power cut more than 3 minutes)

In order to estimate the reliability indices of the MV (medium voltage: 20 kV) distribution network, ERDF (the DSO Distribution System Operator in France) has:

- to estimate the failure rate of the different MV electrical component,
- and to compute at the level of the distribution network the reliability and availability indices.

A first approach (2004–2007) was to obtain for each component the Weibull law associated to the failure rate of the electrical component [Spelleman 2007]. Since 2006, in a second approach, more precise reliability model was developed to take into account the seasonal variation of the failure rate due to external weather constrains. Reliability model for the component taking into account weather parameter, such as the temperature, the humidity or the intensity of the lightning, was developed.

Reliability model elaborated for the electronic device such as the reliability "Peck" model [Peck 1986], [Blischke 2000] (Temperature, humidity) had been adapted for the MV electrical component. In the following model for one type on electrical equipment, the diffusion of the humidity represents the aging phenomena with the year of operating of the component, and the temperature is varying with the seasons of each year:

$$\lambda(t,T) = \lambda_o \cdot \left[1 + \left(\sqrt{D \cdot t}/h_o\right)\right]^n \cdot \exp\left[-\left(T_o/T\right)\right]$$

t: age of the component
T: temperature function of the season of the year
n: parameter
D: diffusion coefficient of humidity with the age
λ_0: nominal failure rate
h_0: nominal relative humidity of the component

New model to estimate the consequence of the lightning on the reliability of the MV/LV overhead transformer was developed based on the analysis of different failure reports.

These reliability model developed for different component are characterized by a seasonal increase of the failure rate during the summer due directly or indirectly (lightning) with the temperature.

Usually the customer is supply at least by two redundant MV electrical lines. The seasonal variation (increase) of the failure rate of some electrical component leads to an increase of the probability that the electrical redundant supply diagram fails. This phenomena is illustrated in the paper with a very simple example electrical diagram with active redundancy.

The work presented in this paper will contribute to the improvement of the estimation probability of the power cut frequency in the different regions of France.

REFERENCES

Blischke, W.R. & Murthy, D.N.P. 2000. Reliability Modeling, Prediction and Optimisation. New York: Wiley.

Peck, D.S. 1986. Comprehensive model for humidity testing correlation, Proc. of Int. Reliab. Phys. Symp., 44–50, 1986.

Spelleman, C. & Gauthier, L. 2007. Impact of aging on the MV underground asset reliability Proc. 19th CIRED International Conference on Electrical Distribution Vienna, 2007.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

On a goodness of fit test for gamma process: Comparison of an observed process with a reference

Edith Grall-Maës
Institut Charles Delaunay—CNRS UMR STMR—Université de Technologie de Troyes, Troyes, France

ABSTRACT

The applications of maintenance optimisation models are numerous. The modeling of deterioration is the basis of most of the maintenance models. Usually, the rate of deterioration is modeled in terms of a time-dependent stochastic process and generally assumed to be a Markov process. Gamma processes have been satisfactorily fitted to various data such as creep of concrete, fatigue crack growth, and thinning due to corrosion. The gamma deterioration process has been applied to model time-based preventive maintenance as well as condition-based maintenance [3].

Statistical goodness of fit tests characterize the discrepancy between observed values and the values expected under a model. For example, they can be used to test if an observation sample follows a specified distribution. Since their introduction [2] they have been widely studied in respect to general or specific distribution but rarely studied for processes. As far as the author knows, no study deals with goodness-of-fit test for the gamma process. Such test would be of real interest to decide if an observed process is fitted to a reference process in the aim of concluding if an optimal maintenance decision rule is valid for the observed process.

This paper presents a study of a statistical test based on the Kolmogorov-Smirnov test for comparing an observed gamma process with a reference gamma process, in the case of periodic or aperiodic inspection. The null hypothesis is defined as "the observed gamma process sample follows the reference gamma process". The test is built for satisfying a given first order error.

The well known Kolmogorov-Smirnov test allows to decide if a sample of independent and identically distributed observations is drawn from a reference distribution for a given first order error. In the case of a gamma process sample composed of observations with equal time increments, this test can be applied directly. It has been pointed out that the influence of the time increment is almost as important as the number of observations for the power of the test.

In the case of a process sample with unequal time increments, a method is proposed for building a sample composed of observations with equal time increments so that the Kolmogorov-Smirnov test can be used. Observations are generated using the gamma bridge [1] and the original sample. This requires to choose a shape parameter value because the true value for the sample is unknown. It has been shown that the best value to choose so that the targeted first order error is satisfied corresponds to the shape parameter of the reference gamma process. It has been proposed to choose as constant time increment the mean of the unequal time increments of the original sample, and an approach has been proposed to sort the original observations for improving the fitting of the observation instants with the constant time increment. The feasibility of the approach has been proved. Simulations have shown that the power of test is slightly enhanced thanks to the sort of observations and it decreases only a little when the variance of the time increments increases.

REFERENCES

[1] Avramidis, A.N., L'Ecuyer, P. & Trem-blay, P.-A. (2003). New simulation methodology for finance: efficient simulation of gamma and variance-gamma processes. In *Winter Simulation Conference*, pp. 319–326.
[2] Massey, F.J. (1951). The kolmogorov-smirnov test for goodness of fit. *Journal of the American Statistical Association 46*(253), 66–78.
[3] van Noortwijk, J. (2009). A survey of the application of gamma processes in maintenance. *Reliability Engineering and System Safety 94*(1), 2–21.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability prediction model of a multi-state system subject to general repair and maintenance with limited failure data

Masdi Muhammad, Ainul Akmar Mokhtar & Mohd Amin Abdul Majid
Universiti Teknologi PETRONAS, Malaysia

ABSTRACT

Effective maintenance management is essential to reduce the adverse effect of equipment failure to operation. This can be accomplished by accurately predicting the equipment failure such that appropriate actions can be planned and taken in order to minimize the impact of equipment failure to operation as well as optimizing maintenance resources. However, accurate failure prediction is often bounded by the scarcity of time to failure data as mentioned by several researchers.

The current study focuses on the development of reliability assessment model for repairable equipment subjected to degradation by utilizing equipment performance data instead of the normally used time to failure data. The system performance data is gathered and then clustered into several discrete states using a combination of *k*-means data clustering method and silhouette plots. The theory of multi state repairable system is then used to determine the system reliability based on the state definitions and different repair assumptions.

A repairable system is defined as a system which can be restored to satisfactory working condition by repairing or replacing the damaged components that caused the failure to occur rather than replacing the whole system. In other words, the system performance degrades into several discrete states prior to total system failure. The degradation process, if left unattended, will often lead to degradation failure that can be attributed to a myriad of factors including variable operating environment, fatigue, failures of non-essential components and random shocks on the system. In addition, the system can experience random failure from any state at anytime upon which a general repair will be performed bringing the system back to the state between new and old. A general preventive maintenance is performed when the system reaches the last unacceptable state, again, bringing the system back to state between old and new.

This paper presents a development of model based on discrete time Markov process for a degraded multi-state system subject to both general repair and maintenance to assess the system reliability. The system degradation was quantified by discrete level of system's performance from perfect functioning state to complete failure. An actual case study is presented to illustrate the applicability of the model. The results indeed prove the relevancy of discrete time Markov in assessing the reliability of multi-state systems using the system performance data when there is very limited time to failure data. This is shown by the statistical comparison of reliability predictions results from traditional binary assumption using time to failure data.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability prediction of oil wells by support vector machine with particle swarm optimization for variable selection and hyperparameter tuning

I.D. Lins, M.C. Moura & E.L. Droguett
Departamento de Engenharia de Produção, Centro de Estudos e Ensaios em Risco e Modelagem Ambiental Universidade Federal de Pernambuco, Recife, Pernambuco, Brazil

E. Zio
Laboratoire Génie Industriel, Ecole Centrale Paris-Supelec, Paris, France
Dipartimento di Energia, Politecnico di Milano, Milan, Italy

C.M. Jacinto
CENPES, PETROBRAS, Rio de Janeiro, Brazil

ABSTRACT

In oil industry, sudden failures of wells are not desirable since they bring non-planned costs, *e.g.,* loss of assets, costumer dissatisfaction, environmental damages, among others. In order to prevent these situations, reliability prediction can be performed so as to enable proper maintenance planning. Different factors, such as operational and aging conditions, impact the reliability behavior of production systems and a comprehensive analytical treatment may be prohibitive due to the increased complexity of the problem.

Alternatively, an empirical modeling based on observations such as regression via Support Vector Machine (SVM) may be effective as a reliability prediction tool. One of the main advantages of using SVM are: (i) the training step involve a quadratic optimization problem for which the Karush-Kuhn-Tucker conditions for a global optimum are necessary and sufficient, thus SVMs are not trapped in local optimum; (ii) the training objective function trade-offs the machine generalization capacity with training errors. Nevertheless, the performance of SVM depends on a set of hyperparameters required by the training optimization problem.

Besides, in regression problems, the available data set may contain numerous explanatory variables that may be redundant or even irrelevant to enlighten the variability of the response variable. Situations like this may arise mainly when there is lack of knowledge about the functional relation between the target and the other variables, which is common when Support Vector Regression (SVR) is chosen as learning approach. Common methods for variable selection, such as the backward elimination strategy, do not allow for the concurrent adjustment of hyperparameters. However, during this incremental procedure, optimal values of the SVR hyperparameters may change, given that the training data set is progressively modified. In spite of that, a new search for the SVR hyperparameters is often skipped due to the additional computational effort.

Therefore, this paper presents a Particle Swarm Optimization (PSO) algorithm, which is a probabilistic optimization technique based on the group motion of organisms, for the simultaneous variable selection and SVR hyperparameter tuning. The resulting PSO+SVR methodology is used for the prediction of times between failures of onshore oil wells located in the Northeast of Brazil. Although being related to mature wells of low productivity, onshore activities are responsible for a non-negligible part of the national oil production. The obtained results show that the variable selection procedure, combined with hyperpa-rameter adjustment, enhances the predictive ability of SVR. The outcomes also indicate that PSO+SVR is a promising tool for reliability prediction and it could be part of maintenance framework so as to support decisions concerning preventive actions.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability prognosis for mobile phones: A case study

A. Braasch, F. Plinke, D. Althaus & A. Meyna
University of Wuppertal, Germany

ABSTRACT

Nowadays, technical devices are expected to operate faultlessly and reliable. Failures especially when occurring during the warranty period result in extensive costs for the manufacturer and displease the customer. As there are no absolute reliable products, measures have to be taken by the manufacturer to deal with occurring failures quickly and customer-friendly.

As shown in Pauli (1998) Reliability prognosis models have been proved to be suitable in practice in the automotive industries since the 1990s to answer quality and reliability issues and to provide an opportunity of predicting the future field failure behaviour. Using this information facilitates a more accurate prediction of required repair capacities or replacements like presented in Braasch et al. (2007). In this paper modified reliability prognosis models concerning the needs of the mobile industry are developed for the first time to provide assistance when predicting serial or end of life replacements.

The reliability prognosis model, which is based on the well known prognosis model of the automotive industry, uses field failure data being available during the warranty period. This assures the consideration of the real field stress in the further steps of the reliability prognosis model. Based on methods like the Weibull-Analysis or parameter estimation a model is presented that analyses the occurring field failures in connection with additional information such as the influence of registration or reporting delays. Furthermore, an approach has been developed concerning the influence of failure candidates (or failure aspirants) due to the censored warranty data (e.g., two years for electronic devices in Germany). By giving an example of a mobile phone which was sold in the Mediterranean region the steps of the reliability prognosis model will be displayed and the challenges will be shown. After presenting the prognosis model a verification of the model will be given. Therefore several mobile phones of different sales countries were analyzed. To check the accuracy of the model the existing field failure data was censored. Afterwards two prognoses were performed both with the uncensored and the censored data. The final step was to compare the results of both prognoses which should be nearly the same if the approach is suitable. As one can see in the following figure the theoretical function of the uncensored data given by the dashed line and the theoretical function of the censored data given by the black line are quite similar.

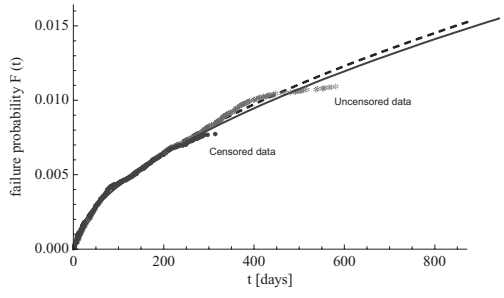


Figure 1. Comparison of censored and uncensored data.

REFERENCES

Braasch, A., Specht, M., Meyna, A. & Hübner, H.-J.: An approach to analyze software failure behavior of automotive telecommunication systems. Proceedings of ESREL 2007, Taylor & Francis Group, London, 2007.

Pauli, B.: Zuverlässigkeitsprognosen für elektronische Steuergeräte im Kraftfahrzeug. Shaker Verlag, 1998.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Risk of postoperative complications after surgeries: Laparoscopic versus open surgery

P. Jahoda & R. Briš
Department of Applied Mathematics, Technical University of Ostrava, Ostrava, Czech Republic

L. Martínek
Clinic of Surgery, University Hospital Ostrava, Ostrava, Czech Republic

ABSTRACT

Gross numbers presenting morbidity and mortality are often misguided and distorted because they do not consider the whole range of factors. For example the variability of health conditions of the evaluated sample of patients, conditions in the moment of surgery, the process of surgery, health conditions of the population and many more. Hence, they do not allow an objective comparison of the results achieved and the evaluation of recently implemented methods is problematic as well.

Therefore, in the beginning of the nineties the scoring system *POSSUM* was developed by Copeland et al. (Copeland et al., (1991)). Using logistic regression it allows to estimate the risk of complication for individual patients or groups of patients. The explanatory variables are the *physiological score*, *P*, (characterising the patient's health conditions) and the *operational score*, *O*, (characterising the surgical performance). In this model, the probability of postoperative complications is estimated by the relation

$$\pi(P,O)=\frac{e^{\phi(P,O)}}{1+e^{\phi}(P,O)}, \tag{1}$$

where

$$\phi(P,O)=-5{,}91+0{,}16P+0{,}19O, \tag{2}$$

The numbers of postoperative complications estimated by the original Copeland's model *POSSUM* were compared with the actual numbers collected by colorectal surgeries operated in years 2001–2006 in the University Hospital Ostrava. It was learnt that this model does not simulate the mentioned data sufficiently.

Considering the failure of above mentioned model to predict postoperative complications in our group of patients, we have created models of postoperative complications based on new explanatory variables. We have focused on the group of patients with diagnosis C20.

The values of statistical variables *Leucocytes* (*L*), and the *Operative Severity* (*S*) were proven statistically significant by laparoscopic surgeries. The values of statistical variables *Cardiac Signs* (*C*), and the *Operative Severity* (*S*) were proven statistically significant by open surgeries. Focusing only on these variables, we gained simple, nevertheless very accurate models $Os-POSSUM^2(l)$ for laparoscopic surgeries and $Os-POSSUM^2(O)$ for open surgeries.

$Os-POSSUM^2(l)$:
$$\phi(L,S)=-9{,}57078+3{,}04722L+0{,}892555S, \tag{3}$$
$Os-POSSUM^2(o)$:
$$\phi(C,S)=-2{,}07602+0{,}467884C+0{,}175036S.$$

Using the models $Os-POSSUM^2(l)$ and $Os-POSSUM^2(o)$, it is possible to choose an optimal operational technique for a particular patient, to minimize the risk of postoperative complications. Our recommendation is to use laparoscopic method if and only if the unequation

$$7{,}49476+0{,}467884C-3{,}04722L-0{,}715519S>0. \tag{4}$$

holds. We estimate, that choosing the right operational method, the number of postoperative complications can be reduced by 47,56% (but not more) in comparison with the worst scenario possible (all the patients operated with the unsuitable operational technique) and by 31,75% compared to the possibility, where the operational technique is chosen randomly in proportion 1:1.

REFERENCE

Copeland, G.P., Jones, D. & Wakters, M. (1991). POSSUM: a scoring system for surgical audit. *Br. J. Surg. 78*, 356–360.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The RAW concept: Early identification and analysis of product failure behaviour in the use phase

S. Bracke & S. Haller
University of Wuppertal, Department of Safety Engineering and Risk Management, Germany

ABSTRACT

The increasing complexity of product functionality and manufacturing process parameters often leads to complex product damage symptoms during the product life cycle. The damage causes must be detected at an early stage after product market launch to avoid further risk effects of the field failure modes. The very early identification of the damage causes requires new risk analysis approaches: The analysis of field data based on a small amount of field data is one excellent possibility.

Regarding to the outlined requirements the Chair of Safety Engineering and Risk Management at the University of Wuppertal developed the 'reliability analysis based on warranty databases (RAW)' concept for the early, economical and detailed statistical reliability analysis of guaranty and warranty databases. The application of the RAW concept has the following goals:

- Comprehensive mapping and analysis of component failure behaviour. Furthermore analysis of conducted product optimisations, climatic and regional influences (through customer usage) based on different production months/batches or different points of use.
- Detection of damage causes based on few field damage cases (small sampling sizes) at an early stage after market launch.
- Support the selection of appropriate actions for product improvement at an early stage is feasible.
- Technical analysis of damaged components based on a reduced amount of requested field components.

The elementary phases of the presented RAW concept are field data acquisition, graphical analysis as well as analysis with nonparametric and parametric statistics. Performing field data analysis at an early stage of the field monitoring phase leads to a small amount of data with respect to the damaged field components. For realising an early field data analysis, the RAW concept contains a combined application of nonparametric statistics. Nonparametric distribution-independent statistics allows significance analysis based on a small amount of data. More extensive data at a later time period enable the usage of parametric statistics. The analysing results based on nonparametric analysis are now verified and supplemented with the appendant parameter interpretation.

This paper outlines the effectiveness and use of the RAW concept in a close to reality case study of the automotive industry. The focus of the case study is the analysis of an electronic control unit including different failure modes and software updates. The results of the RAW concept application show significant identifications with respect to changes of the control unit failure causes, the failure rates, frequencies and trends. Therefore, a comprehensive evaluation of the control unit and software optimisations is feasible.

THEMATIC AREAS

Reliability and Safety Data Collection and Analysis,
System Reliability Analysis,
Automotive Engineering

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Trialling the use of safety performance indicators within Great Britain's railway industry

K. Thompson, J. Heavisides, G. Bearfield & D. Griffin
RSSB, London, UK

ABSTRACT

Safety critical industries traditionally rely heavily on failure and incident data to monitor performance and this is certainly true of the railway industry, with the key monitoring database, the Safety Management Information System (SMIS), primarily reporting safety related incidents. Such measures are referred to as 'lagging', 'reactive' or 'outcome' related. The consequence of this approach is that improvements or changes are only determined after something has gone wrong. However emerging practice in safety management asserts that effective management of hazards requires a proactive approach. Information to confirm critical systems (such as competency management, inspections and responding to audit findings etc.) are operating is also needed. These measures are referred to as 'leading', 'active' or 'activity-related'). Both types of measures need to be effectively integrated into an organisation's safety management system—a practice known as 'dual assurance'.

There is much emerging practice in the area of the application of safety indicators across a range of safety critical industries internationally. Progress in the practical application of the theoretical concepts has advanced as a result of the recommendations of the *Baker Report* (Baker et al., 2007) into the Texas City oil refinery accident which was published in 2007. In the United Kingdom (UK) the Health & Safety Executive (HSE) has published guidance (HSE 2006) on the development of process safety indicators for major hazard industries and this guidance has been successfully implemented in a range of different industries. At the outset of this research, within the railway industry in Great Britain (GB) the concepts had been considered by some organisations, however no clear and consistent practice had yet emerged.

Research was undertaken to survey and review good practice in the area of safety related indicator. The ultimate objective of which was to develop guidance and industry-wide processes to review, identify, analyse, report and act upon safety performance indicators. Although the outputs of the research are relevant to the whole rail industry, the specific focus for examples was taken to be Train Operating Companies (TOCs).

The research included completing a literature review, undertaking industry surveys, identifying and consideration of risk control measures for the purposes of developing safety performance indicators, developing industry guidance and trialling it with two TOC organisations. The overall process for managing safety performance indicators incorporated the good practice identified from the literature and surveys, how to prioritise and identify risk-based indicators, and characteristics that should be considered when formulating indicators. These were incorporated into industry guidance, the first draft of which is currently being trialled.

REFERENCES

Baker, J, et al. 2007. The report of the BP US refineries independent safety review panel.

HSE. 2006. Developing process safety indicators: A step by step guide for chemical and major hazard industries. Sudbury: HSE Books, ISBN 0 7176 6160 6.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Warranty data analysis for service demand forecasting: A case study in household appliances

O. Borgia, F. De Carlo & M. Tucci
"S. Stecco" Energetics Department of Florence University, Florence, Italy

EXTENDED ABSTRACT

The prediction of warranty claims is a major interest for the after-sales department of a manufacturing company, since all the goods produced are subjected to a warranty of varying duration. Indeed, the costs that the producer has to pay for the failures occurred during the warranty period, are one of the items that contribute to form the goods retail price.

This article presents a methodology to predict the number of technical assistance interventions during the warranty period. The study was developed relying the expertise gained by analyzing a product in the household appliances.

We carried out a case study to assess the quality of the approach. Starting from field data of technical support for products manufactured in a given year and using a simulation approach, we predicted the number of technical assistance interventions for the products of the following year.

The ability to predict the cost-related technical assistance during warranty enables to appropriately size the necessary resources and, therefore, to optimize costs. The advantages are twofold: on the one hand, you can reduce the selling price and, on the other, you can increase the contribution margin.

The study shows that it is possible to predict the demand for technical assistance during the warranty period for products manufactured during a given year, relying on knowledge of the technical data of the products made in the previous year.

The main difficulty in this type of analysis lays in the fact that, during its life cycle, a product exhibits a varying reliability that changes over time. Indeed, if we consider a generic product, we observe that, during the launch, it has a certain service request. With the passing of time, we can appreciate that reliability tends to increase by means of re-engineering and manufacturing refinements. This improvement is not obvious because other causes may, however, generate a deterioration of quality such as, for example, changing a supplier, or changing a component of the product.

As a result of what has been said, we can say that the characteristic parameters of the reliability function of the product (like the shape factor and characteristic life of the Weibull function), may vary over time.

The goal of this study is the prediction of service demand related to the warranty claims of a population of products.

It was decided to proceed with a simulation approach by developing a model to simulate the service calls of a products population, known its production profile. The main information used were the field data from the warranty calls.

The major strengths of the adopted approach are twofold.

First of all, the simulation model considers the latency period of the products. This is the time that elapses from the date of product manufacturing and the first use by the costumer. This analysis was the key to determine the correct time to the first failure.

The second distinctive feature of the study is the use of a variable failure distribution depending on the manufacturing date of the products. This type of approach was necessary since we had clearly identified the phenomenon of product maturity.

In general, the maturity of the product is due to a dynamic management of the product life which aims to a continuous improvement. It also translates into a dynamic behavior of the product service demand. It is obvious that this approach has required a thorough study of the field data aggregation criteria to determine the product groups with a homogeneous reliability behavior.

Specific business needs, which have arisen in the course of the study, and research interests will be developed in following studies with the goal of maintaining the current model performance in terms of predictive capabilities, despite of a strong reduction of the historically database.

This requirement is justified in the light of the continuous reduction of the products life cycle. So in the future works we are going to face a fast reliability prediction and not more the simply reliability prediction.

Risk and hazard analysis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A modelling framework for model based risk analysis

Jean-Marie Flaus
G-SCOP, Laboratoire des Sciences pour la Conception, l'Optimisation et la Production de Grenoble—UMR5272, Grenoble Cedex 1, France

ABSTRACT

Traditionally, risk analysis projects use a document based approach: the description of the system and the result of the analysis are expressed in a textual way or in drawings without an explicit semantics. The consistency and the relationships between documents are difficult to assess and it is rather difficult to extract and manipulate needed information for validation or for another purposes, or to capitalize knowledge.

An approach to overcome these limitations is to use a model based approach for risk analysis. This would allow to represent knowledge in a consistent manner, easy to manipulate and to transform.

In this work, we present an approach for model based risk analysis, which can be used with any classical methods such as PHA, HAZOP and FMEA.

The idea is to describe the physical system according to three views:

- the first one describes the structure (physical and functional),
- a second one, optional, with information about the behaviour when this is useful,
- and a third one to express the risk analysis result.

The first view, called SysFis, has three kinds of models blocks: systems, functions and resources: a *system* may be seen as an entity whose goal is defined by a set of *functions* which requires and/or consumes physical elements, called *resources*, to produce and/or acts on others resources.

From a system engineering model point of view, the SysFis modelling view uses function and resources that may be seen as two types of components used to describe two complementary aspects of the system: the physical and functional ones.

This view may be optionally completed by the behaviour view, called SimFis, which allows for the addition of variables and constraints in order to provide more details about some parts of the system. As the goal is to avoid modelling overhead to the risk analyst, this model view is optional and may be partial.

The result of the analysis is then expressed using the last view, called DysFis, which allows the representation of the abnormal behaviour of the system at a level of abstraction which is relevant for risk analysis. This view is based on model blocks defining abnormal events and rules for connecting them. A small set of abnormal events types has been defined. This model is related to the structuro-functional model and to the behaviour model. It allows to automatically generate tables for various risk analysis and various representations such as fault tree, consequence tree, bow tie diagram and to compute probability or severity.

A software tool, XRisk, has been developed to implement and to test this modelling approach. This tool allows to perform model based risk analysis and is able to generate, from a common representation, various risk analysis views such as PHA, FMEA, HAZOP, or MOSAR.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A linear programming approach to risk prioritization in FMEA

Pauli A.A. Garcia, Ilton C. Leal Jr. & M.A. Oliveira
Fluminense Federal University, Volta Redonda—RJ, Brazil

ABSTRACT

Risk analysis is an activity which is commonly done by reliability engineers and/or risk analysts from any industry. The results of a Probabilistic Safety Analysis (PSA) provides much information to make decisions about maintenance policies or about care to be taken over some critical points of a system (Fullwood, 2000). The purpose of a Failure Mode and Effect Analysis (FMEA), in a PSA, is to find and supply semi-quantified information about the different ways that the system can fail, and constitute relevant inputs to the system modeling (IAEA, 1992).

The data gathered through a FMEA should be considered in a decision making process concerning risk. The data which should have influence over the decision maker are associated with occurrence probability (O), severity of the respective effect (S) and with the potential to detect that something is going wrong. This potential is called detectability (D). (Bowles, 1998, Bowles & Bonnell, 1998).

Up to now, different approaches have been considered in turn to reduce the erroneous interpretation occasioned by the traditional Risk Priority Number (RPN) (Bowles & Bonnell, 1998, Bowles, 2003).

The traditional RPN consist of the product of the three criteria, i.e., RPN = O.S.D. These criteria are considered in an ordinal range, commonly, from 1 to 10, where greater the order worsts the case.

The main problem was the one associated importance of the severity criteria. For example, a failure mode with the following criteria, O = 1, S = 10 and D = 1 is considered less important than another one with O = 4, S = 4 and D = 4. The former have an RPN = 10 and the last one have a RPN = 64, which will be prioritized.

In the present work one proposes the use of the traditional constant return to scale DEA model (Charnes et al., 1978), considering an output approach. In this approach, the efficiency frontier identifies the improvements for each critical failure mode, enveloped by the frontier. To make the prioritization proposed by DEA more realistic, we will consider the effect of weight restriction, i.e., the importance of the criteria will be differentiated in turn to consider the relevance of the severity criteria. Without loss of generality one will considers equally important the occurrence and detectability. The severity will be considered more important than the others criteria simultaneously.

$$
\begin{aligned}
&Max\ h_0 = \sum_{j=1}^{S} u_j y_{j0} \\
&s.t. \\
&\sum_{i=1}^{r} v_i x_{i0} = 1 \\
&\sum_{j=1}^{s} u_j y_{jk} - \sum_{i=1}^{r} v_i x_{ik} \le 0, \forall k \\
&v_s - \left(v_0 + v_D\right) \ge 0 \\
&u_i, v_i \ge \varepsilon \forall i, j
\end{aligned} \tag{1}
$$

The obtained results showed that we can establish, effectively, a priority ranking between the failure modes. It was also showed that it is possible to identify how much each criteria index must be reduced in turn to improve the system under analysis.

REFERENCES

Bowles, J.B. (1998). The new SAE FMECA standard, In: IEEE *Proceedings of the Annual Reliability and Maintainability Symposium*, Anaheim, CA, pp. 48–53.

Bowles, J.B. (2003). An assessment of RPN prioritization in failure modes, effect and criticality analysis, In: *IEEE proceedings of Annual Reliability and Maintainability Symposium*, FL.

Bowles, J.B. & e Bonnell, R.D. (1998). Failure mode, effect and criticality analysis: what it is and how to use it, In: Topic in Reliability and Maintainability and Statistics, *Annual Reliability and Maintainability Symposium*, Anaheim, CA.

Charnes, A., Cooper, W.W. & Rhodes, E. (1978). Measuring The Efficiency of Decision Making Units, *European Journal of Operational Research,* n. 2, pp. 429–444.

Fullwood, R.R. (2000). *Probabilistic risk assessment in chemical and nuclear industries*, MA, Butterworth-Heinemann.

Intenational Atomic Energy Agency – (1992). *Procedure for conducting probabilistic safety assessments of nuclear power plants (level 1): a safety practice*. Safety Series No. 50-P-4, Vienna.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Ageing and life extension for safety systems on offshore facilities

S. Håbrekke & P. Hokstad
SINTEF Technology and Society, Safety Research, Trondheim, Norway

ABSTRACT

A large number of facilities on the Norwegian Continental Shelf are approaching or have exceeded their design life. Many fields, however, have remaining recoverable oil and gas reserves, so that life extension can be profitable. But in order to extend operation beyond the design life of the facility it must be assured that the safety integrity is maintained throughout a life extension period. This means that it is required to investigate the condition of structure, equipment, procedures and organisation, and also the compliance with requirements etc. for the entire facility.

So far, studies on ageing of offshore facilities have focused on main systems, such as structures and pipelines. The present paper in particular addresses ageing issues related to offshore safety systems, including Safety Instrumented Systems (SIS), during a potential life extension period.

It is a main objective to prevent that Life Extension (LE) will increase the probability of major hazards, such as for instance blowout, fire, explosion, ship collisions or structural collapse. To avoid major hazards, it is important to have control with the safety systems, the barriers, their state, and the risk factors influencing each barrier. Thus, to ensure the integrity of the entire facility throughout a possible life extension period, the main focus is on such systems and barriers. Each system should therefore be broken down into subsystems or components, following a barrier line of thinking. The focus is on physical barriers related to the actual equipment and barrier systems. In a complete analysis of ageing, the level of breakdown should proceed until we arrive at units with unique degradation mechanisms or to maintainable items. Typical barrier elements for offshore safety systems are power supply, logic, detectors and valves.

When LE is considered the main question is how to perform the process for deciding whether LE can be performed without compromising safety. The length of a possible LE period depends on the facility's ability to maintain the technical, operational and organisational integrity.

The first task is to identify all (possible) challenges related to ageing and future operation; incorporating the whole facility and all safety related systems and equipment on the facility. For instance, will there be any *changes* during a future operational period, resulting in challenges? Secondly, the risk related to these challenges should be analysed (for the entire LE period). Finally, a maintenance and modification plan to reduce the risk contribution from all equipment and systems must be prepared and implemented in order to maintain (or, if required, improve) the safety integrity and to comply with the current requirements.

Lack of knowledge about ageing and degradation mechanisms for certain equipment types, is relevant for safety systems, in particular ageing of electronic systems may be a challenge. Besides increasing failure rates due to e.g. material degradation, increasing demand frequency is important to be aware of during LE. Tripping the safety systems (either due to real demands or spurious trips) can increase as the entire facility ages. Also, Common Cause Failures (CCFs) are important for the life extension evaluations, in particular for redundant equipment. There are various types of dependencies, e.g. physical-, functional, location-/environmental-, plant configuration—or human dependencies. In general a CCF analysis should consider failures due to common causes/stresses.

Common ageing of various components and equipment on a facility during the LE period can possibly result in a common (sudden) increase in the failure rate. This means that the contribution from CCF, which often is the largest contributor to the total PFD compared to independent failures, may increase.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Applying a systemic model of accident within a system for treatment of contaminated materials

K. Hardy & F. Guarnieri
A.A. Center for Research on Risk and Crisis, Mines ParisTech, France

ABSTRACT

Contaminated sediments are a source of hazards to people and ecosystems because of the presence of toxic substances that can cause major natural disturbances. The situation of some contaminated sites is not without consequences on health, economics, politics or law.

Therefore, any approach to treatment of contaminated sediments must be accompanied by a hazard analysis approach in order to avoid any collateral damage on the entire system. Indeed, any manipulation of sediments contaminated always causes a release of contaminants into the environment. Furthermore, this manipulation exposes operators to numerous risks, mostly chemicals.

Thus, treatment of contaminated sediments requires a comprehensive approach taking into account the safety assessment and maintenance of a set of constraints in order to avoid accidents.

In this context, a solution is provided through the systemic accident model called STAMP (System-Theoretic Accident Modeling and Processes).

This model was developed by Professor Nancy Leveson, Massachusetts Institute of Technology (MIT), within the framework of socio-technical system to address a safety need for non-linear behavior.

This model does not consider an accident as a chain of events but as a problem of control within its structure. It allows the analysis of a system for reducing pollution by modeling its structure and its dynamic behavior.

STAMP model is a systemic model based on Bertalanffy's general theory of systems. This theory is not without limits to consider complex systems.

This article is organized into three sections:

– A presentation concerning the system of treatment of contaminated sediments
– A presentation of STAMP model and technology STPA
– An implementation of STPA on the processing system and a discussion of results.
– A presentation of limits of STAMP model.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Assessment of loss results by means of multi—criteria analysis

P. Suchardova, A. Bernatik & O. Sucharda
VŠB—Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

This paper discusses the results from the long–term research that focused on the assessment of major accident consequences using the MDCA approach. The research has been carried out in cooperation with industrial companies and includes modeling of potential extraordinary events affecting technological parts. Within previous research parts of the infrastructure that transport metallurgical and technical gases, gas—holder with coking gas and storage of the hazardous benzole were modeled and evaluated. This article presents these technological parts in detail.

The goal of this article is to demonstrate the usage of MDCA in a risk management area. This task is supported by a real case study which has been carried out in a metallurgical international industrial company situated in Moravian—Silesian region of the Czech Republic in the middle of Europe. This paper also discusses contribution of this analysis to the risk management area.

The proposed MDCA approach determines the consequences of major accidents where the goal is to evaluate particular serious accidents, to determine their order and their significance such as gas–holder, vessels, infrastructure and others.

The Figure presents the ranking value for five extraordinary accidents for stipulated criteria.

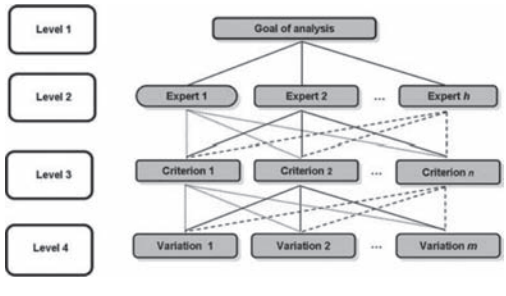


Figure 1. Multi—criteria decision analysis.

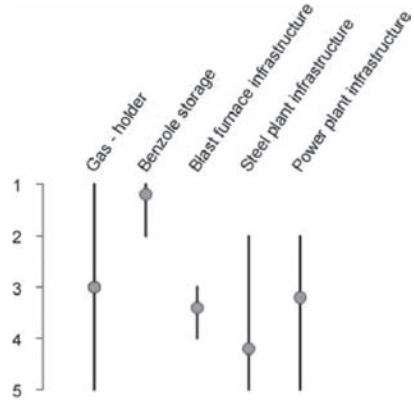


Figure 2. Range of rankings.

REFERENCES

Barron, F.J. & Barret, B.E. 1996. Decisions quality using ranked attribute weights, Management Science, 42.

Bernatik, A. & Libisova, M. 2004. Loss prevention in heavy industry: risk assessment of large gasholders. Journal of loss prevention in the process industries. vol. 17, DOI: 10.1016/j.jlp.2004.04.004.

Brutsaert, W. 1982. Evaporation in the atmosphere. Theory, history, and applications. D. Reidel, Higham, MT, USA.

Clemen, R.T. 1996. Making Hard Decisions, an Introduction to Decisions Analysis. Duxbury Press Belton, CA. 2nd ed. Company documents.

CPR (Committee for the Prevention of Disasters). 2005. Methods for the calculation of physical effects due to releases of hazardous materials: liquids and gases: yellow book. 3rd ed.

FERMA (Federation of European risk management associations). 2009. A risk management standard, <http://www.ferma.eu>.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Evaluation of regional risk analyses in Norway

O. Njå
University of Stavanger, Stavanger, Norway

G.S. Braut
Stord/Haugesund University College, Norway

K. Russell Vastveit
University of Stavanger, Stavanger, Norway

ABSTRACT

The regional, public system of governance in Norway is traditionally divided into 19 counties (including the capital Oslo which is a municipality as well as a county) and 430 municipalities. The highest ranking governmental representatives at the county level, the county governors, are tasked with carrying out county risk and vulnerability analyses. The purpose of conducting the assessments is the development of county risk pictures. Though the county risk and vulnerability analyses are mandatory the content, nature and process of the task have not been rigidly defined, thus the different county governors have solved the task in quite different ways. An aim of this project is to suggest topics that should be considered when describing the expectations and clarifying the formal requirements to such analyses.

This paper presents an evaluation of these regional risk and vulnerability analyses based on data collection done through a project for students at a master degree course in risk governance. The overall goals, organization of the risk analysis process, hazard identifications, risk modeling, data collection, risk presentations and the anticipated subsequent use of the CRAVAs have been the focus of the evaluation. There are many different ways to interpret the role of risk analyses in risk management. In this evaluation we have adopted Stephen R. Watsons 20 year old view on risk and risk analysis which we find should be the perspective that guides regional public risk governance. Watson says: "Probabilistic safety analysis should be interpreted as reasonable argument, rather than an objective representation of truth." This view may be seen as a request for dialogue and reflection about risk analyses.

At present we find that the risk analyses undertaken by the counties show a large degree of variation in terms of contents and comprehensiveness. They range from being analyses that show signs of being mandatory bureaucratic exercises, focusing on services provided by public bodies to analyses that are designed to influence and guide activities in entire counties. Despite the current large differences we find that such analyses can be important tools for county governors in their work to provide and implement strategies for developing county risk pictures. Based on our evaluation of the different risk analyses we suggest that a new approach to uncertainty assessment in the analyses is needed. This approach must encompass an openness to comprehending changes, a willingness to search for a better understanding of critical systems in the counties, and an understanding of the functionality of the systems, the intersections between them and the related vulnerabilities. Only making more specific requirements related to the format of the analyses and proposing questions to be answered will probably not be sufficient to ensure a more uniform approach to this task by the county governors. In addition we find that clarification of the role CRAVAs should play in county wide and municipal planning as well as the work done by the county governor is necessary.

The data that has been gathered and the broad discussions that have often taken place during the analyses offer good opportunities for continued learning. This learning should not only be seen as a process for increasing knowledge and competence, but also as a fundament for continuous updating of the analyses so that valid risk pictures can be presented to the different actors in the societal planning processes. If this is to become a reality a core requirement will be that the county governors should strive to establish a sound knowledge base for the CRAVA-process. This knowledge base must contain general scientifically based information in addition to knowledge about local conditions. Systems for gathering information and knowledge from the municipalities should be a part of this as the CRAVAs must not only present a top-down perspective.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fragment launching conditions for risk analysis of explosion and impact scenarios

R.G. Salhab, I. Häring & F.K.F. Radtke
Fraunhofer Ernst-Mach-Institute, Efringen-Kirchen, Germany

ABSTRACT

Explosives and impact are an often used tactic in terrorist events. For a quantitative risk analysis of such security threatening scenarios in particular the fragment hazard sources must be described. Examples for the generation of fragments are homemade bombs, vehicle born improvised explosive devices, contact detonations and building structures penetrated or perforated for example by fragments, bullets or rockets.

We present distributions that describe the initial launching conditions of the generated fragments or debris. Within risk analyses these distributions determine initial positions, velocities, directions and masses. They can be used to represent experimental, empirical-analytical and computational simulation data. We discuss the restrictions of the often used point source approximation, various normalization conditions and effects of discretizations of distributions. We also use multiple and higher dimensional distributions going beyond the standard point source approximation. The advantages of the distribution types are discussed for typical applications.

First of all a fundamental set of sizes needed for describing hazard sources as well as ammunition storage depots are introduced, which give an insight to the complexity of the problem of determining launching conditions of fragments or debris.

To simplify descriptions approximations and simplifying assumptions are presented. Often only based on these, analytical or numerical calculations are possible. Their advantages and their disadvantages as well as limitations are presented.

To specify launching conditions, the rotational symmetric fragment matrix is introduced, which is the most used structure in this field. Possible generalization and simplifications are discussed, which can also be used for determining debris launching conditions.

Analytical-empirical as well as experimental approaches for the determination of launching data of fragments and debris are described. Several distributions that in combination form an example for an analytical-empirical method are presented, as well as the arena tests (Zaker 1975; Hillstrom & Starkenberg 1998) as an example of an experimental approach. For fragments (Crull, jr. et al., 2009) and debris (Dörr, Gürke et al., 2004) different distributions are used, as their generation processes are significantly different.

Finally a projective coordinate system is given, which can be used for describing debris and fragment fluxes through specific areas without abandoning the assumption of a point source, see Figure 1.

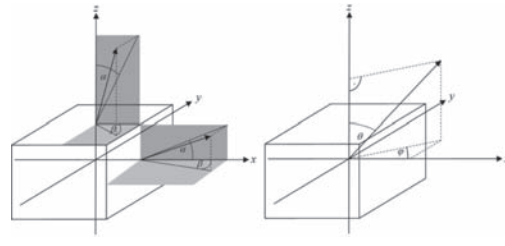


Figure 1. Left side: (α,β)-coordinates shown for the roof and one side of a structure. Right side: global spherical coordinates.

REFERENCES

Crull, M.M., M.M.S. jr & Hamilton, S.D. 2009. Methodologies for Calculating Primary Fragment Characteristics, *DoD Explosives Safety Board*.

Dörr, A., Gürke, G. & Ruebarsch, D. 2004. The Debris Throw Model DHP. *31st DoD Explosives Safety Seminar*, San Antonio, Texas, USA.

Hillstrom, W.W. & Starkenberg, J. 1998. Benchmark Tests for Fragmentation and Propagation Models, U.S. Army research Laboratory, Aberdeen Proving Ground.

Zaker, T.A. 1975. Fragment and Debris Hazard. Technical Paper 12, *Department of Defense Explosives Safety Board*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
 ISBN 978-0-415-68379-1

Improving reliability allocation in a complex repairable system using STRR allocation technique

W. Baun
UTC Power, South Windsor, CT, US

ABSTRACT

The task of allocating failure rates to components within a complex repairable system is executed early in a product development process in order to set reliability targets for those components. This allocation process is often accomplished versus more than one constraint, for instance to achieve an overall system-level failure rate target, λ_{sys}, and to achieve an overall system Life Cycle Unplanned Maintenance Cost target (LCUMC).

Traditional allocation methods leave it to the judgment of the analyst to decide how to allocate failure rate amongst the components. Presumably, there exists an optimum component allocation solution that would most effectively meet those goals. Because there are an infinite number of combinations of component failure rate allocations which could achieve the system-level targets, these approaches are somewhat unsatisfactory in that they leave the analyst to question if their particular allocation solution is a good one.

This paper demonstrates the application of an alternative allocation technique which employs genetic algorithms to find better allocation solutions—solutions which meet product reliability goals while attempting to minimize a metric called System Total Reliability Risk (STRR).

STRR is a measure of the aggregate risk inherent in the allocation solution, where risk is defined from the perspective of eventual product reliability and maintenance costs. It is the probability that the actual λ_{sys} is ultimately found to be higher than its allocation, and the consequences of that higher failure rate in the form of higher-than-expected LCUMC and λ_{sys}. It is also a measure of the degree of difficulty to achieving the proposed component failure rate allocations, given that different types of components generally have a limit to the best failure rate that can be achieved in practice.

The practical utility of such an approach is that it finds better allocation solutions—solutions which reduce the STRR, while still meeting the customer-driven reliability targets for λ_{sys} and LCUMC. The STRR approach can also reduce program risks by selecting an allocation that may be easiest to achieve in practice. Finally, the technique reduces the time required to complete the task of failure rate allocation, since the process is automated.

This paper outlines the STRR allocation method, demonstrates the application of this method to a real world complex repairable system of nearly 400 components, and compares the results obtained versus those from traditional allocation techniques.

REFERENCES

Baun, W. *Optimization of Component Reliability Allocation in a Complex Repairable System Using a System Total Reliability Risk Metric*. Proceedings of the 2009. ASME International Mechanical Engineering Congress & Exposition, November 2009.

Ebeling, C. *An Introduction to Reliability and Maintainability Engineering*; McGraw Hill: New York, 1997.

Konak, A., Coit, D.W. & Smith, A.E. *Multi-Objective Optimization using Genetic Algorithms: A Tutorial*. Reliability Engineering & System Safety, Volume 91, Number 9, September 2006, pp. 992–1007.

Levitin, G. *Genetic Algorithms in Reliability Engineering*. Reliability Engineering & System Safety, Volume 91, Number 9, September 2006, pp. 975–977.

Marseguerra, M., Zio, E. & Martorell, S. *Basics of Genetic Algorithms Optimization for RAMS Applications*. Reliability Engineering & System Safety, Volume 91, Number 9, September 2006, pp. 977–991.

OREDA, 2002. *Offshore Reliability Data*, 4th Edition, Published by OREDA Participants, Prepared by SINTEF Industrial Management, Høvik, Norway, 2002.

Reliability Information and Analysis Center (RIAC) Automated Databook, Version 2.20. IIT Research Institute, Rome, NY, 1999.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Managing inconsistency in safety analysis: An initial exploration

L. Sun & T. Kelly
Department of Computer Science, University of York, York, UK

ABSTRACT

It is typical for any system safety justification to rely upon multiple forms of safety analysis. It is unacceptable to have (unexplained) inconsistency between these models. However, inconsistency will commonly arise in safety analysis. Safety analysis is often conducted iteratively throughout the engineering lifecycle, using a variety of different techniques, and according to different viewpoints, boundaries and assumptions. Although engineering practice shows that it is difficult to eliminate these inconsistencies completely, it is necessary to understand how analyses can be inconsistent and what we can do to rationalize and justify the inconsistencies.

The usage of the term of consistency is very different according to its context. In this paper, we clarify and frame the working meaning of consistency in safety analysis in this study as the description of logic and data in safety analysis is in agreement with each other or hold some predefined relationships.

Then, a small-scale case study is introduced and the initial observations from a set of safety analysis results from different analysis groups are presented. The major findings from the case study include the inconsistent analysis structural data, the inconsistent language expressions, and the inconsistent content of the results. In addition, the limitations and features of the cases under study are analyzed.

On the basis of the clarification of the meaning of consistency and our direct observations obtained from the case study results, the following five possible organizing principles are explored to support the classification of the inconsistency in safety analysis: data elements required by the safety analysis methods; the location of inconsistency in safety analysis; the causes of inconsistency, the consequences of inconsistency; and the types of consistency checking rules.

Considering the variability and features of the organizing principles described, taxonomy for describing inconsistency in safety analysis is proposed. The primary perspective is from the location of inconsistencies in safety analysis that can manifest the concrete situations in which analysis inconsistencies exist. The second perspective is from the data elements in safety analysis results, which show the direct characterization of the potential differences that may emerge in the varied versions of safety analysis conducted by different people utilising diverse safety analysis techniques. After that, we explain the usage of the taxonomy regarding the inconsistency management and safety reviews. Future work is presented at the end.

REFERENCES

Amendola, A. 1986. Uncertainties in systems reliability modelling: Insight gained through European Benchmark exercises. *Nuclear Engineering and Design*, 93, 215–225.

Everdij, M.H.C., Blom, H.A.P. & Kirwan, B. 2006. Development of a structured database of safety methods. *NLR-TP-2006-687*.

Haley, D.T., Nuseibeh, B., Sharp, H.C. & Taylor, J. 2004. The conundrum of categorising requirements: managing requirements for learning on the move. *Requirements Engineering Conference, 2004. Proceedings. 12th IEEE International*.

Kolovos, D.S., Paige, R.F. & Polack, F.A.C. 2008. Detecting and repairing inconsistencies across heterogeneous models. *Software Testing, Verification, and Validation, 2008 1st International Conference on*.

Nuseibeh, B., Easterbrook, S. & Russo, A. 2000. Leveraging inconsistency in software development. *Computer*, 33, 24–29.

Nuseibeh, B., Kramer, J. & Finkelstein, A. 1994. A framework for expressing the relationships between multiple views in requirements specification. *IEEE Trans. Softw. Eng.*, 20, 760–773.

Rouhiainen, V. 1992. QUASA: A method for assessing the quality of safety analysis. *Safety Science*, 15, 155–172.

Straeten, R.V. 2005. Inconsistency management in model-driven engineering. *Department of Computer Science*. Vrije Universiteit Brussel, Brussel, Belgium.

Suokas, J. 1988. The role of safety analysis in accident prevention. *Accident Analysis & Prevention*, 20, 67–85.

Taylor, J.R. 2009. The QARQ project. Taylor Associates ApS, http://itsa.dk/default.htm

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

New approach to analysis of falling objects in the offshore petroleum industry—operational categorization of events

J. Seljelid, S.A. Kvalheim & O.M. Nyheim
Safetec Nordic AS, Trondheim, Norway

J.E. Vinnem
Preventor AS/University of Stavanger, Stavanger, Norway

ABSTRACT

The Trends in Risk Level project initiated in 2000 by the Norwegian Petroleum Safety Authority (PSA) aims to monitor the risk level development on the Norwegian continental shelf. An extensive database containing 1300 descriptions of incidents of falling objects in the petroleum industry between 2006 and 2010 have been analysed based on the initiating event categories developed in the BORA (Barrier and Operational Risk Analysis) project. The BORA categories were modified to fit events of falling objects, using a sample of 100 event descriptions from the database. The remaining 1200 events were categorized using the new categories. The aim of the project is to identify and validate operational categories that are suited to inform the industry of specific hazards connected to common offshore work processes. The complete procedure of category development, testing and results are presented and discussed in the paper.

The Risk level project has established a large database of incidents with falling objects from cranes, in the derrick and on the drill floor, from movements of equipment in the process areas as well as from various scenarios where objects may fall, such as during erection of scaffolding. The paper gives an overview of causes of falling objects in the work processes related to:

- B_: Drilling and well activities.
- K_: Crane related work processes.
- P_: Processing related work operations.
- G_: Work processes not related to drilling, well, crane or process operations.

Based on the generic main categories in BORA (Vinnem et al., 2007), a set of sub-categories was developed through an exploratory review of incidents. The categories were clarified through discussion and then validated in a new sample through a blinded peer review. Inter rater agreement of 26 initiating causes of 29 reviewed was judged to be satisfying, and the categories were applied to the whole data set.

The main causal categories applied to the data material were:

- A: Technical degradation or failure
- B: Human activity, introducing latent hazard
- C: Human activity, immediately triggering an incident
- E: Design
- F: External conditions

Category B and C together constitute situations where some sort of human activity is taking place and it may be noted that this comprises 44% of all fallings objects. It is further shown that fallings objects due to external conditions, category F, represents 29% of the total followed by technical failures (19%). A detailed picture of the distribution of causes and sub categories of causes in the earlier described work processes is presented in the paper.

REFERENCES

Hare, J. & Johnson, M. 2009. Underlying causes of offshore incidents. HSE, Crown copyright.

Health and Safety Executive (HSE) (2005); Accident statistics for Floating Offshore Units on the UK continental shelf 1980–2003, Delivered by DNV.

Health and Safety Executive (HSE) (2007); Accident statistics for fixed offshore units on the UK continental shelf 1980–2005, Delivered by DNV.

Haugen, S., Vinnem, J.E. & Seljelid, J. 2011. Analysis of Causes of Hydrocarbon Leaks from Process Plants, presented at SPE European Health, Safety and Environmental Conference in Oil and Gas Exploration and Production held in Vienna, Austria, 22–24 Februrary 2011.

Sparrows Offshore LTD for the HSE (2000); Lifting equipment project. Offshore technology report – OTO 2000 024.

Vinnem, J.E., Bye, R., Gran, B.A., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J. & Vatn, J. 2011. Risk modeling of maintenance work on major process equipment on offshore petroleum installations, (submitted for publication).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

On software interoperability in accident consequence assessment

S. Contini, L. Fabbri & V. Matuzas
European Commission, Joint Research Centre, Ispra, Italy

M. Binda
THS Informatica, Besozzo, Italy

ABSTRACT

The Interoperability of different risk analysis software tools is a very important aspect that would strongly and effectively support the work of safety authorities in their reviewing activity of safety reports for Seveso-type installations. This reviewing activity could indeed be not very straightforward if the models and software tools used by the authority are different from those used by the operator of the industrial facility under scrutiny.

Software interoperability has recently been addressed in many application fields and it consists of the definition and the recognition of a common data format for data exchange amongst different software, which are intended to perform similar tasks and functions. This would clearly allow the use of the same set of input data and facilitate a lot the comparison of the software output and the associated results. In the case of risk analysis, software interoperability would facilitate the dialogue and accelerate the consensus building between the manufacturer and the licensing authority. Moreover, it would be of great benefit also to model developers and software developers.

Some initiatives in this direction have already been launched in the nuclear sector. The "Open Initiative of Next Generation PSA Software" is an important activity to advance the state of the art in methodologies and tools for the probabilistic analysis of nuclear installations. A "Model Representation Format for Probabilistic Safety Assessment"—based on Fault Trees and Event Trees—was developed. A major task of this initiative was the definition of a common format for data exchange and the execution of a series of experimental tests on a number of software tools for PSA.

A first attempt to study the interoperability among accident-consequence tools (fire explosions, dispersion of toxic substances into the environment), used in the chemical sector, was performed by the authors. The consequence assessment represents a very critical phase in the risk analysis process of Seveso-type installations.

A first prototype of a common data exchange format was developed and tested on a number of commercially available software tools. Even if this preliminary study did not touch all aspects of the problem, it allowed addressing some of the main issues associated with the definition of a common data format.

The paper will describe the reasons for the need of a standard format in risk analysis, the results of the project and possible future extensions.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Risk assessment of dropped and dragged anchors to offshore pipelines

Luiz Fernando Oliveira & Darío Gusovsky
DNV, Paris, France

ABSTRACT

Dropped and dragged anchors are among the dominant causes of potential external damage to subsea pipelines in general. There are records of several accidental events of anchor damage to offshore pipelines in the North Sea area reported in the UK-HSE PARLOC database (UKOOA 2003). The pipeline damage caused by such events varies from simple scratching of the external coating to complete rupture of the pipeline. The associated consequences may vary from large expenditures with stoppage and repair of the pipeline to significant loss of lives in case of rupture of a gas pipeline near a populated offshore installation and severe environmental problems in case of rupture of a large oil pipeline.

This problem has already been studied in some papers in the open literature (Kim, B.M. 2005, Rességuier, S. et al., 2009). In this paper a comprehensive methodology for the quantitative risk assessment of dropped and dragged anchors to offshore pipelines is presented which makes use of existing AIS ship tracking data for defining trajectory and crossing frequency, distribution of ship and anchor types, emergency anchoring conditions, anchor impact energy, damage mechanisms, pipeline mechanical characteristics, soil properties and conditional probability of damage levels.

An application is presented for the case of a 24" oil pipeline from an offshore platform to an onshore terminal. The pipeline runs through an area of intense and varied ship traffic. Results are presented per pipeline kilometer (kp) and compared to typical risk tolerance criteria used by international pipeline operators. the pipeline.

The anchor damage to the subsea pipelines are divided in two types of interaction mechanisms: 1) damage caused by dropped anchors, and 2) damage caused by dragged anchors.

Damage caused by dropped anchors occurs when a passing vessel drops an anchor and it directly hits the pipeline leading to a certain degree of damage. On its turn, damage caused by a dragged anchor occurs when a passing vessels drops an anchor and drags it across the pipeline. This can bring damage to the pipeline by two different reasons: a) the mechanical damage caused when the dragged anchor hits the pipeline, and b) the mechanical damage caused when the dragged anchor hooks the pipeline and drags it because of the continued ship motion.

The risk to the pipeline is represented here by the frequency of different damage levels (minor, moderate and major) as proposed in DNV RP-F107 (Det Norske Veritas 2001). This frequency is calculated as the product of two terms: the frequency of interaction and the conditional probability of a damage level given an interaction.

The analysis of obtained results indicates that in addition to the frequency of crossing ships, the resulting risk level depends very much on the relative dimensions of the ship anchors and those of the pipeline, mainly because of the predominance of the hooking mechanism by dragged anchors.

REFERENCES

Det Norske Veritas, DNV RP-F107, "Risk Assessment of Pipeline Protection", March 2001.

Kim, B.M. "Upper Bound Analysis For Drag Anchors In Soft Clay", PhD Dissertation, Texas A&M University, 2005.

Rességuier, S. et al. "Assessment of Trawl Board and Anchor Penetration in Different Soils for Use in Selection of Burial Depth to Protect Submarine Cables or Pipelines", OMAE 2009, Honolulu, Hawaii, USA, June 2009.

Spouge, J. "Guide to Quantitative Risk Assessment for Offshore Installations", Centre for Marine and Petroleum Technology, Publication 99/100, 1999.

UKOOA, "PARLOC 2001: The Update of Loss of Containment Data for Offshore Pipelines", prepared by Mott MacDonald Ltd for UKOOA and the Institute of Petroleum, 5th Edition, July 2003.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Safety assessment methodology for a UAV development program

Celik Sirma
TAI—Turkish Aerospace Industries, Inc, Ankara, Turkey

ABSTRACT

Risky missions and pilots' physiological limits render Unmanned Aerial Vehicles (UAV) advantageous in both civil and military operations. With the rise in their usage, UAVs started to share the civilian airspace with manned aircrafts. Resultantly, people on other aircrafts and populated areas started to be endangered. Even though there are some rules for UAVs flying in the civilian airspace, they are still considered as a potential for mid-air collisions and uncontrolled crashes. In either case, catastrophic conditions are possible. This is the main reason of why safety issues of UAVs are popular and important.

Safety analyses of the UAVs are more serious than those of manned aircrafts, since these intelligent systems comprise highly complex systems such as autopilot, sensors, airframes, and embedded computing platforms. Ground systems, controlling software(s) and data links make system safety analyses more challenging when compared with conventional aircrafts' analyses. Furthermore, failures of UAVs are harder to identify due to lack of pilot sensing (such as noise, smell, vibrations etc.). There are several systems which the pilot is the primary means to sense the failure such as ice, fire etc. For UAVs, failure cases can lead to more critical repercussions since they may not be detected in a timely fashion.

Therefore, it is important to define appropriate safety objectives and requirements, and decide on the process. There are several regulations and study groups for UAV safety issues. However these regulations are too general such that they enclose all types of UAVs. Thus, indigenous and innovative approaches need to be carried out during the safety analysis of the UAV design process, according to the operational areas of the UAVs.

This paper highlights system safety analysis process implemented during the design phase of a Medium Altitude Long Endurance (MALE) UAV. Since available regulations do not completely meet the needs, additional rules are applied and these supplementary rules are hereby described. Applied standards, participants, system safety process sub-contractor management for safety program, analysis details, and tools are illustrated. Results of the study are explained and main differences in approach are explained.

This paper was prepared aiming to be a guide for future UAS safety studies.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Towards an integrated risk model for hydrocarbon industry operation

B.J.M. Ale, D. Hanea, C. van Gulijk, P.-H. Lin, S. Sillem & P. Hudson
Technical University Delft, Safety Science, The Netherlands

ABSTRACT

The recent blow-out and subsequent environmental disaster in the Gulf of Mexico have highlighted a number of serious problems in scientific thinking about safety. One of these is that our current thinking about how accidents happen, and all the management systems based on that approach. This is particularly clear in the case of what can be described as low-probability high-consequence accidents which, while quite rare, do not appear to be reducing in frequency unlike simpler and higher frequency personal accidents. The suggestion is that linear and deterministic models of accident causation are insufficient to catch the residual factors and their interactions.

The current development builds on the earlier developments in the IRISK, ORM and CATS projects to connect the descriptions for management, human behaviour and technology into a single framework that allows a more in depth analysis of the interdependencies. Probability *distributions*, rather than simple bifurcations, are used to take account of the wide range of context-dependent factors that can ultimately result in disaster. This novel approach to probabilistic models, based on Bayesian Belief Networks, has already been successfully applied in civil aviation and developed a rigorous framework capable of being applied to other high-hazard industries.

To develop the human behavior model the overall context has been examined within which risks are taken by organizations given a license to operate by regulatory bodies. Perceptions of risk appear to be misaligned between the top and the bottom of organizations and there is a clear need to develop a common understanding, between executive management and those performing the actual operations. A well motivated theoretical framework has been developed to allow the move from hindsight to foresight in the broad area of risk.

Specific attention is given in the development to the incentive structure of operators, staff and managers, which in the previous models was indicated more generally by motivation and conflict resolution. An incentive structure represents an empirical framework for an organisation which characterises the relationship between specific behaviours of employees and the probabilities of receiving various incentives.

The work reported here was aimed at a proof of concept of the approach at two sites of the same company.

This paper described the initial preparatory steps towards an integrated model for risk model for the risks of hydrocarbon industry operation. It feasibility of basing this model on previous work in the WORM project and the Bow-Tie analyses and using the BBN approach developed is CATS is shown.

The expectation from defense in depth thinking, that adding an extra barrier will always reduce overall failure rates may not be valid. The failure rate of this extra component is in part influenced by the same managerial mechanisms that influence the probability of failure of the existing safety systems and the addition of extra barriers may increase the isolation of operators from the reality they are controlling and even make failure to detect (one of the necessary defenses) less likely.

The initial analysis shows that such common cause failures can be adequately modeled in the BBN system, without the need for artificial non-model correction factors.

This does not take away the considerable uncertainties in the numerical evaluation that still exist and need further analyses, especially for the cases in which large investments are under consideration at the one hand, and large negative outcomes could be the unfortunate result on the other.

Even though these numerical uncertainties exist, the comparison between different policies can be made on a much sounder basis, recognizing the overarching effect of human behavior, on which the management of the company has a large, but not necessarily determining influence.

The work was fully funded by Royal Dutch Shell plc.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Towards CFD fire modelling applied to quantitative risk analysis

S. Vianna, K. Shaba, J. Pujol & A. Garcia-Sagrado
Det Norske Veritas, Energy Solutions, London, UK

L.F. Oliveira
Det Norske Veritas, Energy Solutions, Paris, France

ABSTRACT

Fires on offshore platforms contribute to a significant part of the overall risk. Nevertheless, the methodologies that are currently used to estimate fire risks, impairment of safety functions and design of fire protection and mitigation means may be coarse and based on subjective opinions and standard solutions. Prediction of fires and radiation impact could be performed using free field models. These models are based on fires in open terrain, and work fine for the far-field which is a typical situation of interest for most onshore installations. However, in an offshore module, the fire is constrained by walls and decks and confinement which will completely change the location and impact of the fire. The free field models usually apply constant surface emitting powers from the flame surface. This radiation flux is largely varying dependent on the flame thickness and temperature, causing the free field model to have a considerable uncertainty compared with a more detailed CFD (Computational Fluid Dynamic) model. Figure 1 shows the fire dynamics comparison with experimental data for two different numerical approaches. It can be noted a good agreement with experimental data.

After Piper Alpha accident in particular, the utilisation of CFD has become reality. An example of CFD combined with risk analysis techniques can be found in Vianna (2005). CFD (Computational Fluid Dynamics) has been combined with risk analysis techniques in order to provided a better understanding of the risk and help on its management. Gas dispersion, gas detector optimisation, explosion modelling, toxic release are some of the analysis which have been performed with CFD combined with risk analysis approach (Oliveira & Vianna (2005), Vianna & Cant (2010)). The fire modelling is also an important aspect of the risk. The assessment of impairment of escape routes, temporary refuge, structural collapse and risk analysis itself are some of the areas in which accidental fire modelling has played a key role Vianna & Huser (2010). The present paper compares the findings from fire modelling using RANS (Reynolds Averaged Navier-Stokes), LES (Large Eddy Simulation) and far field models with experimental data and among themselves.

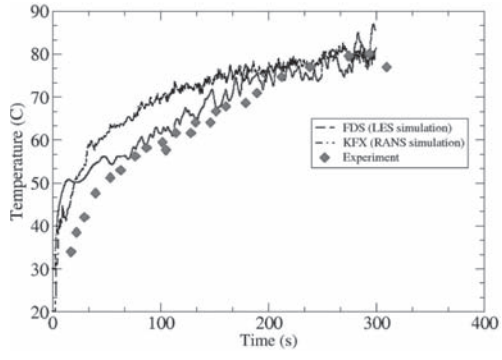


Figure 1. Fire dynamics comparison with experimental data.

REFERENCES

Oliveira, L.F.S, H.A. & Vianna, S. (2005). Cutting costs through detailed probabilistics fire risk analysis using cfd. *CFD Oil. Rio de Janeiro - Brazil*.

Vianna, S. (2005). Flacs explosion calculation combined with neptune for offshore risk assessment. *GEXCON Risk Conference. Milan - Italy*.

Vianna, S. & Cant, R. (2010). Modified porosity approach and laminar flamelet modelling for advanced simulation of accidental explosion. *Journal of Loss Prevention in the Process Industries. 23*, 3–14.

Vianna, S. & Huser, A. (2010). Fire cfd modelling applied to offshore design. *FIRESEAT 2010 - Fire Safety Engineering in the UK the State of the Art 1*, 65–76.

This page intentionally left blank

Risk governance

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An evaluation of the risk governance of civil aviation during the 2010 volcanic ash cloud

H. Veland & T. Aven
University of Stavanger, Stavanger, Norway

ABSTRACT

In this paper we evaluate the European authorities' handling of the 2010 volcanic ash cloud originating from the eruption of the Icelandic volcano Eyjafjallajökull. The evaluation is based on a comparison of the actual risk management against established principles and criteria for risk governance (management) as well as a set of risk governance deficits developed recently by the International Risk Governance Council (IRGC). Risk governance deficits are defined as deficiencies (where elements are lacking) or failures (where actions are not taken or prove unsuccessful) in risk governance structures and processes. These principles, criteria and deficits relate to the assessment and understanding of risks, including the collection and development of knowledge, and to the acceptance of responsibility and the taking of action in order to manage risk. In the paper we specifically address the assessment and treatment of uncertainties, and the use of the cautionary and precautionary principles.

Our initial hypothesis was that the actual risk governance was, to a large extent, in compliance with defined principles and criteria of good risk governance. In the evaluation, we focused especially on the handling of uncertainty, and on three aspects of risk governance relevant for this case: available factual knowledge about risks, the designing of effective risk management strategies, and how dispersed responsibilities were dealt with.

A recognized lack of scientific knowledge existed prior to this volcanic eruption: namely, on the ash concentration levels for safe flying. We have argued that in a wider decision-making perspective, the available knowledge and related uncertainties should be seen in relation to the actual risk management strategies implemented at that time. In the period prior to the Eyjafjallajökull eruption, a strict cautionary/precautionary approach was maintained as a strategy to handle the uncertainties/risks. When new knowledge became available during the volcanic eruption, the policies were revised to allow aircraft operations under specific, well-defined conditions.

We argue that there was a deficit of risk governance in the dealing with dispersed responsibilities in the time period prior to the volcanic eruption. This became apparent in the first period of the 2010 volcano eruption, when national authorities were paralysed, i.e. unable to respond effectively because it could lead to diversion from the internationally established guidelines that recommended avoiding all flying in airspace potentially contaminated with volcanic ash. During the eight days of the first intense phase of the eruption, the European Commission took an initiative to coordinate the national authorities' response to the crisis, resulting in a new set of harmonized and differentiated guidelines for risk assessment and risk management.

The first priority of civil aviation policy is to ensure safety. Going back to the first reported encounter in 1982, no fatal accidents have been registered from flying in airspace contaminated with volcanic ash. This could be seen as a testimony of the authorities' successful handling of the specific risks for civil aviation during the 2010 Icelandic volcano ash cloud, and for the handling of historical volcanic ash cloud incidents in general. However, there have been several close calls, and the international civil aviation community still has several major issues to resolve in order to further improve the response of future volcanic ash cloud incidents.

Nevertheless, the overall conclusion of our evaluation remains that the actual risk governance (management) in this case was, to a large extent, in compliance with the defined principles and criteria, and few severe deficits were identified. We cannot see that the massive level of criticism directed at the authorities was justified.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Regulatory response to hazards. Case studies from the Norwegian petroleum industry

P.H. Lindøe, O.A. Engen & Anita Moen
Faculty of Social Science, University of Stavanger, Norway

ABSTRACT

For some years new principles of risk regulation has been introduced as alternatives to detailed prescriptive regulations. Enforced self-regulation, where part of the regulatory process is delegated to the industry was introduced in the 1980s. This regulatory regime implies a process of negotiation and interpretation among the regulator and regulated regarding risk assessment, norms and safety practice. The purpose of this paper is to give a better understanding of what factors that may influence the outcomes of this process. An analytical framework including risk images and hazardous identification, arenas of negotiations and discursive practice is introduced. This framework is tested against three case studies (1) Hazardous workload, (2) Chemical Hazards and (3) Technical assessment of platform. The findings from the three cases are summed up in figure below.

The cases illustrate how diverse risk problems require different solutions, procedures and implies different amount of stakeholder involvement. The more complexity and ambiguity, the more involvement is seemingly required to manage risks. Ordinary and traditional risk problems are usually best handled using an instrumental discourse among agency staff, directly affected organization and enforcement personnel. When uncertainty and complexity increases and disputes about values or consequences arise, a discursive practice concerning risk is required.

The model promotes "discursive aspects" of risk regulation. A discursive practice concerning risk may confront sloppy and ignorant attitudes at local levels and challenge the actors' attitude towards responsibility. Trust and legitimacy is embedded in the organizational structure and in the relationship that characterizes by the affected agents. Decision making is a result of negotiation, and new regulations are prepared and implemented according to consensus between the regulators, organizations and stakeholders. The organizations' reactions to the decision making processes depend on whether the choices meet the institutional identity. All involved actors will try to have influence on priorities, and the decisions are judged according to whether they are recognized as rational, effective

	Hazardous work-loads	Chemicals hazards	Acknowledgement of compliance
Socio-economic factors	Minor groups of workers with low status. Industry argues on that high cost and disputable benefit	Minor group of workers belonging to low status service providers. Limited cost of improvement.	Regulatory issue to be solved by coordination of actor with unlike power basis
Risk images and hazard identification	Working hours offshore go far beyond reasonable and safe limits. Lack of research	Assessment of exposure hampered by lack of information, measurement and long term effect of health problems	Assessment according to well defined technical standards
Discursive practices	Controversies between industry and regulator concerning cost and benefits. Unlike alliances between unions, research communities and regulators.	A process of muddelling-through and continuous discussion between regulators, unions and industry.	Several arenas for co-operation and discussion between governmental and industry actors across national borders
Outcomes	Unsolved dispute. Possible solution is more prescriptive rules and reduced flexibility in the regime.	Hazards has gradually been reduced by a combination of enforced regulation, technical design and effort among the stakeholders	Pragmatic solution where AoC represents an exception from the main principles of the offshore regime.

and fair. However, this form of regulative practice, accounting for social and cultural values when designing and implementing new routines and procedures, may lead to less responsibility aversion by the actors involved. Accordingly, rules and procedures with local involvement gain greater legitimacy among the participants but also demand a higher willingness to take responsibility for the working conditions.

The article proposes a process of regulatory practice to a larger extend is adjusted to the character of the risk and hazard of the working conditions.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The effect of the Deepwater Horizon accident on the Norwegian debate concerning future oil and gas development in Lofoten and Vesterålen

I.L. Johansen
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

In April 2010, the blowout of the oil rig Deepwater Horizon in the Gulf of Mexico caused the loss of 11 lives and the largest quantity of oil spill ever experienced. The objective of this paper is to address how the accident has affected the ongoing debate concerning whether to open up for oil and gas development in the vulnerable areas of Lofoten and Vesterålen (LoVe) in the North of Norway, and the implications for risk assessment to inform the decision process.

For almost ten years, the debate on LoVe has engaged a wide range of stakeholders from ministries and oil companies to environmental groups. The Deepwater Horizon accident has made visible the opposing stakeholders, who have used the event to argue against development and the adequacy of risk assessment to inform decision making. Proponents, on the other hand, have accentuated the differences which limit its relevancy to North Norwegian conditions. Those who have wavered inbetween have generally maintained their ambivalence in quest for more knowledge. The perceived relevancy of Deep-water Horizon to LoVe is thus shown to correlate with the stakeholders' fundamental reasons of interest in the decision, which can be intuitively arranged on a value spectrum from environmental preservation to value creation as shown in Figure 1. A clear connection is indicated between stakeholder values and the conception of risk; while the opposition emphasizes consequences, proponents accentuate probability, and the political midst highlights uncertainty.

Even though the Deepwater Horizon accident has served to confirm rather than alter the prior positions, it has definitely affected the arguments, momentum, and dynamics of the debate. Through the mechanisms of social amplification of risk, an information gulf has arisen as stakeholders use values as pervading benchmarks for selecting and interpreting risk information to strengthen their positions. Ultimately, this has brought the parties farther way from a shared understanding of both the quality and quantity of major accident risk in LoVe.

The Deepwater Horizon accident has also seemed to alter the views on what makes a suitable strategy to risk evaluation and the role of risk assessment in the decision process. Apparently, the accident has masked what this author considers to be the two defining challenges of the situation; complexity and ambiguity. Instead, the debate has been reframed as a problem of uncertainty, at the risk of reducing value conflicts to a mere factual level of risk debate while leaving analytical disagreements still unresolved.

The study concludes that the Deepwater Horizon accident has jeopardized the extent to which risk assessment is to be accepted as decision support, by increasing skepticism, pragmatism, and the gulf of knowledge and understanding. In order to regain analytical integrity in a debate which is necessarily politically laden, this calls for explicit attention to problem framing and establishment of scientific conventions through broad deliberation prior to risk assessment.

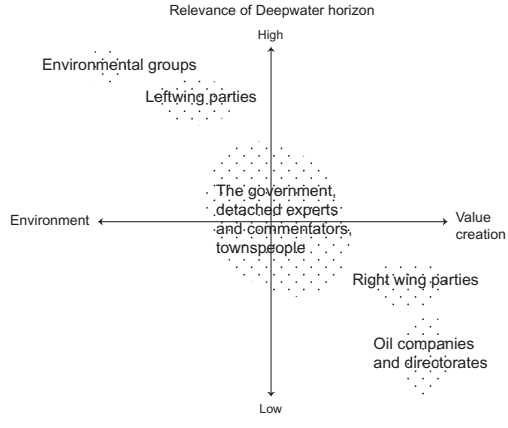


Figure 1. Principle drawing of the correlation between values and the perceived relevance of Deepwater Horizon.

Risk management

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Benchmark study on international functional safety standards

F. Massé
Ineris, Verneuil-en-Halatte, France

R. Tiennot
Ligeron, Saint-Aubin, France

J.P. Signoret
Total, Pau, France

P. Blancart
PSA Peugeot Citroën, La Garenne-Colombes, France

G. Dupin
RATP, Paris, France

L. Marle
IMdR, Gentilly, France

ABSTRACT

The practice in use for the development and the evaluation of safety related systems is to follow the requirements of international functional safety standards. Thus, the quality of these standards and the way they are applied are particularly critical. That is why several partners (Total, PSA, RATP, INERIS) decided to realize a study on this subject in the framework of the IMdR (French Risk Management Institute). This study was realized by Ligeron. The motivations and the main results IMdR Project P08-2 are given in this paper.

In order to develop and evaluate their safety related systems, various industrial sectors have developed their own standards. These standards were defined by taking into account sector-based practices and constraints and without reference to a common state of the art. Consequently, there are strong disparities between the standards and often important inconsistencies with the state of the art in safety and reliability engineering.

Each standard defines its own multiple degree qualification scale like SIL for the IEC 61508, ASIL for the ISO 26262, DAL for DO 178, Category for machines. Each one introduces its specificities and leans on different hypotheses. The Different semantics and definitions are in use and similar terms have different meanings depending of the standard in which they are used. Furthermore the principles, the underlying hypotheses or the simplifications introduced are sometimes ambiguous or scientifically questionable.

In front of those difficulties of interpretation and use, it appears necessary to list the standards, make a critical analysis and compare them in order to identify the convergences, the main differences and the possible weaknesses.

The following issues have been studied:

Identification of existing safety standards
Feedback on standards application
Standards comparison and critical review
Vocabulary status

The results of the identification and analyze of functional safety standards of main industrial sectors provided:

A vocabulary comparison and analysis
The qualification criteria
The conditions for standards applicability
The benefits and limitations of each standard
The relevance of each standard with regards on technologies and operation philosophy.

In this paper, the safety lifecycles and the main requirements of the IEC 61508 and three standards derived from IEC 61508 are presented. Then, a few vocabularies issues are summarized. Finally, the main qualities and weaknesses of these standards are discussed.

REFERENCES

Brissaud, F., Barros, A., Bérenguer, C. & Charpentier, D. 2010. Design of complex safety-related systems in accordance with IEC 61508 In: R. Bris, C. Guedes Soares, S. Martorell (eds), *Reliability, risk and safety: theory and applications*, *proc of the European Safety and Reliability Conference,* Prague, 7–10 September 2009.

Gentile, M. & Summers, A.E. 2008. Cookbook versus performance SIS practices. *Process Safety Progress*, 27: 260–264.

IMdR Project P08-2, 2011. *Benchmark study on safety instrumented systems safety approaches*.

Langeron, Y., Barros, A., Grall, A. & Bérenguer, C. 2008. Combination of safety integrity levels (SILs): a study of IEC61508 merging rules, *J Loss Prevent Process Ind* **21**, pp. 437–449.

Lundteigen, M.A. & Rausand, M. 2010. Reliability of safety instrumented systems: Where to direct future research?. *Process Safety Progress*, 29: 372–379.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Correlating risk and innovation management in projects

F. Marle, M. Jankovic & G. Turré
Ecole Centrale Paris, France

ABSTRACT

Innovation management is inherent to many projects. Namely, the competitiveness of a company is partially given by its capacity to innovate, on both its products (services or systems) and on its internal performance (organization, methods, process). But constraints are increasing and include more and more dimensions. Today health, society, safety, security, environment should be considered as objectives in addition to the classical cost, time and quality. Finally, increasing project complexity induces new challenges for innovation management.

Innovation may have a direct positive impact, but as well indirect negative or positive impacts which in our opinion are not properly considered today. Moreover, innovation integration timeline is not certain in the project. Most of the times it is planned at the very beginning; but it can also be required during the project because of the occurrence of an undesired event, like a change in the laws context, or a change in the budget or a change in the customer requirements. This means that already identified risks have to be updated due to this change.

In the first place, this paper aims at identifying the portion of the project which contains innovation (distinguishing the desired innovation and the novelty or change of a parameter). Secondly, it aims at anticipating the potential propagation of innovation to the rest of the project in order to analyze related risks, including positive and negative ones.

The methodology consists of four steps. Firstly, we propose to identify the novelty degree and the link with innovation, if it is a desired innovation or an obligation (not flexible constraint) or a novelty (a new version/a change in a parameter). As uncertainty is inherent to innovation, the expected direct benefit may be balanced by indirect negative impacts.

The second step consists of identifying these impacts which can be additional risks or increasing values of existing risks. For instance, a desired innovation on the product performance may involve the necessity to innovate on the development process in order to save 2 months. Since this second process innovation is not desired, but the consequence of the previously planned product innovation, it often increases the risk of project failure.

The third step consists of assessing, analyzing and eventually mitigating its indirect risks. It enables to assess, based on uncertainty assessment and propagation, and therefore to increase the global potential benefit of this innovation.

Finally, the fourth step consists of making the decision, eventually considering a tradeoff between the benefits of the initial innovation and the potential drawbacks of its indirect consequences.

This preliminary work focuses on identification of the potential propagation chains, and further works will address the question of their numerical analysis.

KEY REFERENCES

Clarkson, P.J., Simons, C. & Eckert, C. (2004). Predicting Change Propagation in Complex Design. Journal of Mechanical Design, 126(5), 788–797.

Gatignon, H., Tushman, M.L., Smith, W. & Ander-son, P. (2002). A Structural Approach to As-sessing Innovation: Construct Development of Innovation Locus, Type, and Characteris-tics. Management Science, 48(9), 1103–1122.

Giffin, M., de Weck, O., Bounova, G., Keller, R., Eckert, C. & Clarkson, P.J. (2009). Change Propagation Analysis in Complex Technical Systems. Journal of Mechanical Design, 131(8), 081001–081014.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Drilling consortia—new ways of organising exploration drilling in the oil and gas industry and the consequences for safety

L. Hansson & G.M. Lamvik
SINTEF, Trondheim, Norway

S. Antonsen
NTNU Social Research, Trondheim, Norway

ABSTRACT

Drilling for oil and gas is a high risk activity. This has recently been illustrated by the Deepwater Horizon disaster, which caused the deaths of 11 people as well as the worst environmental disaster ever to occur in the Gulf of Mexico. Traditionally, the exploration drilling activities in the oil and gas industry have been carried out by a single operator and a drilling contractor. The drilling rig is usually owned by this contractor and the drilling operations are done according to the specifications and requirements from the oil company.

Recently, a new model for organizing exploration drilling has emerged, especially on the Norwegian Continental Shelf. Smaller oil companies are now joining forces by creating a temporary organisation called drilling consortia. Several oil companies contract a drilling rig while outsourcing several planning and operational functions to a well management company. In this way, the drilling activities are becoming more and more organized as networks than traditional hierarchical organization models. This is an organization form which is rarely addressed in the literature on safety management, which usually presupposes that risky activities can be governed within the boundaries of single organizations (e.g., Petersen 1978). How safety is to be managed in more transient organization forms is thus a largely unanswered question in safety research.

This paper presents the preliminary results of a study of the safety consequences for this way of organising exploration drilling. It is based on a study where two minor oil companies and two well management companies are involved in a project funded partly by the Norwegian research council. One of the study's focus areas is the split between the HSE responsibility and the execution of the HSE related activities. We find that this split involves both strengths and challenges with regards to safety. One possible challenge is found in an increased need for coordination when such a large number of separate companies are to cooperate in high risk activities. On the positive side, and somewhat counterintuitive, we found that the new model can actually lead to greater continuity in the execution of many HSE-related activities.

REFERENCE

Petersen, D. (1978). Techniques of safety management, New York, McGraw-Hill.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Effectively mitigating and managing the risk to public assets

D. Prochazkova
Institute of Security Technologies and Engineering, Faculty of Transport Sciences, Czech Technical University, Praha, Czech Republic

ABSTRACT

The paper presents the overview of results of systematic research of negotiation with disasters in the Czech Republic that was realised in the frame of four national projects in 2004–2008. The research itself was based on basic data sets on disasters from last millennium and it was performed by 17 high educated experts, 23 technical workers and by 11 PhD students with use more than 5000 professional sources and 12 special investigations; all sources are given in original research documents (Prochazkova, 2006, 2007 a, b, 2008). The territory including the human society is considered as the human system with assets: human lives and health; property and public welfare; environment; infrastructures and technologies; mainly the critical ones. The all human aim is to ensure the safe territory and the leading role belongs to public administration that is responsible for risk governance in the territory. Because the risk management is very challenging to knowledge, experiences, data, data processing method, quality of result interpretation, decision-making and of implementation capability, there is necessary to separate tasks for strategic, proactive territory safety management between research institutes and public administration itself. The integral territory safety management is new task for public administration, and therefore, it needs correct tools and they have been prepared under the research mentioned above. Principles used coincide with those in (EMA, 1996, FEMA, 1997, etc.).

The paper summarizes results obtained from representative data sets from the mathematical statistics viewpoint, i.e.: list of disaster types that might be considered at application of the All Hazard Approach (FEMA, 1996); basic terms for discipline which deals with integral territory safety; concept of tool for public administration that ensures its capability to separate expected disasters into categories (relevant, specific, critical) and to apply correctly and effectively preventive, mitigation, response and renovation measures and activities; set of 12 methods that help to public administration correctly and effectively to fulfil its responsibilities connected with territory risk governance.

The present paper shows the summary of project results, complex lesson and tool for judgement of quality of risk governance in territory performed by appropriate public administration. It contains the checklist for identification of risk connected with territory management.The results presented correspond to those from other regions (EMA, 1996, FEMA, 1997, Gustin, 2002).

ACKNOWLEDGMENT

The research was supported by the Ministry of regional development, Ministry of interior, Ministry of Agriculture of the Czech Republic, the Czech Technical University, Faculty of Transport Science, Institute for Security Technologies and Infrastructures and by the EU – project FOCUS.

REFERENCES

EMA, 1996. *Australian Emergency Manual Disaster Recovery*. Emergency Management Australia. Sydney, p. 166.

FEMA, 1996. *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washinton: FEMA.

FEMA, 1997. *Multi Hazard Identification and Risk Assessment*. The Cornestone of the National Strategy. Washington, DC: U.S. Government Printing Office. Availability.

Gustin, J.F. 2002. *Disaster & Recovery Planning: a Guide for Facility Managers*. The FairMont Press, Inc., ISBN 0-88173-323-7 (FP), 0-13-009289-4 (PH). Lilburn, p. 304.

Prochazkova, D. 2006. Professional Reports to Project MMR 28/04 "*Methodology forEstimation of Costs for Property Renovation in Territories Affected by Disasters*" (in Czech). Praha: Ministry of Regional Development, p. 1175.

Prochazkova, D. 2007a. Professional Reports to Project MMR WB-21-05 "*Principals for Compilation of Plans of Renovation of Property in Territories Affected by Disasters that Consider Ensuring the Critical Infrastructure Continuity*" (in Czech). Praha: Ministry of Regional Development, p. 514.

Prochazkova, D. 2007b. D. Procházková: Professional Reports to Project MV RN200552005003 "*Model Solution of Interaction of Risk Analysis for Emergency and Crisis Planning*" (in Czech). Praha: Ministry of Interior, p. 605.

Prochazkova, D. 2007c. *Metodology for Estimation of Costs for Property Renovation in Territories Affected by Disasters*. Ostrava: SPBI SPEKTRUM, ISBN 978-80-86634-98-2, p. 251.

Prochazkova, D. 2008. Professional Reports to Project MZe 1R56002 "*Auxiliary Multi Criteria System for Decision-Making Supporting the Sustainable Development of Landscape and Settlemens*" (in Czech). Praha: Ministry of Agriculture, p. 1020.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Empowered agents or empowered agencies? Assessing the risk regulatory regimes in the Norwegian and US offshore oil and gas industry

P.H. Lindøe
University of Stavanger, Norway

M. Baram
University of Boston, MA, US

G.S. Braut
Norwegian Board of Health Supervision, Norway

ABSTRACT

This paper deals with the contrasting regulatory approaches taken by Norway and the US towards the prevention of major accidents in the exploitation of offshore oil and gas resources. Our purpose is to assess the two regimes as models or prototypes of different control paradigms which define the relationship between the regulator and the regulated. In one model, companies serve as the *instruments* of risk control and are *empowered* agents exercising "internal control" (self-regulation). In the other model, agencies are the empowered agents and control risk by imposing external controls (detailed prescriptive requirements) on companies.

In the 1970's and 80's, major accidents at drilling platforms on the Norwegian continental shelf (Bravo 1977, Alexander Kielland 1980) and the UK shelf (Piper Alpha 1988) led the Norwegian government to replace its prescriptive regulation of offshore safety with a system of enforced self-regulation. As a result, Norwegian regulators established broad functional requirements in the form of performance-based rules, and transferred responsibilities for implementation to companies.

In contrast, the US regulatory approach has remained essentially unchanged with a prescriptive regime. It involves technically-detailed regulatory programs, adoption of industrial standards and practices when these are available, inspecting company activities, and penalizing companies found to violate the regulations.

The US approach, which has been applied to drilling in the Gulf of Mexico (GOM) and other parts of the US continental shelf, involves several federal agencies which are directed by law to carry out a prescriptive program. Another feature is that companies are subject to significant liability of two types: liability to government for oil spill clean-up costs and damages to resources, and liability to individuals and private entities for negligently-caused damage to private property and personal injury. However, the BP Deepwater Horizon disaster in 2010 is causing a major re-evaluation of the regulatory regime.

Multiple sources of information provide the empirical basis for the analysis. First, a portfolio of research projects on the Norwegian and US approaches related to technological change, safety management and regulation. Secondly, we have assessed legal documentation from both countries, and thirdly, we have reviewed the rapidly increasing body of documentation and reports following the BP Deepwater Horizon disaster.

The two regimes are assessed and compared by using an analytical framework with five dimensions; basic regulatory approach, goal setting and measurability, stakeholder participation, learning processes, and how the control dilemma is being addressed. Finally, the strengths and weaknesses of the different approaches and the interchangeability of elements in the two regulatory systems are discussed.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Experience from chemical industry for controlling patient safety

C. van Gulijk & B.J.M. Ale
Technical University Delft, Safety Science, Delft, The Netherlands

D. Dongelmans & M. Vroom
Academic Medical Centre of Amsterdam, Amsterdam, The Netherlands

ABSTRACT

Controlling medical errors is just as difficult as controlling any other error. Unfortunately, these errors can lead to deadly victims all too easy. It was estimated that the number of unintended deaths in hospitals in the Netherlands may be anywhere between 1700 and 6000 on a yearly basis on a population of 16 million people (Wagner & de Bruijne 2007). Ever since that information became public in 2007, hospitals in the Netherlands are urged to design systems that can reduce the number of victims. A safety management system is obligatory since the beginning of 2010.

Hospitals have limited experience with complex safety management systems, so they turned to an industry with an abundant experience. A report by a former director of Shell shared the experience in the petrochemical industry to Dutch hospitals (Willems, 2004). However, the rigid technical approach was difficult to handle by the medical and nursing staff. The experience from chemical industry had to be adapted before it could be applied in hospitals. Therefore, the aim of this work was to design and test a safety management system based on experiences from chemical industry that fits into the normal way of working in the hospital. The development of that system was performed for the Intensive Care department at the Amsterdam Medical Center

Prior to the design and implementation of the safety management system the intensive care department was analyzed and an ethnographic study took place. These analyses resulted in important implications for the design of the safety management system for patient safety. The implications were incorporated into the safety management system proposed by Willems (2004) so that it could be used in the hospital.

An important part of the analysis were interviews with the staff to assess their opinion about patient safety. The investigation shows that they perceive their own efforts and the efforts within their immediate working environment as the most important for patient safety. In that sense, the caretakers are individualistic in their approach to their work. Their personal development and experience is perceived to the most important parameter for delivering good health care. Therefore, it is essential that the safety management system is accepted and operated by the staff on the working floor. Also, the management system has to support personal development, knowledge and experience.

The activities of the hospital central organization and other departments are partly invisible for the staff. As a result, many efforts of the central organization are regarded with some sense of suspicion but more importantly, they are perceived to be too generic for the intensive care department. One of the problems here is that any system that the central organization develops has to be useful to the intensive care department but also to the psychiatric department where the demands for patient care are very different. Therefore, it was decided that the management system should be a modular system that could be adapted to the needs of departments of different types.

The management system was designed as a medical protocol and put to work in April 2009. Some risk analysis techniques typical the chemical industry are now independently performed by the medical and nursing staff. Three bow-ties were created: medication, transport of critical care patients and auto-extubation (the unintended removal of the breathing tube by the patient) and two tripod analyses were performed; one on an incident were medication was administered subcutaneously and another on an incident were blood pressures were not measurable during a handover procedure. These activities indicate that the experience from chemical experience *can* be used in the hospital.

REFERENCES

Wagner, C. & De Bruijne, M. (2007). Unintended damage in Dutch hospitals (in Dutch), Emego and NIVEL, Amsterdam.

Willems, R. (2004). Work safe or don't work here (in Dutch), Shell Nederland, The Hague.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Integrated safety management based on organizational resilience

T.O. Grøtan
Norwegian University of Science and Technology (NTNU),
Department of Production and Quality Engineering, Trondheim, Norway
SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

F. Størseth
SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

ABSTRACT

Resilience (Engineering) is about to become a significant part of safety thinking and practice. Although not fully developed and mature, increasing evidence of its relevance raises a forthcoming challenge, namely how to combine resilience with other (traditional) safety approaches into a coherent sociotechnical and organizational scheme of protection. The prime issue of this paper is how measures of resilience (engineering) can be added to the existing portfolio of principles and practices of *safety management*. Resilience is not just advances in applied methodology, but another approach based on different assumptions (e.g., on normal variability) and a radically different system model. Hence, the integration of resilience into the safety management portfolio will have implications for existing principles.

A *complexity* perspective, related to *social emergence* (Sawyer, 2005) acknowledging that complexity is (also) *endogenous* to the practice of any risk/safety management, is employed to explore how the "new" *emerging safety through resilience* and the "old" *resultant safety through compliance*relate to each other. Moreover, resilience as a theme reinforces with urgency an already pressing, but rather unattended distinction between a) the abilities/properties that we want the systems to comply with (e.g., "the ability to anticipate"), and b) the *situated* MTO (Man-Technology-Organization) measures that have to be employed in order to accomplish these objectives in a composite organizational context.

The notion of *Organizational* Resilience (OR) signifies the full MTO premise of its implementation, and the organizational *intent* of its achievements. Incorporating a full MTO perspective ultimately demands that safety management is willing to look behind the organizational facades (e.g., questioning unified actors, homogeneous environments and long lines of uninterrupted action), relax its traditional stronghold on a "realist" position stemming from a distinct focus on accidents, incidents and errors, and employ a sense of "constructivist" view on resilience as well as on safety as a whole. A crucial point will be to search for *actionable* knowledge and models that can enablea dialectical interactivity between safety management and operating "agents" throughout different organizational contexts.

The paper suggest a set of actionable "contact points" between (resilience) management and the situated practice of being resilient in a diversified and stratified organization comprising a multitude of operational and decision contexts. It is argued that these contact points may serve as the basis for a model of various 'controls' over resilience. As safety indicators often are desirable from a managerial viewpoint, the above considerations also demand a reinterpretation of the role of such indicators

Acknowledging that *resultant safety through compliance* and *emerging safety through resilience* are complementary issues, what still remains unresolved is a feasible comprehension of their joint management. This challenge resembles many of the challenges related to Organizational Resilience (OR) as discussed above. Hence, inspired by what Hutter and Power (2005) denote the Organizational Encounter With Risk, we attend to these issues by referring to "OR of the 2nd order", or just "2OR".

REFERENCES

Hutter, B. & Power, M. (eds). 2005. *Organizational Encounters with Risk*. Cambridge.

Kurtz, C.F. & Snowden, D.J. 2003. The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal*, Vol. 42, No. 3, pp. 462–483.

LeBot, P. 2010. The meaning of human error in the safe regulation model for risky organizations.In Hollnagel., E. (Editor): *Safer complex industrial environments: a human factors approach*. Taylor and Francis.

Nathanael, D. & Marmaras, N. 2008. Work Practices and Prescription: A key issue for organizational resilience. In Hollnagel/Nemeth/Dekker (Eds.): *Remaining Sensitive to the possibility of failure*. Ashgate.

Sawyer, K. 2005. *Social emergence. Societies As Complex Systems*. Cambridge University Press.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Principles for setting risk acceptance criteria for safety critical activities

E. Vanem
Department of Mathematics, University of Oslo, Norway

ABSTRACT

Nearly all activities in life involve risk in some way or another, and there is no universally agreed criteria for what levels of risk are acceptable. Identified and unidentified risks are always sought to be controlled and minimized. The most commonly used strategy for managing risk in the public interest is through legislation and regulation, although everyone is constantly voluntarily managing personal risk in daily life on an individual level, both consciously as well as unconsciously.

Risk reduction will come at a price and there will be a trade-off between the level of risk one accepts and the cost one is willing to spend to mitigate it. For decision-makers responsible for public safety, at the expense of the public wealth, this trade-off needs to be considered carefully and thoroughly. The overall objective is to best allocate the society's scarce resources for risk reduction, by supporting the implementation of efficient risk reduction measures and to avoid wasting efforts on inefficient ones.

Risks introduced to the society from a given activity may be of different types. Fatality risks or health risks are the risk of depriving members of the community of their lives or their good health. Other types are property risk, economic risk and environmental risks. When decisions about safety are made, all risks should be considered, and appropriate acceptance criteria for fatality, health, environmental, economic and property risks should all be met before an activity can be declared safe enough. However, this paper focuses on safety risk.

Safety is surely an important objective in society, but it is not the only one and allocation of resources on safety must be balanced with that of other societal needs. In the literature, different fundamental principles for appropriate risk acceptance criteria have been proposed and extensive research is continuously going on; new principles for establishing and evaluating criteria are continually being introduced.

Having adopted a set of fundamental principles to govern the establishment of risk acceptance criteria, specific risk acceptance criteria can be formulated. In the full paper, some important principles for establishing risk acceptance criteria are presented and discussed. At first sight, some of these may seem exclusive but it will be demonstrated how the different principles can be employed to complement each other in one and the same regulatory regime. Brief considerations on the ethical foundations of the various principles will also be given. Some examples will be given from the maritime industries, but the principles and discussions are believed be general enough to apply to all areas of technical risk.

Some of the principles that will be discussed in the full paper are

- Absolute risk criteria
- The ALARP principle
- The principle of equivalency
- The utilitarian principle of maximum benefit to all
- No mandatory risk reduction measures
- The accountability principle
- The holistic principle
- The precautionary principle
- The principle of parsimony.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Quality aspects in planning of maintenance and modification on offshore oil and gas installations

S. Sarshar, A.B. Skjerve & G. Rindahl
Institute for Energy Technology (IFE), Halden, Norway

T. Sand & B. Hermansen
Den Norske Veritas (DNV), Høvik, Norway

ABSTRACT

The process of planning maintenance and modifications activities on offshore installations is complex. The planning process is traditionally carried out in sequences by different departments in the organization, depending on the time frame and level of granularity of the plan: from 5-year plans to daily plans. It involves highly skilled persons representing different professions, which are located at different physical sites (onshore/offshore). Planning is performed using various software tools such as SAP, SAFRAN or Microsoft Project.

People involved in the planning process are under constant pressure for ensuring that the plans will have a minimum negative impact on production, i.e., in terms of time, cost and resource constraints. The specific attributes that characterize a high quality plan are, however, not readily defined. The robustness of plans, i.e. the inherent ability to keep as much as possible of the original structure as time moves forward, is furthermore, considered as a key concern. The reason is that robustness will reduce the amount of re-planning between each level of planning and it will enable more accurate cost estimates and better basis for material/logistics planning earlier on in the process.

This paper explores aspects in planning of maintenance and modifications of offshore oil and gas installations: *What are the characteristics or aspects of a high quality plan?*

To answer this question, insights are needed about how plans are developed. This paper describes how the different planning levels from annual plans down to work preparations for activities to be undertaken the following day are handled. Risk assessment is performed in each of the planning phases, but with different means and purposes. It is of high importance that risk detected in early phases of the planning are communicated through each step of the planning activity to maintain a high level of safety. The personnel involved, the required skills, prerequisites and methods of interaction necessary to build safety into the planning process from the top level down to execution is outlined. The handover from one level of planning to the next and also re-planning routines is illustrated. The description reflects the planning process commonly seen in the North Sea.

This paper reports the method used to derive aspects of high quality plans identified in the present study. Data was obtained as part of a usability test of a prototype tool to support planning called *Maintenance and Modification Planner (IO-MAP)* (Skjerve et al., 2011). The findings from the usability study are discussed, in light of the overall characteristics of planning processes identified. They include several interesting observations that can point to future improvement in tools designed to support planning, as well as in evaluations of plan, distributed across three categories: Health, safety and environment; Cost issues; and Workmanship of maintenance and modifications.

The reported work outlines a set of characteristics that should be addressed in assessments of the quality of maintenance and modification plans for offshore oil and gas installations.

The study reported in this paper is a direct continuation of the study presented at ESREL 2010 (Sarshar & Sand, 2010), which concerned identification of improved management of safety aspects for maintenance and modifications planning.

REFERENCES

Sarshar, S. & Sand, T. 2010. "Communicating Risk in Planning Activities Distributed in Time", in *Proc. of Risk, Reliability and Societal Safety, ESREL 2010*, Rhodes, Greece, 2010.

Skjerve, A.B., Sarshar, S., Rindahl, G., Braseth, A.O., Randem, H.O. & Fallmyr, O. 2011. "The Integrated Operations Maintenance and Modification Planner (IO-MAP) – The first usability evaluation – study and first findings", Center for Integrated Operations in the Petroleum Industry, Norway, 2011.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reducing the risks faced by small businesses: The lifecycle concept

S. Clusel
AFNOR Group / Crisis and Risk Research Centre, Mines Paris-Tech, La Plaine Saint Denis, France

F. Guarnieri
Crisis and Risk Research Centre, Mines Paris-Tech, Sophia-Antipolis, France

C. Martin
ESAIP / Crisis and Risk Research Centre, Mines Paris-Tech, Grasse, France

D. Lagarde
AFNOR Group—Marketing and Innovation Department, La Plaine Saint Denis, France

ABSTRACT

In France, more than 99% of failed businesses are Small or Medium-sized Enterprises (SMEs) (Altares, 2010).

Failure is considered here in practical terms as a state of insolvency, i.e., the company is unable to meet its liabilities from its available assets. This final and extreme demonstration of the difficulties that a company can experience (De la Bruslerie, 2006) is the result of deeper causes, which are for the most part predictable, and for which the most frequently cited problems are financial and managerial, related to demand and/or a crisis within the organization.

One of the solutions classically envisaged is global risk management that allows analysis of the major risks for the business (loss of a significant debtor, significant increase in production costs, loss of a key worker etc.) using a methodical, systematic and iterative process. The idea is attractive, however, the implementation of such approaches within SMEs, and specifically within micro— and small businesses (defined by EU regulation 2003/361/EC as having less than 10 or 50 employees respectively) is far from obvious. In fact, on the one hand there is a little interest in the implementation of such procedures from business owners, who look at the ratio of the time and complexity of implementation with respect to the relevance of the results for strategic orientation of the organization, and on the other hand, the inadequacy of tools which are really only 'lite' versions of systems under the control of big business.

The aim of this current work is to rethink current commercial approaches which do not take into account the metamorphosis of the SME and its changing needs at different stages of its evolution.

To consider the deployment of a comprehensive risk management approach within an SME, in addition to the reconsideration of persistent prejudice, implies the need to describe and explain the particularities of these organizations in relation to the needs and expectations that are specific to them and which change over time. It is therefore appropriate to study the different phases of development of SMEs using the lifecycle concept. This concept highlights the modifications and configurational changes of this type of organization during its development.

This article therefore aims to define and legitimize the use of the lifecycle concept as a basic component of a global risk management approach in an SME. It attempts to characterize the vulnerabilities of SMEs in terms of a model which brings together hazards, consequences and the different stages of company development. Finally, it describes an operational approach to reducing the vulnerability of this type of structure based on their level of organizational maturity.

REFERENCES

Altares, 2010. Bilan 2009 défaillances et sauvegardes d'entreprises en France. Analyse annuelle du 19 Janvier 2010. p. 37.

Antonosson, A-B. 1997. Small companies. In D. Brune et al. (ed.) The Workplace, vol. 2, part 5.3: 466–477.

Crutzen, N. 2009. Essays on the Prevention of Small Business Failure: Taxonomy and Validation of Five Explanatory Business Failure Patterns (EBFPs). Thèse de doctorat HEC- Ecole de gestion de l'Université de Liège.

De La Bruslerie, H. 2006. Analyse financière - Information financière et diagnostic. Paris: Dunod.

Scott, M. & Bruce, R. 1987. Five Stages of Growth in Small Business. Long Range Planning. vol. 20 N°3: pp. 45–52.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Risk assessment method for shopping centres

S. Nenonen
Tampere University of Technology, Department of Industrial Management, Center for Safety Management and Engineering, Tampere, Finland

K. Tytykoski
Inspecta Tarkastus Oy, Tampere, Finland

ABSTRACT

The unique features of shopping centres (e.g., large numbers of visitors and design of premises) create specific risks for the management of safety and security (European Agency for Safety and Health at Work, 2011). Shopping centre hazards, if realized, may endanger the safety of both visitors and people working and doing business in shopping centres (Finnish Council of Shopping Centres, 2005). Therefore, the management of safety needs to cover both the customers who visit the shopping centres and the personnel working in the premises. However, even though the prevention of safety and security risks plays a critical role in shopping centres, safety and security issues have not received much attention in scientific literature to date.

This paper discusses risk assessment in shopping centres and presents an assessment method developed particularly for shopping centres. The aim was to construct a comprehensive risk assessment method on shopping centre safety and security by considering significant factors regarding shopping centre property and premises, as well as the activities of those working and doing business in the premises. The development of the risk assessment method was started by reviewing the special features of safety and security in shopping centres by a literature review, interviews directed to the personnel of two Finnish shopping centres and a questionnaire carried out among a group of Finnish shopping centre operators. Based on the gathered information, a new shopping centre specific risk assessment method was compiled.

According to the results of the interviews and the questionnaire, shopping centres are perceived as safe and serious incidents seem to be rare. The main risk that was brought out related to undesirable behaviour of visitors. Other potential risk factors were considered to relate, if poorly managed, preparedness for emergencies, different operators (e.g., tenants, safety personnel), introduction and training, operation and sufficiency of technical systems particularly in the context of emergencies.

The risk assessment method presented in the paper has been developed to ease the identification of hazards and the assessment of risks in shopping centres. The developed method discusses shopping centre safety comprehensively by paying attention to both the performance of employees and visitors and the issues regarding shopping centre property and premises. The method can be utilized in reviewing the present safety level of a shopping centre, in identifying potential hazards, and in planning improvement measures to diminish or remove the existing risks. The model also helps shopping centres to pay attention to the relevant legal requirements, and it enables effective organisation of safety measures between different shopping centre operators such as maintenance, security and management.

The risk assessment method presented in this paper has been developed in Tampere University of Technology as part of a larger research project, namely 'Shopping centre safety management'. The originator of the project was the Finnish Council of Shopping Centres and the funding was obtained from Tekes—the Finnish Funding Agency for Technology and Innovation and the project partners.

REFERENCES

European Agency for Safety and Health at Work, 2011. Kauppakeskukset. (In Finnish; Shopping centres). Available in http://osha.europa.eu/fop/finland/fi/good_practice/alakohtainen/kaupan-ala/kauppakeskukset?set_language=fi (21.3.2011)

Finnish Council of Shopping Centres, 2005. Kauppakeskusten turvallisuusjohtaminen. (In Finnish; Shopping centre safety management) Available in http://www.rakli.fi/kky/attachements/2005-09-06T12-50-5348.pdf (21.3.2011)

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Security risk management in Norwegian aviation meets nordic traditions of risk management

O.A. Engen
University of Stavanger, Norway

ABSTRACT

Both the aviation sector and the petroleum sector are technologically based organisational systems and both aspire to be associated with best practises of high reliability. Traditionally the safety regime on the Norwegian Continental Shelf has been developed and governed by a sophisticated body of laws and regulations coined as the "Nordic model" of Occupational Health and Safety and based on a three-part pillar with the regulator, the employer and the employees/unions as legitimate. It is reasonable to claim that the Nordic Model and the safety system that has developed in the Norwegian oil industry are closely connected. The traditional Norwegian safety system is found in the system-oriented approach where socio-technical design and organizational factors adjusted to how humans act are seen as the dominant factors.

The terrorist attacks that took place September 9/11, 2001, demonstrated that the security system, comprising legislation, regulation, and implementation were not adequate to handle an intentional event of this magnitude. The 9/11 attacks caused a major reshuffling in the regulatory system and made it mandatory for all member countries. The convention formed the basis for EU's new frame regulation 2320/2002 which evolved into a detailed, deterministic system The risk management systems in the Norwegian aviation sector in the aftermath of 9/11 have system that aimed at securing civil aviation through a detailed and uniform system for all of the European countries. From the more goal-based way of regulating, the new security regime essentially followed a 'prescriptive' regulatory approach which is based upon mandated compliance.

This paper discusses how the security regime in aviation deviates from traditional "Nordic" practises of technological risk management in the petroleum sector. The paper highlights differences and similarities between the two systems and questions whether local participation and stakeholder involvement are necessary prerequisites for successful safety/security management.

The safety regimes in aviation and the Norwegian petroleum industry have been a goal based regulatory system accompanied by participatory processes where the unions have played a leading and dominating role. In the safety regimes within the petroleum sector there have been however been attempts to undermine the system by introducing more prescriptive procedures and detailed control with workers behaviour. The security system that has developed in aviation is typically prescriptive by nature an also elitist by the fact that very few participate in the decision making processes and where it is secrecy about the motives and reasons of the regulations. Such regulatory traits are found both in the petroleum industry and in aviation. Even though the relative importance of security is far less in the petroleum sector than in aviation, it seems that the security agents in petroleum prefer a movement towards a more prescriptive and elitist system. In aviation on the other hand, the revealed preferences is to reduce the prescriptive character and open up for a more goal based and flexible system. It is however important to underline that the safety and security regimes in both sectors are under constant revisions and our analysis only intend to describe the movements on a general level.

The security challenges both facing the petroleum industry and the aviation sector have shown that traditional participatory ideal and socio-technical approaches are not appropriate dealing with terrorist threat. As the risk problems of any socio-technical system are ambiguity induced we are faced with a discrepancy between risk governance theory and regulatory practice. However, it leads us to remind ourselves what contextual factors that explain why a top down instrumental regulatory regime has been developed. Actions taken after 9/11 have challenged democratic values worldwide where "war against terror" exclusively has been based on military premises. Following the definitions of safety and security there are arguments in favor of also divide the organizational instruments. However, it may be more to win by searching for how these two concepts may mutual benefit from each other than build up two incompatible regimes.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The collective risk, the individual risk and their dependence on exposition time

J. Braband
Siemens AG, Braunschweig, Germany

H. Schäbe
TÜV Rheinland, Köln, Germany

ABSTRACT

he exposition of an individual or a group of persons to a hazard is important, when a risk analysis is carried out to derive a safety integrity level. The same holds true, when the achieved risk of a system is computed, e.g., for a safety case. The exposition time is mentioned in several standards when the safety integrity level is derived. There, the exposition is used as a parameter, e.g., in IEC 61508 as "exposure in the hazardous zone". Risks are sometimes given per calendar year, sometimes per hour of use. In other cases, risk is presented per person kilometers for a traffic system. The values of risk might differ, depending on the time unit which is used for indication of the risk. In section two, we give an introduction and show, which standards use hazard exposition as a parameter.

In section three, we describe collective risk, F-N., curves and individual risk and their interrelationship. We show, which important role is played here by exposure time of an individual and cumulated exposure of a group of persons when relating individual and collective risks to each other.

In the fourth section, we provide application examples. Different sources provide different risk values with different time units and, consequently, different absolute values. We discuss examples, where the risk figure is so vague, that it becomes useless, because exposition to the hazard is completely undefined.

We show that a risk is presented best for a general unit of exposition time, e.g., per hour. This holds true, if exposition time cannot be neglected as e.g., for Bungee jumping. If risk is given per calendar time, the assumptions about exposition need to be considered in the form of exposition time per event and the number of events or the cumulative exposition time in order to avoid misunderstanding. When talking about transport systems, also the risk per unit of transport capacity, i.e., person kilometer. This makes sense for collective risks. If exposition time is incorrectly taken into account, one might easily have differences of one order of magnitude or even more.

REFERENCES

Bepperling, S. 2009. Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik, *Dissertation*, TU Braunschweig, 2009 (Validation of a semi-quantitative approach to risk assessment).

CENELEC, 1999. *Railway applications – Systematic allocation of safety integrity requirements*, Report R009-004.

EN 50126, 1999. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS).

EN 50129, 2003. Railway applications - Commmunication, signalling and processing systems – Safety related electronic systems for signaling.

European Transport Safety Council 2003, *Transport Safety Performance in the EU Statistical Overview*, Brussels.

IEC 61508, 2010. *Functional safety of electrical/electronic/programmable electronic safety-related systems*, parts 1–7, ed. 2.

IEC 61511, 2003. *Functional safety - Safety instrumented systems for the process industry sector*.

IEC 62061, 2005, *Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems*.

ISO DIS 25119, 2008. *Tractors and machinery for agriculture and foresty—Safetyrelated parts of control systems*, part 1–4.

ISO DIS 26262, 2009. *Road vehicles—Functional safety*.

Kafka, P. 1999. How safe is safe enough, *Proc. ESREL* 1999, vol. 1, pp. 385–390.

Kuhlmann A. 1986. *Introduction to Safety Science*, Springer, New York, 1986.

Melchers, R.E. Structural reliability, Analysis and Prediction, J. Wiley & sons, New York, 1987.

Modarres, M. 2006. *Risk analysis in Engineering: Techniques, trends, and tools*, CRC press 2006.

Proske, D. 2008. *Catalogue of Risks*, Springer, New York.

Yellow Book 2007. *Engineering Safety Management* Volumes 1 and 2, Fundamentals and Guidance, Issue 4, Rail Safety and Standards Board, 2007.

Wikipedia 2010. Bungee-Springen, http://de.wikipedia.org/wiki/Bungee-Springen, last access 2010-06-29 (Bungee jumping).

This page intentionally left blank

Safety culture and risk perception

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Development of a safety management system for Small and Medium Enterprises (SME's)

Edgar McGuinness
College of Engineering and Informatics, National University of Ireland Galway (NUIG), Galway, Ireland
Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Ingrid B. Utne
Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway

Martina Kelly
College of Engineering and Informatics, National University of Ireland Galway (NUIG), Galway, Ireland

ABSTRACT

It is widely reported in the literature that employers in the Small and Medium sized Enterprises (SME's) sector consider the available safety management standards to be costly and bureaucratic, paper-driven exercises, of no materialistic value to the organization (Duijim et al., 2008). This paper presents a generic guideline for development of a simple Safety Management System (SMS) to be implemented by (SME's). The outlined guideline possesses the strengths covered by existing commercial standards but without their inherent limitations, such as cost, man hours, excessive documentation and record keeping. The generic format of the proposed guideline is based on the simplification and adaptation of available standards, and specifically designed for non-health and safety professionals, working with limited resources. The guideline needs to be introduced in manner that is easily understood, implementable and maintainable, combining simplicity and a strong self-help element. In addition, the SMS guideline aims at keeping financial and manpower costs low while delivering ownership and interest in continuous improvement in to an organization.

Since, health and safety legislation has placed the emphasis on risk assessment and risk management (Vassie et al., 2000), the guideline proposes the development of a SMS based on a simple risk assessment. The guideline is divided into three steps, consisting of 1) risk assessment, 2) system management and 3) performance evaluation. The elements determined as essential in the construct of the SME SMS guidance document were hence divided into each of these steps based on their influence on safety. An extensive literature review was conducted to identify the most salient points regarding the elements required for the construction of an operational SMS.

Risk assessment, management commitment, communication and employee participation are important constituent factors in the development of an efficient and effective SMS (Fernandez-Muñiz et al., 2007a), but additionally vital, is the development of an organizational safety culture. Safety culture is held as the next evolutionary step in development of safety management for the protection of workers.

A questionnaire and a provisional guidance document were drafted and circulated to a small population of safety officers/ managers working in SME's in Ireland to determine if the developed SMS guideline met with industry approval for its applicability, usability and validity. The respondent's feedback rated each of the elements of the proposed guideline highly, expressing satisfaction with the explanations, format and content of the proposed system as a platform by which to implement a SMS. The industry specific results demonstrated that many of the requirements for SMS implementation are already in practice in SME's. What is required is the structure to make them into a system, as is provided in the guidance document. Further work includes a pilot study, whereby the developed SMS could be tested in an enterprise, truly testing the ability of the proposed system to manage safety in SME's.

REFERENCES

Duijm, N.J., Fievez, C., Gerbec, M., Hauptmanns, U. & Konstandinidou, M. 2008. Management of health, safety and environment in process industry. *Safety Science* 46: 908–920.

Fernandez-Muñiz, B., Montes-Peón, J.M. & Váz Quez-Ordás, C.J. (2007a). Safety culture: Analysis of the causal relationships between its key dimensions. *Journal of Safety Research* 38: 627–641.

Vassie, L., Tomas, J.M. & Oliver, A. (2000). Health and Safety Management in UK and Spanish SMEs: A Comparative Study. *Journal of Safety Research* 31:35–43.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Relation between organizational culture styles and safety culture

M.A. Mariscal Saldaña & S. García Herrero
University of Burgos, Spain

A. Toca Otero
Sta. Mª de Garoña Nuclear Power Plant, Spain

J.M. Gutierrez Llorente
University of Cantabria, Spain

ABSTRACT

An analysis of the main accidents that have taken place throughout history shows that these events cannot be explained by random equipment failures alone, but also by a combination of human and organizational factors. In the nuclear industry, the IAEA's International Nuclear Safety Advisory Group introduced the term of "safety culture" to highlight this fact.

However, Safety Culture (SC) may not capture all the management and organizational factors which are important for the safety of the plant operation. The key problem with most existing SC models is their lack of integration with general models of organization and organizational culture.

In research studies, no attempt has been made to link safety culture with organizational culture. Therefore, the objective of this study is to show how to improve the Safety Culture in one NPP acting on organizational culture styles.

In order to establish this relationship, probabilistic Bayesian Network (BN) models have been used. Data was gathered through a survey in June 2007, in a Spanish NPP (Sta. María de Garoña).

The safety culture questionnaire was based on the five characteristics established by the International Atomic Energy Agency (IAEA). They are: 'safety is a clearly recognized value', 'accountability for safety is clear', 'safety is integrated into all the activities in the organization', 'leadership for safety is clear' and 'safety is learning driven'.

In order to assess organizational culture, the Organizational Culture Inventory (OCI) was used. The OCI questionnaire focuses on the behavioral norms and expectations associated with the values shared by members within an organization. The OCI proposes 12 types of organizational cultures. The constructive types are 'humanistic-encouraging', 'affiliative', 'achievement', and 'self-actualizing'. The passive/defensive types are 'approval', 'conventional', 'dependent' and 'avoidance'. The aggressive/defensive types are 'oppositional', 'power', 'competitive', and 'competence/perfectionistic'.

The BN models have thus identified the most relevant variables which help enhance or hindrance the safety culture in the NPP.

A global model with those variables was constructed in order to identify the behaviors that play the greatest role in improving the SC. Of importance within the humanistic style are resolving conflicts constructively, involving others in those decisions that affect them, worrying about the needs of others and being supportive of them. In the affiliative style the following stand out: collaborating with others, treating others in a friendly and pleasant manner and thinking in terms of satisfying the group. Negative influences in the avoidance style include: keeping out of sight when difficult situations arise and avoiding being blamed for mistakes. In the oppositional style, looking for errors, pointing out flaws and not remaining on the sidelines have an exceedingly high influence on SC. Within the achievement style, knowing the company's activity. And lastly, in the self-actualizing style, communicating ideas.

REFERENCES

Castillo, E., Gutiérrez, J.M., & Hadi, A.S., 1997. Sensitivity analysis in discrete Bayesian networks. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, 27(4): 412–423.

Cooke, R.A. & Lafferty, J.C., 1987. Organizational Culture Inventory. Human Synergistics, Plymouth, MI.

IAEA, 1991. Safety Culture (Safety Series No 75-INSAG-4). International Nuclear Safety Advisory Group, International Atomic Energy Agency, Vienna.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Risk perception in health care—A study of differences across organizational interfaces

S. Wiig
Department of Health Studies, University of Stavanger, Stavanger, Norway

ABSTRACT

This paper examines risk perception among officials and employees across organizational interfaces within the health care system as a risk regulation regime. Officials and employees at different levels of a given regime may perceive risk differently (Hood et al., 1999; 2001; Rothstein, 2003), developing divergent attitudes towards the regulation and demands for risk management (Kewell, 2006). This paper focuses on institutional and instrumental aspects of risk regulation regimes—namely, the context (type of risk, public preferences and attitudes, organized interests) and backdrop of regulation—as well as the content (size, structure, style) involving the objectives and styles of regulation. The paper explores how these institutional and instrumental aspects shape risk perception among officials and employees across organizational interfaces in the Norwegian specialized health care system. The research question is:

How do contextual and content elements of risk regulation regimes shape risk perception among officials and employees across organizational interfaces in health care?

The study design is an embedded single case study approach covering the specialized healthcare. Data were collected using a triangulation of qualitative and quantitative methods such as interviews, document analyses, observations, and statistical analyses (Patton, 1999). A total of forty-nine tape-recorded interviews were conducted using structured interview guides. Furthermore, a total of 894 written error reports from two hospital divisions were registered and analyzed using an Excel database. Document analyses have been conducted of healthcare legislation, Norwegian White Papers, guidelines and policy documents, inspection reports, and annual reports.

The results showed that risk perception varied according to officials' and employees' location within the regime (national or local regulator or within the hospital hierarchy), responsibility, profession, and personal experience with medical errors (Tamuz et al., 2004; Kaplan et al., 2003; Hutter, 2001; Hutter & Lloyd-Bostock, 1992). The results show amplification of certain risks and attenuation of others; implying that there exists a potential for latent conditions not to be discovered, managed, and learned from.

The study revealed heterogeneous risk perception across organizational interfaces in the regime. A regime involving complex structures and strong formal regulatory enforcement caused occupational and hierarchical variations in understanding risk. These content-related aspects alone do not shape risk perception; contextual aspects also have to be taken into account. Among the contextual elements, type of risks was the most vital for shaping risk perception. Some risks were observable and managed, but several risk types emerged due to the changes and complexity within the regime, turning out to be perceived differently across interfaces in the regime—if perceived at all.

REFERENCES

Hood, C., Rothstein, H., & Baldwin, R. 2001. *The Government of Risk—Understanding Risk Regulation Regimes*. Oxford: Oxford University Press.

Hood, C., Rothstein, H., Baldwin, R., Rees, J., & Spackman, M. 1999. Where Risk Society Meets the Regulatory State: Exploring Variations in Risk Regulation Regimes. *Risk Management: An International Journal* 1 (1): 21–34.

Hutter, B.M. 2001. *Regulation and Risk*. Oxford: Oxford University Press.

Hutter, B.M. & Lloyd-Bostock, S. 1992. In Short, J.F. Jr. and Clarke, L. (eds) *Organizations, Uncertainties, and Risk*. Boulder: Westview Press.

Kaplan, H.S. & Rabin Fastman, B. 2003. Organization of event reporting data for sense making and system improvement. *Quality & Safety in Health Care* 12: (Suppl II): ii68–ii72.

Kewell, B.J. 2006. Language games and tragedy: The Bristol Royal Infirmary disaster revisited. *Health, Risk & Society* 8 (4): 359–377.

Patton, M.Q. 1999. Enhancing the Quality and Credibility of Qualitative Analysis. *Health Services Research* 34: 1189–1208.

Rothstein, H. 2003. Neglected risk regulation: The institutional attenuation phenomenon. *Health, Risk & Society* 5 (1): 85–103.

Tamuz, M., Thomas, E.J. & François, K.E. 2004. Defining and classifying medical error: Lessons for patient safety reporting systems. *Quality & Safety in Health Care* 13: 13–20.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Safety theoretical issues: Scientific please, but keep it brief

Fred Størseth
SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

Tor Olav Grøtan
SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway
Norwegian University of Science and Technology, Department of Production and Quality Engineering, Trondheim, Norway

ABSTRACT

The current paper seeks to address formal theoretical issues in contemporary safety research.

Pursuing the thesis that *theory is method*, the paper advocates the value of taking the theoretical 'long road'; that is, staying wary for, and actively trying to match ones theoretical effort against formal theoretical principles. This does not imply that 'a' theory-method is suggested. Rather, it reflects acknowledgement of working with ideas, the conception that any shortcut in these respects is an actual short-cutting of reasoning and theoretical development.

The paper starts by positioning 'science' and 'theory', within the context of our area of research interest (i.e., organizational resilience). By reference to concepts like complexity and emergence, resilience can be said to challenge traditional assumptions of correlation, causation, "laws", and system regularities. In a way, resilience challenges the very rationality of enforcing rule and procedure compliance in the name of safety. Thus, what we need is a notion of science and theory that is not trapped in a notion of 'science as common sense'. Inspired by Alvesson and Sköldberg (e.g., 1994), we emphasize the need to go beyond chasing ever-increasing exactness of methods to crystallize 'definitive' terms and variables; and that (our) research need to stay sensitive of new (emerging) relations, perspectives, and world views.

The following set of principles is suggested as a kind of formal theoretical navigation points for consideration along the long road: *Concept elaboration*, *conjecture beyond description*, *traceability*, and *association specification*.

It is however well recognized that the long road is an ideal case, and that today's research practice often is forced or willingly attuned with quick business. Thus, the paper raises issues related to what may be serious obstacles to the ideal long road, e.g., illusions, double edged swords (and standards, e.g., scientific, yes please; but keep it brief).

The paper specifically brings attention to and discusses (1) dangers of how theory typically is utilized and developed, and (2) in recognition of the first point, to what extent these formal theoretical principles have effectively been employed as groundwork for our own specific task at hand: i.e. to explore principles of organizational resilience.

Acknowledging that we are captives of our own words, the discussion pertains to issues of how we, in our own theoretical efforts in the making have addressed formal theoretical principles. We argue that a constant dialogue with formal theoretical principles seem to have added a propeller in our attempt to theoretically accentuate *organizational* resilience by issues like episodic resilience, dispersed decision contexts, dialectics of prescription vs. practice (Nathanael and Marmaras, 2008), looking behind rational facades/impermanent organization (Weick, 2009), actionable knowledge, strata based on communities of practice, and social emergents (Sawyer, 2005). Constant moves between formal theoretical issues and specific examples as faced throughout our research has both created theoretical momentum and triggered imagination. This way, at least on formal grounds, we are intentionally taking the long road, by working with theory—as method.

REFERENCES

Alvesson, M. & Sköldberg, K. 1994. *Tolkning oc reflection. Vetenskapsfilosofi och kvalitativ metod (Interpretation and Reflection. Philosophy of science and qualitative method)*. Studentlitteratur.

Nathanael, D. & Marmaras, N. 2008. Work Practices and Prescription: A key issue for organizational resilience. In: E. Hollnagel and S. Dekker (Eds.): *Remaining Sensitive to the possibility of failure*. Ashgate.

Sawyer, K. 2005. *Social emergence. Societies As Complex Systems*. Cambridge University Press.

Weick, K.E. 2009. *Making Sense of the Organization Volume 2. The Impermanent Organization*. Blackwell Publishing.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The challenge of system change in aviation: The Masca project

M.C. Leva, N. McDonald & S. Corrigan
Aerospace Psychology Research Group—School of Psychology Trinity College Dublin, Ireland

P. Ulfvengren
KTH Industriell Teknik Och Management, Stockholm, Sweden

ABSTRACT

The main object of MASCA is to develop and deliver a structure to manage the acquisition and retention of skills and knowledge concerning organisational processes for managing change in the 'whole air transport system'. Different stakeholders in a common operational system (airlines, airports, maintenance companies, etc.) joined together in the project to change the shared operational system to deliver a better service. An Original Equipment Manufacturer (OEM) and software designer will offer technology solutions which support a more effective integrated operation. The participating companies will develop and maintain new skills and knowledge in change management. MASCA will develop the 'concepts and techniques' which can develop, manage, and support the effective deployment of these skills and knowledge in the management of change.

The workprogramme takes an action research approach with a primary focus on the transfer of change management capability into the organisations that are responsible for and involved in change. Thus the workprogramme is organised around two complementary objectives:

- The development of a system to support the development and deployment of an integrated change management capability (Change Management System—CMS).
- The deployment and evaluation of the CMS in selected change management initiatives, both simulated and actual.

Transformation or change of the social system within Masca is seen not just in terms of the ways in which the system "affords" (enables, encourages, directs, mandates) appropriate actions and interactions from its members, but even more, how to influence the common understanding of how the system works, taking into account the background of accumulated collective experience that has formed that cultural expression. It is in fact believed that organizational culture is as much about how things work in the organizational system—"why we do things this way around here" as it is about a simple aggregation of meanings and activities "the way we do things around here" (Deal and Kennedy 1982). This approach has already influenced the tools and methods used to determine the target case studies for change within the end user organizations.

The MASCA consortium covers the range and balance of partners to address the 'whole air transport system'—an airline includes flight, maintenance and ground operations companies; an airport authority; an original equipment manufacturer—world leader in aircraft technologies; two universities; an aeronautics research organisation, and an SME with a strong profile in technology and human factors services to aviation

REFERENCE

Deal, T.E. and Kennedy, A.A. (1982). Corporate Cultures: The Rites and Rituals of Corporate Life, Harmondsworth, Penguin Books.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The impact of safety climate on risk perception on Norwegian and Danish production platforms

H.B. Rasmussen
Centre of Maritime Health and Safety, University of Southern Denmark, Esbjerg, Denmark

J.E. Tharaldsen
Petroleum Safety Authority, Stavanger, Norway

ABSTRACT

The study explores the impact of safety climate on subjective risk perception of personal accidents and process accidents on Norwegian and Danish offshore production platforms.

Due to geographical location and history Denmark and Norway always have been closely connected. The same tendency is seen with cooperation in the oil industry. Both the Danish and Norwegian shelves constitute mature oil producing regions. The common view in the Scandinavian countries is that there is some kind of a common Scandinavian identity? However, in this study we will look for potential differences. Yet, no comparative safety study on Danish and Norwegian offshore employees has been carried out, but one study in the building and construction sector has compared Danish and Swedish construction employees. The study found differences in their safety performance, where the Danes were found to be more accident prone than the Swedish workers. One of the explanations was better education of the Swedish employees and cultural differences between Swedes and Danes (Spangenberg et al., 2003).

Danish data consists of a survey sent to employees on all productions platform on the Danish sector in 2010. The Danish survey was translated from the Norwegian questionnaire used the "Trends in risk level" project being performed every second year by the Norwegian Petroleum Authority. Data from these two surveys were thereafter merged together and a five dimensional solution of safety climate were tested on both populations in SPSS and LISREL. The dimensions Safety management and involvement, System perception and Safety versus production held the best model solution and were used further in the statistical analyses. T-test and step wise regression analysis were used to compare groups.

We expect that Norwegian offshore employees will show more positive safety perceptions compared to their Danish colleagues, due to the longer experience and history with offshore petroleum work and its safety challenges. The risk perception we anticipate will be will the same on both sectors.

The result of the current study shows that the Norwegian offshore employees have more positive safety climate perception compared to their Danish colleagues. The t-test shows that the average on the dimensions: safety prioritization and safety management and involvement was higher between Norwegian offshore employees than between their Danish colleagues.

The Norwegian offshore employees indicated higher subjective risk perception to personal injuries and process incidents compared to Danish offshore employees.

As expected, better safety climate predicted lower risk perception. The study carried out in the Norwegian sector indicated the same tendency (Tharaldsen et al., 2008).

REFERENCES

Spangenberg, S., Baarts, C., Dyreborg, J., Jensen, L., Kines, P. & Mikkelsen, K.L. 2003. Factors contributing to the differences in work related injury rates between Danish and Swedish construction workers. *Safety Science*, *41*(6), 517–530.

Tharaldsen, J.E., Olsen, E. & Rundmo, T. 2008. A longitudinal study of safety climate on the Norwegian continental shelf. *Safety Science*, *46*(3), 427–439.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Training for compliance and beyond: Enabling high performance deliveries in the work permit process

H. von Hirsch Eriksen, S. Mjelstad, O.H. Utvik & Helge Smaamo
Operational Training Centre, Development and Production Norway, Statoil ASA, Norway

ABSTRACT

The paper outlines the activities, goals, and results of the Operational Training Centre (OTC) at Development and Production Norway (DPN) at Statoil. Representing a practitioner perspective we underscored that commentary on our practice are very much welcome.

The OTC trains the company workforce on the Norwegian Continental Shelf with the aim to improve risk governed safety behaviour based on compliance. Typically, the training is conducted on-shore over a period of two days. There are two cornerstones in the structure of any program at OTC. Firstly, the focus is oriented towards the process based management system (APOS). Secondly, a company-wide model of Compliance and Leadership contribute as a guide for both participants and facilitators in the 'way to work'. This model focuses on process in the sense that it directs how tasks are planned, completed, and evaluated (Figure 1).

In the design of our programs, several phases of training are addressed. Preparation of participants prior to the on-shore training, as well as follow-up (or extension) activities when the workers return offshore are important criterions for success.

In this paper our point of departure is related to the legislative requirements for conducting offshore operations on the Norwegian Continental Shelf. We note that the legislation rests on the principle of functional requirements. Thus, the responsibility of compliance lies within the responsibility of the operator. In turn, operators specify structures of control and management through governing documents.

In the industry, potential conflicts are linked to the issue of compliance. One part of this picture is for instance the conflict between formal requirements as stated in governing documentation and the local autonomy of action. Another area of contradiction is related to decentralised vs. centralised functions, knowledge, and control (McDonald, 2006). In the paper we suggest that the model of compliance and leadership may be viewed as an effort to connect these inherent contradictions.

The overall goal of the OTC's training activities is to initiate behavioural change/ influence—more specifically to influence safety behaviour and establish a culture of compliance offshore. The paper describes the pedagogical principles utilised at the Training Centre as well as the philosophy for behavioural change and learning that these principles are hinged upon. Further, the design and process of training are described by means of the work permit process as a case example.

The effects of training programs are interpreted thru both quantitative (survey) and qualitative (open-ended exploratory interviews) methods based on Kirkpatricks four levels of assessing organisational training (Kirkpatrick, 1994). The method and results of these are presented in the paper. Results suggest that training effects attitude, behaviour, knowledge (of the management system and the compliance and leadership model), as well as perceived role confidence.

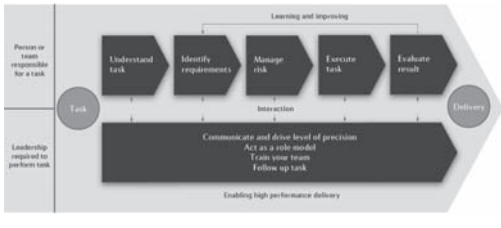


Figure 1. The model for compliance and leadership.

REFERENCES

Kirkpatrick, D.L. (1994). Evaluating Training Programs. San Francisco: Berrett-Koehler Publishers, Inc.

McDonald, N. (2006). Organisational Resilience and Industrial Risk. In Resilience engineering: concepts and precepts, edited by Erik Hollnagel, David D. Woods, Nancy Leveson. Aldershot, England Burlington, VT: Ashgate.

Structural reliability and design codes

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Beams on elastic foundation solved via probabilistic approach (SBRA Method)

K. Frydrýšek
VŠB—Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

The general problem of the beam on elastic foundation (Winkler's theory) is described by ordinary differential equation. In the most situations, the influences of normal force, shear force, distributed moment and temperature can be neglected (or the beam is not exposed to them). Hence

$$\frac{d^4v}{dx^4}+\frac{\mathrm{b}\,K(x)}{EJ}v=\frac{\mathrm{q}}{EJ},$$

where $K(x)$/Nm^{-3}/ is modulus of the foundation which can be expressed as functions of variable x/m/, b/m/ is width of the beam, $v = v(x)$/m is deflection of the beam and EJ is bending stiffness.

Solved beam (Fig. 1) of length L/m/ with free ends is exposed to one vertical force F/N/ and distributed loading q is zero. Modulus of the foundation is given by $K(x) = K_0 + K_1x$.

The approximate solution $v = v(x)$ can be found in the form of polynomial function of 6th order. Hence, the approximate results (i.e. functions of displacement v, slope, bending moment and shearing force of the beam) can be derived. This example is solved via probabilistic approach by Simulation-Based Reliability Assessment (SBRA) Method (i.e., all inputs are given by bounded histograms, AntHill software, see Fig. 2) which is the modern and new trend of the solution in mechanics.

Results parameters (i.e. stiffness of the foundation $k(x)$, displacement $v(x)$, maximal bending stress σ_{MAX}, factor of safety $F_S = R_e - \sigma_{MAX}$ etc.) were calculated for 5×10^6 simulations by Monte Carlo Method. Some results are plotted by histogram in Fig. 3 (distribution of yield stress versus σ_{MAX}).

Hence, the probability that the plastic deformations occurs in the beam is 0.094%. For more information see full version of this text.

This work has been supported by the Czech-USA project LH11073 - KONTAKT II.

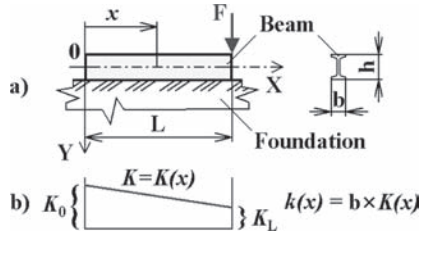


Figure 1. Solved beam on elastic variable foundation.

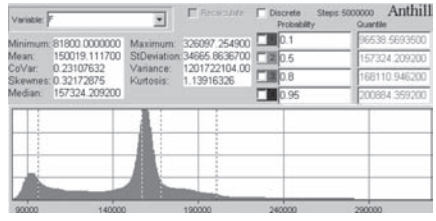


Figure 2. Histogram of input parameter F/N/.

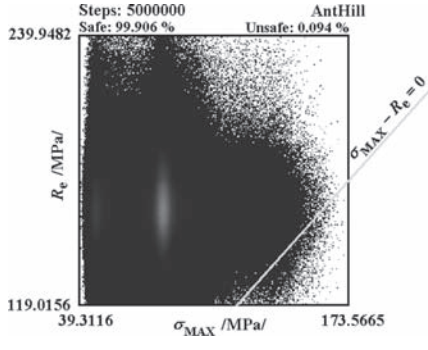


Figure 3. 2D histogram of output parameters (calculation of F_S).

REFERENCES

Frydrýšek, K. & Nikodým, M. 2010. Beams and Frames on Elastic Foundation 3, VŠB - Technical University of Ostrava, ISBN 978-80-248-2257-0, Ostrava, Czech Republic, p. 607.

Marek, P., Guštar, M. & Anagnos, T. 1995. Simulation-Based Reliability Assessment for Structural Engineers, CRC PRESS, INC., Boca Raton, Florida, USA, p. 365.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Deterioration model for large reinforced concrete structures

M. Sykora & M. Holicky
Czech Technical University in Prague, Klokner Institute, Prague, Czech Republic

1 INTRODUCTION

Durability is becoming an important issue of structural design. General principles on the probabilistic approach to verification of structural durability are provided in ISO 13823 (2008). Limited experience with the use of the document indicates that additional studies focused primarily on models of material deterioration and acceptance criteria are required. For large surfaces, spatial variability of basic variables needs to be considered. A simplified deterioration model is proposed in the study as an operational alternative to random field techniques.

2 SIMPLIFIED MODEL FOR SPATIAL VARIABILITY OF DETERIORATION AND NUMERICAL EXAMPLE

A large surface exposed to deterioration effects should be analysed as an assembly of elementary surfaces rather than a whole structure. Probabilistic characteristics of the variables influencing the deterioration should then include also the spatial variability of the variables among elementary surfaces. In the present study it is assumed that:

- The basic variables can be divided into spatially variable quantities $\mathbf{X}_{\text{loc}}$ and quantities attaining a single value for a whole structure $\mathbf{X}_{\text{glob}}$,
- Basic variables $\mathbf{X}_{\text{loc}}$ form homogeneous random fields; in an approximation values of $\mathbf{X}_{\text{loc}}$ in elementary surfaces are considered as independent, identically distributed variables.

The failure probability at a whole surface becomes:

$$P_{\text{f}}(t) = \text{E}_{\mathbf{X}\text{glob}}\{\text{P}[n_{\text{deg}}(t,\mathbf{X}_{\text{loc}}|\mathbf{x}_{\text{glob}}) / N \geq \alpha_{\text{lim}}]\} \qquad (1)$$

where $n_{\text{deg}}(\cdot)$ = number of elementary surfaces for which the limit state is exceeded; N = total number of elementary surfaces; and α_{lim} = limiting deterioration level. The number n_{deg} is obtained from the binomial distribution, which decreases computational demands compared to random filed models.

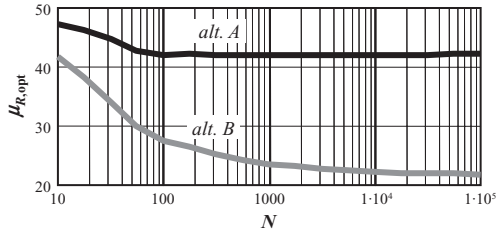


Figure 1. Variation of the optimum mean concrete cover $\mu_{R,\text{opt}}$ with the number of elementary surfaces N.

In a numerical example, a large concrete surface is investigated combining the proposed model for spatial deterioration and model for point-in-space carbonation depth provided in fib (2006). Concrete cover is optimised by the cost minimisation. Variation of the optimum concrete cover $\mu_{R,\text{opt}}$ on N is shown in Figure 1. When all random variables are assumed to be spatially variable (*alt. B*), lower optimum concrete covers are obtained than for the more acceptable *alt. A* based on $\mathbf{X}_{\text{loc}}$ and $\mathbf{X}_{\text{glob}}$.

3 CONCLUDING REMARKS

Spatial variability may significantly affect structural durability and the optimum design. Compared to random fields, the proposed model may require less input data and lower computational demands.

ACKNOWLEDGEMENTS

The study has been conducted within the projects GACR 103/09/0693 and TA01031314.

REFERENCES

Fib 2006. *Model Code for Service Life Design*. Lausanne: fib.
ISO 13823: 2008. *General principles on the design of structures for durability*. Geneve, Switzerland: ISO.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Development of representative seismic fragility function for bridge group by using results of safety factor

M.K. Kim, I.-K. Choi & D.G. Hahm
Korea Atomic Energy Research Institute, Daejeon, Republic of Korea

ABSTRACT

The purpose of this study is a development of a seismic fragility function for railway bridge group based on the results of previous results of seismic safety factor analysis. The results of fragility evaluation of bridge group which developed in this study can be applied to HAZUS for the evaluation of seismic risk. The safety factor is a result of deterministic safety analysis of each bridge system. The safety factors were determined by numerical analysis about failure criteria.

For the evaluation of seismic fragility function for bridge group, safety factors which developed by previous research were used. The safety factors which used in this study were developed considering 54 bridges and eight failure parameters. First, a failure status of structural member was defined according to results of safety factor analysis. The failure status was classified as slight damage, intermediate damage, extensive damage and complete damage like HAZUS. Each damage status was defined as combination of failure of structural member of bridge system.

Second, a fragility function for each of the bridge members was evaluated according to the damage criteria and failure mode. The failure criteria were considered as failure of column, pier and shoe of bridge system and unseating of bridge. The failure was considered a longitudinal and a transverse direction of bridge system. Subsequently, bridge system fragility was evaluated using a fault tree to describe damage status.

Finally, a fragility evaluation method for the bridge system was developed, based on the safety factor derived from the previous research.

Table 1. Element damage status for determination of seismic fragility evaluation for bridge system.

Damage Status of whole system	Damage status of bridge member		
	Damage of shoe	Deck collapse	Damage of pier
Slight damage	Extensive damage	Slight damage	Slight damage
moderate damage	Complete damage	Moderate damage	Moderate damage
Extensive damage	X	Extensive damage	Extensive damage
Complete damage	X	Complete damage	Complete damage

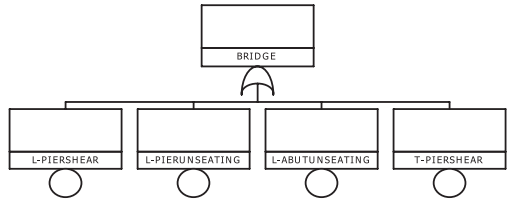


Figure 1. Fault tree for the evaluation of extensive damage and complete damage.

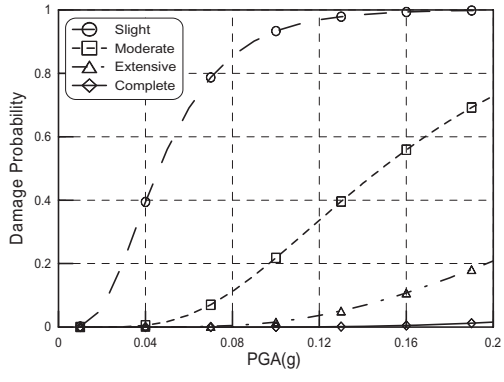


Figure 2. Seismic fragility results of bridge group.

REFERENCES

Ang, Alfredo H.-S. & Tang, Wilson H., Probability Concepts in Engineering Planning and Design, John Wiley & Sons., 1975.

FEMA, HAZUS99 Technical Manual, 1999.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Fatigue loading estimation for road bridges using long term WIM monitoring

M. Treacy & E. Brühwiler
Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland

ABSTRACT

Transport networks form a huge part of a countries assets with the highway system usually the densest component. As bridges form the keystone of these networks, their safe operation with minimal maintenance closures is paramount for efficient operation. Yearly increases in the volume of heavy traffic means a higher number of fatigue damaging load cycles in road bridges. With recent improvements in durability of materials and proactive maintenance strategies, fatigue requires increased consideration.

To efficiently manage a large bridge stock, knowledge of individual bridge fatigue safety is required. While whole life monitoring of all bridges offers the best solution theoretically; the sheer number of bridges, manpower, energy and data storage requirements make it unsustainable at present. This work develops a methodology for the estimation of fatigue load cycles and hence fatigue safety in short to medium span bridges for today's highway traffic.

Theure study utilises real traffic streams from Weigh-in-Motion (WIM) monitoring within the Swiss highway network performed continuously over a number of years. The concept of a Standard Fatigue Bridge Model (SFBM) is introduced which provides long term fatigue cycle data for road bridges based on the real traffic data. An algorithm was developed which simulates the vehicle passages over a bridge model and calculates load effects using the axle positions recorded in real time from the WIM data.

This paper presents an update of the work to date in establishing traffic fatigue cycle load effects from over 7 million heavy vehicle recordings over a 3 year period which can be utilised for improved fatigue safety verification. This information could serve as an identification tool for bridges within a stock where fatigue is likely to be a problem.

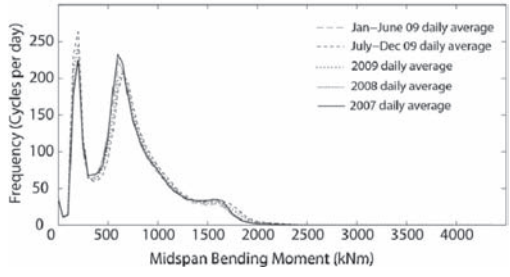


Figure 1. Comparison of midspan bending moment cycles over 3 years for a simply supported 25 m span bridge using traffic in Zurich direction at Mattstetten A1 WIM station, Switzerland.

Table 1. Statistical information on cleaned traffic data set for Mattstetten A1 motorway WIM station.

WIM station	2007	2008	2009
Zurich direction			
GVW > 3.5 t	1,090,330	1,103,443	1,100,071
Mean GVW (t)	17.0	17.1	17.4
Mean Axle load (t)	4.63	4.62	4.71
Max GVW (t)	97.3	99.0	102
Bern direction			
GVW > 3.5 t	1,254,036	1,246,402	1,227,014
Mean GVW (t)	17.0	16.9	17.1
Mean Axle load (t)	4.90	4.81	4.87
Max GVW (t)	98.8	97.9	99.0

REFERENCES

Brühwiler, E. 2008. Rational approach for the management of a medium size bridge stock. IABMAS'08: 4th International Conference on Bridge Maintenance, Safety and Management, Seoul.

FEDRO. 2010. Traffic Survey - Analysis of WIM data for 2007 (In German). Bächtold & Moor / Swiss Federal Roads Authority (FEDRO), Bern.

Jacob, B. & Labry, D. 2002. Evaluation of the Effects of Heavy Vehicles on Bridges Fatigue. 7th International Symposium on Heavy Vehicle Weights & Dimensions, Delft.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Finite difference modeling of formation damage during underbalanced drilling in a tight gas reservoir

M. Naseri
Chemical Engineering Department, Sahand University of Technology, Tabriz, Iran

S.R. Shadizadeh
Ahwaz Faculty of Petroleum Engineering, Petroleum University of Technology, Ahwaz, Iran

E. Sahraei
Chemical Engineering Department, Sahand University of Technology, Tabriz, Iran

S.S. Ghorashi
Research Institute of Petroleum Industry (RIPI), Tehran, Iran

ABSTRACT

Evaluating near wellbore formation damage is a vital factor to deal with tight gas reservoirs due to their low permeability and porosity, high capillary pressure and sub-irreducible water saturation. Based on these properties, Counter-Current Spontaneous Imbibition (COUCSI) damage occurs during underbalanced drilling in the presence of water-based mud systems. Although there are some analytical and numerical models describe COUCSI process, to date, nobody has presented a numerical or analytical model to investigate the effect of COUCSI in water invasion during UBD and its resulting influences on formation damage and hydrocarbon phase permeability reduction.

This paper presents a numerical model to determine water saturation profile during underbalanced drilling in a tight gas reservoir which is mainly because of COUCSI. This model provides significant value by evaluating water invasion and the resulting drop in gas permeability, resulting in a better understanding of formation damage and its consequent effects. Additionally, understanding the potential damage resulting from temporarily overbalanced conditions highlights the importance of completing the well in an underbalanced mode.

During UBD with a drilling fluid alike wetting phase for the reservoir rock, the capillary pressure acts as a counter-current force that leads to flow of drilling fluid towards the reservoir. The differential form of the governing equations can be derived from mass balance and Darcy's equations for two-phase flow model. Applying the required initial and boundary conditions and then solving it using numerical methods, gives water saturation profile. Comparing the new water saturation values with the initial water saturation, can illustrate the amount of invaded water and its resulting reduction in effective gas permeability, which in turn, decreases gas production rate.

One of the other outputs of this model is water invasion depth (damaged zone radius) that can be useful for skin factor calculation. Damaged zone radius is a vital factor in acidizing and further reservoir engineering calculations.

Figure 1 shows water saturation profile in the near wellbore region which can be interpreted as the formation damage during UBD due to COUCSI.

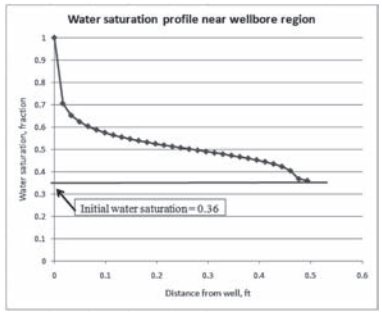


Figure 1. Water saturation profile in the near wellbore region during a 20 hr underbalanced drilling operation.

REFERENCES

Kashchiev, D. & Firoozabadi, A. Analytical Solutions for 1D Countercurrent Imbibition in Water-Wet Media. *SPE Journal, Vol. 8, No. 4, December, 2003*: 401–408.

Naziri Khansari, A. Evaluation of Well Productivity Loss Due to Formation Damage Caused by Spontaneous Imbibition in Underbalanced Drilling. SPE Paper 122268. *IADC/SPE Managed Pressure Drilling and Underbalanced Operations Conerence and Exhibition. 12–13 Febrauary 2009.* San Antonio: USA.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Laboratory simulation technique of non-stationary random vibration environment

C. Mao, Y. Jiang, J. Tao & X. Chen
College of Mechatronic Engineering and Automation, National University of Defense Technology, Changsha, Hunan, China

ABSTRACT

While analyzing the structural dynamic response, random vibration loads are usually assumed to obey stationary Gaussian distribution. But technically, in severe occasions, such as strong winds, storms, earthquakes, tsunamis, explosive blast waves etc, the random excitations that machinery and engineering structures undergo feature non-stationary. Large-scale machinery, such as aircrafts, high-speed rail transportations, offshore platforms, etc, also produce random vibration with a significant characteristic of non-stationary when their operating environment is unstable or faulty. Besides these, non-stationary random vibration might occur during transporting under unstable conditions, for instance, when vehicle accelerates, decelerates or drives on uneven roads. The damages caused by stationary and non-stationary random vibration are different due to their very different characteristics in frequency domain. Currently, the requirements of Environmental Testing and Reliability Testing can't be met that simulating environment accurately due to lacking of simulation methods and experimental equipments on non-stationary random vibration. Under the circumstances, some primary research was made in this paper on simulating cyclostationary random vibration environment which is a kind of non-stationary stochastic processes: firstly, the characteristics of Cyclic Mean and the periodic properties of Linear Periodic Time-Varying system were discussed; secondly, a Linear Periodic Time-Varying system was established to generate cyclostationary random signals with specified statistical parameters, whose structure was built based on trigonometric function and whose coefficients were determined by Least Mean Square algorithm; finally, the signals were loaded to electrodynamic shaker and simulated cyclostationary random vibration environment successfully. This method was verified by numerical simulations and practical experiments, which could be applied to dynamic optimization, fault diagnosis and reliability assessment of engineering structures and machinery.

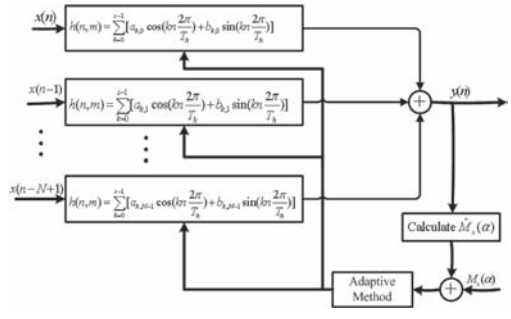


Figure 1. Structural diagram of Linear Periodic Time-Varying system.

REFERENCES

Boyles, R.A. & Gardner, W.A. 1983. Cycloergodic Propertied of Discrete Parameter Nonstationary Stochastic Process. *IEEE Trans. on Information Theory*. 29(1): (105–114).

Gardner, W.A. 1993. Cyclic Wiener Filtering: Theory and Method. *IEEE Trans. on Communications*. 41(1): (151–163).

Gardner, W.A. & Frank, L.E. 1975. Characterization of Cyclostationary Random Signal Processes. *IEEE Trans. on Information Theory*. 21(1): (4–14).

Haykin, S. 1986. *Adaptive Filter Theory*. Englewood Cliffs, New Jersey: Prentice Hall.

Zhu, Z.K. & Feng, Z.H. 2005. Cyclostationarity Analysis for Gearbox Condition Monitoring: Approaches and Effectiveness. *Mechanical System and Signal Processing*. 19: (167–182).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Performance of passive fire protection for liquefied petroleum gas vessels: An experimental and numerical study

M. Gomez-Mares, S. Larcher, A. Tugnoli & V. Cozzani
Alma Mater Studiorum—Università di Bologna, Dipartimento di Ingegneria Chimica, Mineraria e delle Tecnologie Ambientali, Bologna, Italy

F. Barontini & G. Landucci
Università degli Studi di Pisa, Dipartimento di Ingegneria Chimica, Chimica Industriale e Scienza dei Materiali, Pisa, Italy

ABSTRACT

Fire is among the most dangerous accident scenarios that may affect the process industry. Vessels containing pressurized liquefied gases are particularly vulnerable to external fires, since an increase in the vessel temperature by a fire scenario may result in both the rise of the internal pressure and the weakening of the vessel structure. Vessel failures due to accidental fires may yield a significant escalation of accident severity, either by the release of the vessel content or by overpressure generation in the case of catastrophic failure (BLEVE). Passive Fire Protection (PFP) is a robust and effective solution to reduce the probability of accident escalation. In particular, fireproofing delays the temperature rise of the protected surfaces retarding vessel heat up and failure (CCPS 2003).

The assessment of the behaviour of the materials exposed to fire is a critical issue for determining the effectiveness of the PFP system. In particular, thermal coatings may undergo degradation (e.g., devolatilization) that causes the variation of key physical properties during prolonged fire exposure. Though the thermal degradation may be an inherent part of the protective action of the coating (e.g., in the case of intumescing coatings), the progressive deterioration of the material may lead to a decrease in the performance of the protection.

Although some large scale tests on vessels have been carried out (Landucci et al., 2009, VanderSteen & Birk, 2003), further studies are required in order evaluate the effectiveness of PFP systems. It has to be considered that this type of tests is expensive and hazardous. Coping with smaller scale tests and modelling is thus advisable to obtain a more effective route to explore this issue. Finite element modelling (FEM) combined with experimental tests at small scale can be an option which allows to study in depth these systems in a safe and reliable way.

In the present study, an approach to the assessment of the effectiveness of PFP systems is presented. The approach integrates experimental results and finite element modelling. This allowed predicting the expected behaviour of real scale pressurized tanks engulfed by fires. The behaviour of a commercial epoxy intumescent PFP material exposed to temperatures up to 800ºC was analyzed using Thermogravimetric Analysis. The results allowed identifying the main decomposition regions of the PFP. Small samples of PFP were exposed to different temperature histories in a fixed-bed tubular reactor, allowing further characterization of the material degradation behaviour (e.g. morphological, swelling). The data collected in these lab-scale experiments can be used to define an apparent kinetic model for property variation of the PFP material, as well as correlations which allow to predict the expansion, the bulk density and the thermal conductivity of the material with temperature.

At the same time, a Finite Elements Model (FEM) for LPG vessels was developed for simulation of real scale vessels. The model considers a simplified failure criterion, combining temperature and stress distribution, for the evaluation of the time to failure.

A preliminary study, resorting to the obtained experimental data, was carried out comparing the behaviour of coated and uncoated tanks. The results evidenced that the time to failure is clearly increased by PFP coating, but the correct modelling of PFP modification during fire exposure is identified as critical for the definition of PFP effectiveness.

REFERENCES

Center for Chemical Process Safety (CCPS), 2003. Guidelines for Fire Protection in Chemical, Petrochemical, and Hydrocarbon Processing Facilities, New York: CCPS/AIChE.

Landucci, G., Molag, M., Reinders, J. & Cozzani, V. 2009. Experimental and analytical investigation of thermal coating effectiveness for 3m3 LPG tanks engulfed by fire. Journal of Hazardous Materials 161: 1182–1192.

VanderSteen, J.D.J. & Birk, A.M. 2003. Fire tests on defective tank-car thermal protection systems. Journal of Los Prevention in the Process Industries 16: 417–425.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic approaches used in the solution of design for biomechanics and mining

K. Frydrýšek
VŠB—Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

Let us consider the Simulation-Based Reliability Assessment Method (SBRAM), a probabilistic Monte Carlo approach, in which all inputs are given by bounded histograms. In SBRAM, the probability of failure or undesirable situation is obtained mainly by analyzing the reliability function RF = RV – S, see Fig. 1. Where RV is the reference value and S is the load effect combination. The probability of failure is $P(\mathrm{RF} \leq 0)$.

This paper focuses on the probabilistic numerical solution of the problems in biomechanics and mining. Applications of SBRAM are presented in the solution of designing of the external fixators applied in traumatology and orthopaedics (these fixators can be applied for the treatment of open and unstable fractures etc., see Figs. 2 and 3) and in the solution of a hard rock (ore) disintegration process (i.e., the bit moves into the ore and subsequently disintegrates it, the results are compared with experiments, new design of excavation tool is proposed, see Fig. 4).

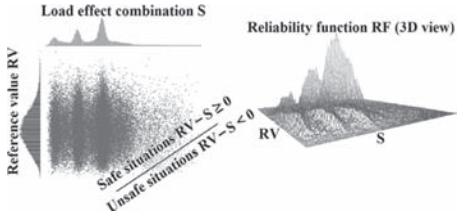


Figure 1. Reliability function RF (SBRAM).

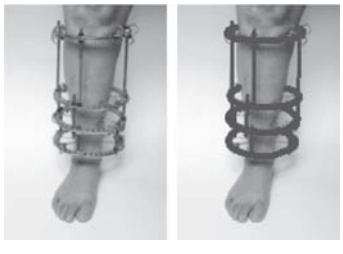


Figure 2. Design of external fixators a) based on metals—current design, heavier, expensive etc. b) based on polymers reinforced by carbon nanotubes—new design, lighter, x-ray invisible—leads to shortening the operating time and reducing the radiation exposure of patients and surgeons, with antibacterial protection cheap, more friendly etc.).

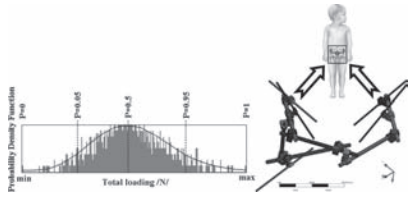


Figure 3. Typical loading spectrum of an external fixator and numerical modelling for treatment of pelvis and acetabulum.

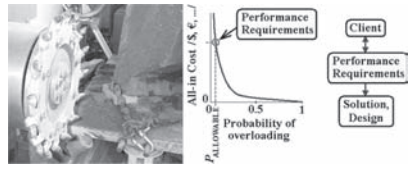


Figure 4. Example of interaction between bits and hard rock and definition of the acceptable probability of overloading.

This work has been supported by the Czech-USA project LH11073-KONTAKT II and by Czech project MPO FR-TI3/818.

REFERENCES

Frydrýšek, K. 2009. Stochastic Solution and Evaluation of the Ore Disintegration Process, In: Proceedings of the 2009 International Conference on Scientific Computing CSC2009, ISBN: 1-60132-098-1, CSREA Press, Las Vegas, USA, pp. 40–46.

Frydrýšek, K., Pleva, L. & Koštiál, P. 2010. New Ways for Designing External Fixators Intended for the Treatment of Open and Unstable Fractures, In: "Applied Mechanics 2010" 12th. International Scientific Conference (Proceedings), Department of Applied Mechanics, Faculty of Mechanical Engineering, Technical University of Liberec, Liberec, Czech Republic, ISBN 978-80-7372-586-0, pp. 43–47.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Probabilistic assessment of an aged highway bridge under traffic load

R.D.J.M. Steenbergen, J. Maljaars, O. Morales Nápoles & L. Abspoel
TNO, Delft, The Netherlands

ABSTRACT

Existing civil infrastructure represents a large economic value. Within the actions applied to the bridges, the traffic load is, in general, the most significant variable action to be considered when the ultimate limit states are under investigation. Consequently, the traffic load models play an important role in the design of new bridges but also in the reliability assessment of existing structures. This article evaluates the safety of an existing highway bridge in the Netherlands. In order to determine whether the structure can be safely used up to the moment of renovation, a probabilistic assessment of the bridge was performed. Important part of that study was a measurement program in order to determine the distribution of the stresses in the main load bearing structure due to the traffic load. From these measurements the design stresses were extrapolated using a technique for fitting an extreme value distribution to the measured data. Design stresses should be derived such that they provide a sufficient safety level of the bridge. After the semi-probabilistic analysis for all the bridge elements, for one bolted connection in the bottom flange of a main girder, a probabilistic calculation is performed in order to establish the safety level, avoiding all schematizations and possible conservatisms in the calculation rules.

This paper describes an assessment method for the structural safety of an existing bridge during a calamity situation where one or more lanes are closed down. The method is aimed at determining the actual safety level of an existing high way bridge by focusing on the accurate determination of the actual traffic load effects. A probabilistic calculation is performed for a bolted connection in the bottom flange at midspan of one of the main girders. It is aimed to assess the safety level of the bridge according to EN 1990 and the requirements specially developed for existing structures by Vrouwenvelder (2010) and by Steenbergen and Vrouwenvelder (2010).

At the location of the connection under consideration, the stresses due to the traffic load were measured using a strain gauge. For the analyses, the distribution of the daily extreme stress has to be derived from the measurements.

A probability density function was fitted to the obtained maxima resulting in a Weibull distribution. Because of the limited time of measurement, the uncertainty in the standard deviation in the Weibull distribution is taken into consideration explicitly. As basis for the strength model of the bolted connection, experiments were used to determine the strength functions and suitable model factors. The distribution functions belonging to the stresses due to the permanent actions and other variable actions were determined using FEM models, measurements, expert judgment and prescriptions given in the JCSS probabilistic model code.

The result is a reliability index of $\beta = 4.3$ for the connection plates for a one day reference period. For existing bridges in The Netherlands, for calamity situations the required reliability index is $\beta = 3.3$ for a minimum reference period of one month. It is concluded that the requirement is fulfilled and that the bridge is safe enough during the calamity situation.

In the paper a receipt is proposed leading to a safety assessment as realistic as possible and therefore including conservatisms as little as possible. This leads to larger lifetimes of existing bridges and viaducts.

REFERENCES

Steenbergen, R.D.J.M. and Vrouwenvelder, A.C.W.M., Safety philosofy for existing structures and partial factors for traffic load on bridges, *Heron 55 no. 2*, 2010.

Vrouwenvelder A.C.W.M. and Scholten N.P.M., Assessment Criteria for Existing Structures, *Structural Engineering International 1/2010*.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic modelling of hygro-thermal performance of building structure

Z. Sadovský, O. Koronthályová & P. Matiašovský
Institute of Construction and Architecture, Slovak Academy of Sciences, Bratislava, Slovakia

ABSTRACT

A probabilistic model of the hygro-thermal performance of the internal surface of an external wall is suggested. Particularly, the daily exceedances of the critical value of relative humidity on the surface during the first year of its transition from 'as built' state to the quasi steady state are studied.

The time dependent internal/external loads are represented by one concrete realization, related to the climate parameters of the site and the activities of inhabitants. In calculations, the hourly measurements of the external temperature, air relative humidity and solar radiation over one year period are adopted. The indoor air temperature is considered as practically constant, which corresponds to the use of an ideal heating system. The indoor air relative humidity results from the activities of inhabitants and the external climatic conditions.

Among the quantities characterising building structure composition, three selected material functions—water vapour permeability, moisture diffusivity and thermal conductivity are described by random variable parameters. The probabilistic model relates to the deterministic 1D simulation of heat and moisture transfer through the building structure, which has been algorithmised in the code NEV3. The time dependent values of relative humidity on internal surface of an external wall resulting from NEV3 calculations are analysed for daily durations of the critical threshold exceedances. Employing the Poisson spike process, the first-passage probability of exceeding a considered duration, conditioned by the actual values of the material parameters, is determined. The total probability is calculated by FORM.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Probabilistic models of thermal actions for bridges

J. Marková
Czech Technical University in Prague, Klokner Institute, Czech Republic

ABSTRACT

The paper is focused on the probabilistic models of thermal actions. It is foreseen that the thermal models will be applied for the probabilistic verification of bridges and other structures. The thermal models may also be used for the calibration of partial factors and reduction factors of thermal actions.

The basic variables influencing the effects of thermal actions on structures include climatic agents, operating process temperatures, characteristics of construction works and properties of atmosphere and terrain. Random properties of these variables may significantly affect the probabilistic analysis.

Four basic components of temperatures are distinguished as given in EN 1991-1-5 (2005). Shade air temperatures have considerable effect on the uniform temperature component being mainly influenced by the daily and seasonal changes, the location of the site (altitude above the sea level, configuration of terrain) and the wind velocity. Solar radiation influences the temperature difference components in the horizontal and vertical direction and partly also the uniform temperature component.

Variation of the upper bound of temperatures x_{sup} with the skewness α considering Weibull distribution is shown in Figure 1.

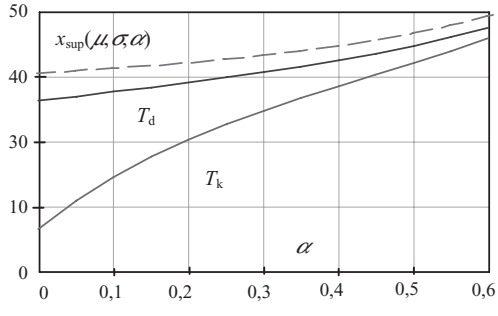


Figure 1. Variation of the upper bound of temperatures $x_{sup}(\mu,\sigma,\alpha)$ in m, the characteristic and design values of temperatures with the skewness α for Weibull distribution.

It appears that despite the Eurocodes recommend the application of the Gumbel distribution for modelling of all climatic loads including thermal actions, the temperature components may be better represented by Weibull distribution. The skewness of the statistically evaluated data of temperature measurements is in a range from –0,2 to 0,4 what is considerably less than the skewness of the Gumbel distribution.

The results of analysis of temperatures based on the experimental bridge measurements indicate that the partial factors of both the uniform and difference temperature components may be reduced to 1,2 for steel and composite steel-concrete bridges and to 1,3 for concrete bridges.

It appears that the application of the unique value of partial factor for all climatic actions in the ultimate limit states should be reconsidered during the period of revisions and maintenance of Eurocodes.

REFERENCES

Background document. 1999. *New European Code for Thermal Actions*. University of Pisa.

EN 1990. 2002. Basis of structural design. CEN.

EN 1991-1-5. 2005. Actions on structures. Part 1–5: General actions – Thermal actions. CEN.

ISO/TR 9492. 1987. Basis for design of structures – Temperature climatic actions.

Marková, J. 2005. Analyses of Temperature Models on Bridges, *Proceedings of the second international conference Reliability, Safety and Diagnostics of Transport Structures and Means 2005*, pp. 217–223, Pardubice, Czech Republic. 2005, pp. 217–223.

Marková, J. & Holický, M. 2010. Serviceability Criteria in Current Codes, In: *Codes in Structural Engineering. Developments and Needs for International Practice*. pp. 887–894, Zagreb, pp. 887–894.

PMC. 2003. Probabilistic Model Code. Joint Committee on Structural Safety.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability based design in tunnelling

M. Huber, P.A. Vermeer & C. Moormann
Institute of Geotechnical Engineering, University of Stuttgart, Stuttgart, Germany

M.A. Hicks
Delft University of Technology, Delft, The Netherlands

ABSTRACT

1 DESIGN PROBLEM FROM A RELIABILITY PERSPECTIVE

The presence of uncertainties and their significance in relation to design has long been appreciated. The engineer recognizes, explicitly or otherwise, that there is always a chance of not achieving the design objective. This element of risk arises, in part, from the inability to assess loads and resistances with absolute precision. Traditionally, the engineer relies primarily on empirical factors of safety to reduce the risk of adverse performance (collapse, excessive deformations, etc.) to an acceptable level. However, the relationship between the factor of safety and the underlying probability of failure is not a simple one. A larger factor of safety does not necessarily imply a smaller probability of failure, because its effect can be negated by the presence of larger uncertainties in the design environment. In addition, the effect of the factor of safety on the underlying probability of failure is also dependent on how conservative the design models and the design parameters are, according to Phoon (1995). As stated by Phoon (1995), the problem associated with the traditional method of ensuring safety can be resolved by rendering broad, general concepts, such as uncertainty and risk, into precise mathematical terms that can be operated upon consistently. This approach essentially forms the basis of Reliability Based Design (RBD), in which uncertain engineering quantities (e.g., loads, capacities) are remodelled by random variables.

2 SUMMARY AND CONCLUSIONS

Within this contribution, the concept of RBD has been explained for two problems in shallow tunnelling. For the problems of tunnel heading stability and the design of the tunnel lining, a cohesive, frictional soil was assumed.

For the probabilistic evaluation of the heading stability, a limit state equation derived from FEM studies was used in two parametric studies into the influence of the variability of soil, geometry and construction process on the probability of failure. The assumption of uncorrelated shear strength parameters was found to be conservative (i.e., it gives a greater probability of failure) in comparison to that of negatively correlated parameters. Moreover, it was shown that the probability of failure is more sensitive to the friction angle than to the cohesion. The results of the parametric studies suggest that the strength parameters of the soil and the tunnel face pressure have the major influence on the probability of failure, in comparison to the soil unit weight and tunnel diameter. The findings of these investigations are compared to the state of the art as presented in CEN (2004). In the case of the tunnel lining design, a closed form solution of a continuum mechanical problem was adapted in order to quantify the influence of soil variability.

This contribution has clearly shown the severe influences of soil variability for two problems in tunneling. It can be concluded that there is a need for additional studies in reliability based design, as in Phoon (2008), in order to get more experience in modelling the influence of variability in geotechnical engineering. Moreover, the linkage between the reliability approach and numerical methods would offer a powerful approach for modelling uncertainty. It would also be useful to aim for reliability based design optimisation, in order to contribute to a cost effective design, as proposed by Lemaire et al. (2009).

REFERENCES

CEN (2004). Eurocode 7 Geotechnical design - Part 1: General rules. EN 1997-1:2004.

Lemaire, M., Chateauneuf, A. & Mitteau, J. (2009). *Structural reliability*. Wiley Online Library.

Phoon, K. (Ed.) (2008). Reliability-Based Design in Geotechnical Engineering - Computations and Applications. Taylor & Francis.

Phoon, K.K. (1995). *Reliability-based design of foundations for transmission line structures*. Ph.D. thesis, Cornell University.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Small failure probability assessment based on subset simulations: Application to a launcher structure

C. Elegbede & F. Normand
Astrium, RAMS and Nuclear Safety Analysis Department, France

ABSTRACT

The standard formulation of structural reliability problem consists of integrating the probability density function of the random vector describing the structure, onto the failure domain. It is common to use Monte Carlo simulation or numerical scheme for the purpose. The difficulties appear when one wants to assess very small failure probabilities with good precision using Monte Carlo simulations. The number of simulations may not be reasonable despite the use of variance reduction techniques. Therefore, a good alternative to classical Monte Carlo may be the subset simulation approach proposed recently by Au et al. which bypasses the need to simulate rare samples for estimating small probabilities. By introducing intermediate failure boundaries, the failure probability is expressed as a product of conditional probability, the evaluation of which only requires simulation of more frequent events. In this paper, some investigations are performed to tune and assess the subset simulation algorithm. Subset simulation algorithm is described and the choices of the algorithm parameters are discussed.

With the basic stress-strength model for which analytical and exact numerical results are available, the failure probability has been assessed. This enables us to have an idea on the number of simulations to be performed according the target safety failure in consideration. The results obtained with the sets of benchmark show the advantage and the efficiency of subsets simulations.

The results obtained with the sets of benchmark shows the advantage and the efficiency of subsets simulations. An algorithm based on subset simulation is assessed. The buckling probability of launchers thin-walled cylindrical structure, subjected to safety requirements, is studied as application of the method for axial compression and external pressure. In addition, a benchmark is provided to illustrate the efficiency of the method used. Subset simulations give the same results as classical Monte Carlo simulation but is less costly time consumer. In engineering point of view, these results are relevant, particularly, for structural analysis if one wants to link reliability code to finite elements code.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty analysis of ultimate limit state of steel bar structures

Z. Kala
Brno University of Technology, Brno, Czech Republic

ABSTRACT

The objective of the present study is an analysis of the influence of number of members under tension on the general random load-carrying capacity of a structure. The analytical mathematical model was applied for calculation of load-carrying capacity.

The analytical mathematical model was applied for calculation of load-carrying capacity. For structure presented in Fig. 1, it is necessary to consider that the load-carrying capacity of any supporting member under tension is higher than the effect produced by the load *F*. The load-carrying capacity of each member under tension is the statistically independent random quantity determined as a multiple of cross-section area and of yield point. The general load-carrying capacity of a structure is equal to the minimum value of load-carrying capacity of individual members under tension.

Eight structures were solved with the number of members from 2 to 9. The random load-carrying capacity depends on the random area and on random yield point, and these are the quantities known from experimental research. The statistical analysis was evaluated by means of the Monte Carlo method for 100 000 simulations.

The change both of mean value and standard deviation of load-carrying capacity of the structures is evident. With increasing number of members under tension, the mean value decreases and, at the same time, also the standard deviation does. The maximum difference between mean values is approximately 6%. The standard deviation of the system with two members is approximately by 41% higher in comparison with the system having 9 members. From the point of view of reliability, the design value is important above all; it is calculated, according to the standard EN1990, as 0.1 percentile. The maximum difference between design values is approximately 1.4%. When considering the differences between mean values and design values, the difference 1,4% is very low.

The article was elaborated within the framework of projects of AVČR IAA201720901, GAČR 105/10/1156 and CIDEAS No. 1M0579.

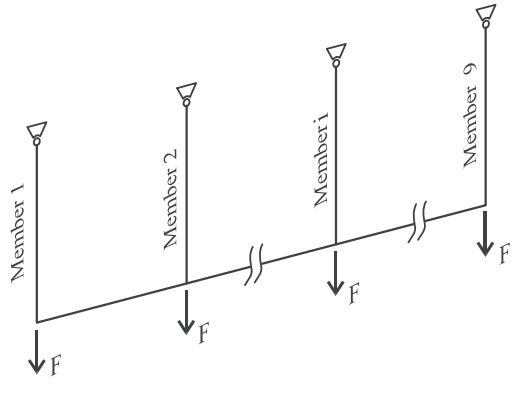


Figure 1. System of members under tension.

REFERENCES

Kala, Z. 2005. Sensitivity analysis of the stability problems of thin–walled structures. Journal of Constructional Steel Research, 61(3): 415–422. doi:10.1016/j.jcsr.2004.08.005.

Kala, Z. 2011. Sensitivity analysis of stability problems of steel plane frames. Thin-Walled Structures, 49(5): 645–651.

Kala, Z., Melcher, J. & Puklický, L. 2009. Material and geometrical characteristics of structural steels based on statistical analysis of metallurgical products. Journal of Civil Engineering and Management, 15(3): 299–307.

Kala, Z., Puklický, L., Omishore, A., Karmazínová, M. & Melcher, J. 2010. Stability Problems of Steel-Concrete Members Composed of High Strength Materials. Journal of Civil Engineering and Management, 16(3): 352–362.

Melcher, J., Kala, Z., Holický, M., Fajkus, M. & Rozlívka, L. 2004. Design characteristics of structural steels based on statistical analysis of metallurgical products. Journal of Constructional Steel Research, 60(3–5): 795–808.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Updating partial factors for material properties of existing structures in a Eurocode framework using Bayesian statistics

R. Caspeele & L. Taerwe
Department of Structural Engineering, Ghent University, Ghent, Belgium

ABSTRACT

The assessment of existing structures becomes increasingly important and influences asset planning and decision making. However, currently a certain duality exists between on the one hand highly complex calculation methods and probabilistic or semi-probabilistic design methods for the design of new structures and on the other hand the current practice for the assessment of existing structures which most often relies on the (subjective) judgment of the investigating engineer.

The way in which laboratory and/or in-situ test results are incorporated in the safety assessment of existing structures can and should be improved and a better consensus should be looked for with respect to the required safety elements (e.g., target safety levels, partial factors, …) for existing structures and more particularly for those which have experienced deterioration. This would result in a coherent, less conservative and more objective basis for establishing improved criteria to decide when preventive actions should be taken and when and to what level an existing structure should e.g., be strengthened in order to meet the safety requirements.

This paper briefly describes some basic ideas regarding an updating procedure with respect to partial factors for material properties, considering a semi-probabilistic design philosophy that incorporates a Bayesian updating technique and is compatible with the current framework provided by the Eurocodes.

Normal-gamma and lognormal-gamma distributions form a class of natural conjugate priors that can be used to easily update hyperparameters for the probability density functions of material properties.

Further, a reduction factor is derived based on a simplified Level II approach in order to update the partial factors for material properties as given in the Eurocodes. More specifically, alternative values for the reliability index can be taken into account (considering cost optimization and remaining working life) and the additional information by in-situ and laboratory testing can be translated into an adjusted value for the partial factor of the material property under consideration. Figure 1 illustrates this reduction factor ω_γ in case the representative value X_{rep} of the material property corresponds to a 5% fractile, considering further also a reliability index for new structures as $\beta' = 3.8$ and a prior predictive coefficient of variation $\delta' = 0.15$. Figure 1 illustrates the influence of the ratio δ_X''/δ_X' of the posterior to the prior predictive coefficient of variation (based on the Bayesian updating of the hyperparameters) on the reduction factor ω_γ for different values of the target reliability index $\beta'' = \beta_t$ for existing structures.

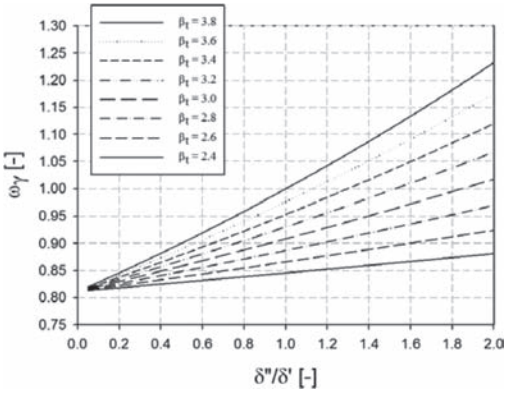


Figure 1. Influence of the ratio δ_X''/δ_X' on the reduction factor ω_γ considering $X_{rep} = X_k$ ($\alpha_R = 0.8$, $\beta' = 3.8$, $\delta' = 0.15$).

Based on these reduction factors, the updated partial factor can be calculated as:

$$\gamma_{X,exist} = \omega_\gamma \gamma_X \geq \gamma_{Rd} \tag{1}$$

with γ_X the partial factor available in the Eurocodes in case of new structures and considering additionally that the reduced partial factor for the material property in case of existing structures should not be smaller than the model uncertainty.

Finally, the developed methodology is illustrated in case of the partial factor for concrete strength.

This page intentionally left blank

System reliability analysis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

A fast augmentation algorithm for optimizing the performance of repairable flow networks in real time

M.T. Todinov
Oxford Brookes University, Oxford, UK

ABSTRACT

Repairable flow networks are a very important class of networks. Particular examples are the production networks, communication networks, transportation networks, energy distribution networks and supply networks. An essential feature of repairable flow networks is that a renewal of failed components is taking place after a certain delay for repair. There is no exaggeration in stating that most of the real flow networks are in fact repairable flow networks. Analysis and optimisation of repairable flow networks is a new, recently initiated area of research.

The paper continues the research on repairable flow networks by stating and proving a new theorem related to restoring the maximum flow in repairable flow networks. The maximum flow in a repairable flow network after a failure of several components can be restored very quickly by a two-stage procedure. The first stage consists of augmenting the *dual network* with a new source and a new sink as much as it is possible. The second stage follows the first stage and consists of augmenting the *dual circulation network* until all outgoing edges from the new source are fully saturated. The initial edge flows in the dual circulation network are the resultant edge flows obtained after augmenting the dual network.

On the basis of this theorem, a very efficient augmentation algorithm has been proposed for restoring the maximum flow in repairable flow networks after a failure of several components. For a single failed component, or few failed components, the average running time of the proposed algorithm is $O(m)$, where m is the number of components in the network. The running time of the proposed algorithm increases linearly with the size of the network and, currently, it is the fastest available algorithm for restoring the maximum flow in repairable flow networks.

The very high computational speed of the proposed algorithm makes it possible to control and optimize the performance of flow networks in real time. Upon failure, the network flows need to be redirected quickly in order to restore the maximum output flow. This is important for example for production networks, power distribution networks, computer networks, emergency evacuation networks, etc. The algorithm is also suitable for designing discrete-event simulators of production systems, where, in order to track correctly the variation of the output flow, the maximum flow needs to be calculated many times, after each component failure and return from repair.

The paper also presents for the first time a study on the link between the topology of complex flow networks with redundancy and their *threshold flow rate reliability*—the probability that on demand, the output flow from the network will be equal to or greater than a specified threshold value.

Determining the threshold flow rate reliability for repairable flow networks with redundancy is particularly important for telecommunication networks. For these, a small part of the network (often only a single path from the source to the destination) is used for a data transfer. Failures of hosts, routers and communication lines are frequent, and are inevitably associated with downtimes for repair.

An important part of the proposed algorithm is the algorithm for restoring the maximum flow after component failures.

By using the simulator, we show that the topology of repairable flow networks has a significant impact on the threshold flow rate reliability. Two networks built with identical type and number of components can have very different levels of the threshold flow rate reliability. The paper also shows that the threshold flow rate reliability depends strongly not only on the network topology but also on the size of the network. With increasing the network size, the influence of the network topology increases significantly.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A Monte Carlo simulation based dependability analysis of a non-Markovian grid computing environment with software rejuvenation

V.P. Koutras
Department of Financial and Management Engineering, University of the Aegean, Chios, Greece

S. Malefaki
Department of Engineering Sciences, University of Patras, Rio Patras, Greece

A.N. Platis
Department of Financial and Management Engineering, University of the Aegean, Chios, Greece

ABSTRACT

Grid computing is an innovative technology for complex systems with large scale resource sharing, wide area communication and multi institutional collaboration. Its main advantage is that it enables sharing, selection and aggregation of a wide variety of resources, including supercomputers, data resources, storage systems that are geographically distributed. In this paper, a grid system with star topology is considered, consisting of a Resource Management System (RMS) and n distributed Root Nodes (RNs). The lifetime distribution of the RMS is assumed to be exponential while its repair time follows a general distribution. Moreover, it is assumed that all the RNs have a common lifetime and repair time distributions. The lifetime distribution of each RN is exponential and the repair time distribution is a general distribution. Each of the RNs can be either in the functioning state or in the failure state. Additionally, the RMS is assumed to experience software aging phenomena due to resource exhaustion. To counteract such phenomena, a preventive technique called software rejuvenation is adopted. Due to the structure of the system, it is not important to be aware of which of the components are functioning but only of the number of the working components. Hence, the state space of the model presented, depends on the state of the RMS's software and on the number of available nodes. The system can be considered as operational when the RMS is available and simultaneously at list one of the n nodes is operational.

Although the evolution in time of each component of the system is described by a continuous time semi–Markov process, this is not the case for the whole system. Thus, in order to study the main dependability measures of the aforementioned system, the well known formulas for the main reliability measures cannot be applied. A common approach for studying these systems is to use Monte Carlo (MC) simulation. Consequently, the system's behavior in time is modeled and simulated by using MC methods. The model is simulated for a large number of times (each time represents one history of the modeled system). The resulting output is used to estimate the principal dependability measures and a key performability measure which consists of the probability of a successful run of a given task.

The simulations show that the dependability and performance measures depend firstly on the operational condition of the RMS and hence on the rejuvenation policy adopted. Consequently, the availability and the performance of the grid increase as often the rejuvenation is performed; on the other hand reliability increases when the rejuvenation interval increases. The number of the distributed nodes affects the dependability and performance measures too. It is obtained that increasing the number of RNs, increases grid's availability, reliability and performance.

REFERENCES

Levitin, G. & Dai, Y.S. 2007. Service reliability and performance in grid system with star topology, Reliability Engineering & System Safety, 92(1): 40–46.

Limnios, N. & Oprisan, G. 2001. Semi-Markov processes and Reliability. Boston: Birkhauser.

Malefaki, S. & Platis, A. 2010, Grid computing dependability analysis based on Monte Carlo simulation. In Ale, B.J.M., Papazoglou, I.A. and Zio, E. (editors), Reliability, Risk and Safety --Back to the Future, CRC Press, pp. 1026–1032. Proceedings of the European Safety and Reliability Annual Conference 2010 (ESREL 2010), 5–9 September 2010, Rhodes, Greece.

Trivedi, K.S., Giardo, G., Malhorta, M. & Sahner, R.A. 1993. Dependability and Performability analysis, Performance Evaluation of Computer and Communication Systems. L. Dontatiella, R. Nelson (eds), Lecture Notes in Computer Science: 587–612, Springer-Verlag.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An adapted application of FMEA in the identification of critical dynamic failure modes of digital reactor protection systems

G. Wang
Technology and Engineering Center for Space Utilization Chinese Academy of Sciences, Beijing, China

S. Li
M.A.R.S. Technology & Engineering Solutions Ltd. Beijing, China

ABSTRACT

In digital Instrument & Control (I&C) systems, the existence of interactions between software and hardware components could incur functional failures in the system level. A digital Reactor Protection System (RPS) comprises complex voting algorithms, switching (fail-safe) mechanisms and communicating networks that could interact to cause the system to fail in dynamic ways. The timing of component failures and subsequent control policies has much impact on the system performance. Although risk-informed decision-making has not been implemented in the review of digital I&C systems yet due to that there presently exists no universally accepted methods for modeling digital system reliability, it is significant that an effective approach must be employed to adequately identify digital system failure modes for decision-makings on design alternatives during the development of such a digital RPS. A comprehensive understanding of these functional failure modes is extremely important in the initial design phase. However, the widely applied traditional Failure Mode and Effect Analysis (FMEA) shows its inadequacy in addressing the interactions. This paper is based on the works in the early development stage of a digital RPS. It is concerned with the dynamic failure modes in digital I&C systems and proposes a Timeline approach as a tool to implement complementary qualitative analyses based on the FMEA results. The Timeline approach shows its capacity to obtain understanding of how the digital I&C systems react and compensate a component failure in a very short time. While it is concluded that the proposed method can be used to obtain qualitative information on the failure characteristics of digital I&C systems, it can also be helpful in the identification of risk important event sequences. Thus, recommendations to reduce the probability of occurrence of safety-critical failure modes can be proposed based on qualitative comparisons between design alternatives. The discussion leads to a study of reliability modeling methodology of digital I&C systems.

REFERENCES

Aldemir, T. et al. 2006. *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901*, USA Nuclear Regulatory Commission, Washington, D.C.

Aldemir, T. et al. 2009. *A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems, NUREG/CR-6985*, USA Nuclear Regulatory Commission, Washington, D.C.

ANSI/IEEE Std 352, 1987. *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, The Institute of Electrical and Electronics Engineers, Inc.

Chrysler L.L.C, Ford Motor Company, General Motors Corporation, 2008. *Potential Failure Mode and Effects Analysis (FMEA) (Reference Manual Forth Edition)*.

Chu, T.L. et al. 2008. *Traditional Probabilistic Risk Assessment Methods for Digital Systems, NUREG/CR-6962*, USA Nuclear Regulatory Commission, Washington, D.C.

IEC 60812, 2006. *Analysis techniques for system reliability –Procedure for failure mode and effects analysis (FMEA)*, International Electrotechnical Commission.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An analysis of applying RCM methodology in a Brazilian thermal power plant

P.H.C. Lins, T.V. Garcez, M.H. Alencar & A.T. de Almeida
Federal University of Pernambuco, UFPE, Recife, Brazil

ABSTRACT

Recently, competition among companies, the globalization of business, the growth of mechanization and automation in addition to the constant technological changes and the implications of these for industries on issues related to the environment have been major factors which have brought about changes in the structure of companies. In this scenario, maintenance actions, which are part of the production process, can influence a company's approach to competition, as well as its business strategy. The availability of an asset is highly correlated with how it is managed. Any strategy must include a plan for maintenance activities because failures generate unplanned actions. One of the biggest challenges for companies with regard to maintenance is to decide what techniques should be used in their organizations in order to improve the performance of assets and to reduce maintenance costs. Therefore, the implementation of approaches related to maintenance has been studied in order to guide companies on how to manage this process better. Among the approaches most used in the maintenance industry, RCM (Reliability-centered Maintenance), an approach that started in the commercial aviation industry, stands out. According to Deshpande & Modak (2002), RCM offers the most systematic and efficient process for addressing an overall programmatic approach to optimizing the maintenance of plant and equipment.

In this context, this paper presents an analysis of applying RCM methodology in a natural gas thermoelectric power plant, located in Brazil. This power plant studied has three turbines in a combined cycle system, two of them being driven by natural gas and the third one, by steam. Power plant systems whether directly or indirectly involved in the process of power generation are quite complex and interconnected. Therefore, should these systems fail, this can easily lead to the plant shutting down. In this scenario, the role of maintenance becomes even more important and acute. Implementing RCM contributes positively to improving the operation of the plant as well as to maintenance planning. Thus, in this paper, introductory aspects of RCM methodology, the segment in which the company operates, and how the system under study fits into this scenario are described by way of contextualizing the process. Then, an examination of the steps for implementing the approach proposed is presented, particular emphasis being placed on the stages of selecting functions, analyzing failure modes and choosing relevant and effective maintenance activities. Finally, a summary of the most important points in the process is made by analyzing the results, the difficulties found, and the items that need to be improved.

REFERENCE

Deshpande, V. & Modak, J. 2002. Application of RCM for safety considerations in a steel plant. *Reliability Engineering and System Safety* 78: 325–334.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

An approach for coupling single component failure event with different common cause groups

Duško Kančev
Jožef Stefan Institute, Ljubljana, Slovenia

Marko Čepin
University of Ljubljana, Ljubljana, Slovenia

ABSTRACT

This paper introduces a new approach for consideration of single component failure in different Common Cause Component Groups (CCCGs) within Probabilistic Safety Assessment (PSA) modelling. Common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or nearly so, and are a direct result of a shared cause. (Mosleh et al., 1988). Several different parametric models exist for qualitative representation and quantification of dependency between equipment failures within Common Cause Failure (CCF) analysis. Some of them are the alpha factor, beta factor, binominal failure rate, multiple Greek letter. Although each of the models is characterized with certain specifics, all of them share the same general idea. This common idea is the fact that component failure probability, i.e., each components failure space, can be divided to independent and dependent, common cause affected portion. The relation between both portions is determined with different parameters defined within the specific parametric model selected (Cepin 2010). The motivation for the study presented herein is the incapability of one of the most widespread PSA softwares (Relcon AB 1998) for simultaneous assignment of one single component failure event in more than one CCCG within the fault tree analysis technique.

The occurrence of such a scenario where a single component fails due to different causes, i.e., assigning one single component failure event to different CCCGs in the fault tree model, is in practice, absolutely probable. On the other side, there is a risk of components failure space breach when one tries to model CCF explicitly. In case when specified component is being simultaneously assigned to different common cause components groups, there is a risk that the dependent portion will increase, suppress and become dominant over the independent portion. In some scenarios, this can progress into logical inconsistencies, i.e. the common cause affected portion becoming bigger than the total components failure space comprising it (Fig. 1).

Thus, a new approach for coupling a basic event of a single component failure with different CCCGs simultaneously, within the fault tree analysis technique, is presented in this study. Additionally, the method suggests a subsequent proportional reduction of all beta factors separately in a way that the cumulative CCF portion becomes less than or, at most, equal to the total component failure space. One version of the method, associated to beta parametric model, is applied on a fictitious case study system and discussed within this paper. This specific version suggests equalization of the cumulative CCF portion to the total component failure space. The results of the application of this approach indicate qualitative shifting of specific Minimal Cut Sets (MCSs) with regard to their contributions in the top event probability.

This method has a perspective in future, especially in the direction of studying existing nuclear power plants safety systems in terms of investigating the mentioned qualitative shifting of the MCSs.

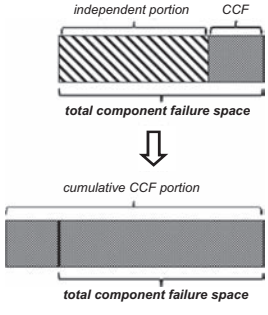


Figure 1. Component failure space partition.

REFERENCES

Cepin, M. 2010. Application of common cause analysis for assessment of reliability of power systems. Proceedings of 2010 IEEE PMAPS Conf., Singapore, 14–17 June 2010.

Mosleh, A. et al. 1988. Procedures for treating common cause failures in safety and reliability studies. NUREG/CR-4780, Vol. 1. US NRC, Washington, DC.

Relcon, A.B. Risk Spectrum PSA Proffesional. Sweden, 1998.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Automated generation of a reliability model for a system undertaking phased missions

S.J. Dunnett & K.S. Stockwell
Loughborough University, Loughborough, Leicestershire, UK

ABSTRACT

There are various mathematical models available to assess the reliability of a given system, these models relate the performance of the system to the performance of the components of which it is comprised and can be used to determine the failure probability or failure frequency of the system in question. The models can be applied at the design stage to investigate alternative design options and influence the development of the system. They can also be used to prove that the system will perform to the required standard once its design has been finalised. However the most beneficial way to use the models is at the design phase when there is the most flexibility in changing the design in response to the predicted performance. Currently there is software available to perform the mathematical analysis of the model but the construction of the model, used as input to the software, is undertaken manually. This is quite a lengthy process and can limit the usefulness of the model, as during the time the models are being developed for a specific system design, and analysed, the system design independently progresses and evolves. Therefore the model and its influence lag behind the actual realised design. Another limiting factor is that design teams do often not have the expertise required to construct the models and it is therefore passed to a specialist group to perform the task. Hence resulting in a loss of overall control and project cohesion. One way of improving this situation would be to automate the construction process. This would enable the performance of alternate system designs to be obtained quickly, allowing for the optimal system design to be selected before progressing.

In this work a procedure is developed to automatically generate a reliability model for a system undertaking a phased mission. Such a mission is made up of consecutive time periods, known as phases, within which the system may have to meet different requirements for successful completion of the phase. System failure during any phase will result in mission failure. Due to the complexity of modelling phased missions simulation techniques have been adopted with the model developed based upon Petri Nets. These provide a graphical modeling tool for dynamic system representation and are very flexible in the system features that they are capable of modelling. The procedure outlined in this work takes as input a description of the system, including the system structure, its usage, phase information and component failure and repair data. From this information decision tables are developed for the components that consider all possible combinations of inputs and component states and their influence on the component output. For systems undertaking phased missions some of the components outputs are also dependent on the phase, this information is also included in the decision tables. For components with different modes of operation, operating mode tables, describing the effect on the operating mode of different inputs and component states are also developed. Using these tables and the system topology distinct Petri nets are generated that model the component failure and repair, the interactions between components within the system and the phase progression and mission success or failure. These nets can then be used to simulate the system reliability.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Contribution to mission profile effect onto sequential system reliability

M. Koucky
Technical university, Liberec, Czech republic

D. Valis
University of Defence, Brno, Czech republic

ABSTRACT

Complex mechatronic systems sometimes do work in difficult and adverse environment. Such environment may affect the system's performance and also dependability characteristics. Since we use complex systems with one shot items we need to know basic characteristics of such a system. The paper deals with advanced mathematical methods used for field data assessment in order to prove presumed impact of mission profile and system real operation profile onto system reliability. Thank to the collected data set it is assumed that operation of the system is actually a kind of time series. The paper presents identification of the time series model, its parameters' estimation and prediction of system characteristics—like reliability/survivability function of the system for instance. Since the model of the time series has not been known, correlations with other system can be further determined and mission duration estimated. This estimation helps to organize support and operation of the system.

This contribution is supposed to contribute to procedures of reliability calculations of the complex (in this case a weapon) system as an object under investigation. We would like to present ways how to determine some characteristics of reliability performance of the set which may be influenced by a mission profile. The goal of this paper is also to verify the suggested solution in relation to some functional elements which might be influenced by the mission profile. Since the system fulfils a required function in a very specific manner we focus on the mission profile impact (Koucky & Valis 2007, Valis & Koucky 2008).

The object under investigation "PL-20 aircraft gun" was designed for the needs of the Czech Air Force and it was fielded into its armament as an onboard weapon for the L-159 advanced light combat aircraft. It refers to a 20-mm calibre twin gun, the automatic function of which is actuated by powder gases from its barrels. A failure of a round of these automatic weapons might result in discontinuation of firing and a non-fired round remains loaded in a chamber of the gun. A mission of that system has a specific profile which is to be respected. Some aspects of the mission are cadency (shooting velocity), number of attacks, number of bursts in one task, etc.

It is dealt with a weapon set which is a complex mechatronics system, designed and constructed for military purposes. We are talking about a barrel shooting gun—a fast shooting two-barrel cannon which has to complete required tasks/missions in required profile. Indeed the weapon works in very adverse, specific and diverse conditions (not only from point of view of the internal operation processes but also from the external environment impacts).

In this paper we are dealing especially with quality in terms of reliability performance. Reliability performance measures are of our interest.

Our task here is to determine the link between specific operating/mission profile and system reliability (Koucky & Valis & Vintr 2010). Based onto the real situation which is affected by thy single system reliability the task becomes more complex than this specification.

REFERENCES

Koucky, M. & Valis, D. 2007. *Reliability of Sequential System with Restricted Number of Renewals.* In: Risk, Reliability and Social Safety. London: Taylor & Francis, pp. 1845–1849.

Koucký, M., Vališ, D. & Vintr, Z. 2010. *Mission profile and its effect onto system reliability*. In Proceedings of the European Safety and Reliability Conference, ESREL 2010 – Reliability, Risk and Safety: Back to the Future. London: Taylor & Francis Group, pp. 1100–1106. ISBN 978-0-415-60427-7.

Valis, D. & Koucky. M. 2008. *Contribution to availability assessment of systems with one shot items.* In. Proceedings of the European Safety and Reliability Conference, ESREL 2008 – Reliability, Risk and Safety: Theory and Applications. London: Taylor & Francis Group, vol. 3, pp. 1807–1812.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Dependability analysis activities merged with system engineering, a real case study feedback

R. Cressent, V. Idasiak & F. Kratz
PRISME / ENSI de Bourges, Bourges, France

P. David
Grenoble-INP / CNRS G-SCOP UMR5272, Grenoble, France

ABSTRACT

The design of modern innovative systems requires the use of processes able to supervise the project, from the needs expression to the system exploitation. Those processes form the System Engineering (SE) deployment. SE activities manage the engineer's tasks to ensure the perenniality of requirements, the following of made choices and the capitalization of the generated technical knowledge. The dependability aspects have to be integrated more directly into SE processes, and currently efforts still have to be made in that direction. To support the interaction between SE and dependability study, our research team developed the MéDISIS methodology (David et al., 2010) (Cressent et al., 2011).

During former projects with various industrial partners, we described processes that were added to MéDISIS in order to integrate several dependability study activities to our partner's SE process. In this paper, we model the activities and the knowledge involved in their SE process and join the requested dependability studies. Thanks to this model, we point out the needs that MéDISIS has to cover in terms of knowledge collection and organization. We underline the central role of the DBD (Dysfunctional Behavior Database), illustrating how SysML permits to collect and organize the knowledge created by the analysis of professional processes using Parametric Diagrams and Internal Block Diagrams. To describe how MéDISIS actions easily fit in a larger Model Based System Engineering (MBSE) strategy, this paper qualifies all the benefits we observed during a real industrial project.

To illustrate this deployment of MéDISIS in a relevant context, the results, obtained recently, will be presented following a six steps merged process. First, the design activities of SE are realized using SysML as a supporting language: requirements formalization (Requirements Diagram), technical and functional specifications (Use case diagram, sequence diagram), constraints qualification (Parametric Diagram) and finally description of the system architecture (BDD and IBD). Then, from the results of these activities we perform the system analysis. The third step brings for the first time dependability studies in the process through partial-FMEA generation, using data extracted from the SysML model and previously gathered technical information stored in the DBD. After that step, a new analysis of the system permits to update our model by taking into account the result of the FMEA. The fifth step consists in easing dependability study using once again the data from the SysML model and all the feedback information contained in our DBD. The last step is to simulate the system and perform fault injection. It is once again supported by generating Simulink model from SysML and it allows testing the effects of the most significant failures listed during FMEA.

More generally, the article illustrates the deployment of safety and dependability analysis within a MBSE context. The level of analysis provided is twofold. A first part of the study examines the process level integration between the traditional SE activities and the safety and reliability assessment operations. The second level of this study exemplifies the application of the preceding principles on the product development through the feedback and experience learnt on a ramjet powered vehicle embedded system.

REFERENCES

Cressent, R., Idasiak, V. & Kratz, F. 2011. Mastering safety and reliability in a Model Based process. *Proceedings of the 57th Annual Reliability and Maintainability Symposium, RAMS2011*, Orlando, Florida, USA, 24–27 January 2011.

David, P., Idasiak, V. & Kratz, F. 2010. Reliability study of complex physical systems using SysML. *Journal of Reliability Engineering and System Safety*, Volume 95, Issue 4, April 2010, Pages 431–450.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Fast mission reliability prediction for unmanned aerial vehicles

J.D. Andrews
University of Nottingham, UK

J. Poole & W.H. Chen
Loughborough University, UK

ABSTRACT

There is currently a significant interest in the use of autonomous vehicles. One such example is the ever increasing use of Unmanned Aerial Vehicles (UAVs), particularly in military operations. UAVs also have potential civil applications which would require demonstration that they are able to respond safety to any potential circumstances, such as the occurrence of component failures, the emergence of threats such as other aircraft in the neighboring airspace, and changing weather conditions. The likelihood that an aircraft will successfully complete any mission can be predicted using phased mission analysis techniques. The predicted mission unreliability can be updated in response to changing circumstances. In the event that the likelihood of mission failure becomes too high then changes have to be made to the mission plan. If these calculations could be carried out fast enough then the quantification procedure could be used to establish an acceptable response to any new conditions. With a view to using the methodology in this context this paper investigates ways in which phased mission analysis calculation time can be reduced. The methodology improves the processing capability for a UAV phased mission analysis by taking into account the specific characteristics of the fault tree structures which provide the causes of phase failure. It also carries out as much of the quantification as possible in advance of the mission plan being formulated.

The calculations carried out prior to the mission definition are referred to as the off-line calculations. The final unreliability prediction requires information about the specific mission configuration and has to be carried out following the mission specification and is referred to as the on-line analysis time.

For a UAV, power supplies and utilities (pneumatic or hydraulic supplies) for systems frequently effect all phases of a mission. On an aircraft certain key aspects of functionality, such as thrust, are also required throughout the flight. The causes of failure of these common subsystems are also of concern in all phases of the mission. As such, sections of the fault trees reoccur frequently throughout the causes of mission phase failure. This enables the phased mission fault tree to be modularised.

To test the effectiveness of the modularisation method is has been run on two different sets of test cases and compared with a non-modularisation approach. The first set of test cases contained phase fault trees where basic events were randomly positioned. The second test set consisted of phase fault trees for UAV missions. Missions featured up to 25 phases.

As expected when events are placed randomly in the fault trees there is no significant difference in analysis times between the two methods.

For UAV mission, the fault trees had a higher degree of modularity. As the missions became more complex and were made up of a greater number of phases the benefits of the modularisation technique became apparent.

REFERENCES

Brazenaite, K., Andrews, J.D. & Chen, W.-H. 2010. Mission Reconfiguration Based on Real-time System Reliability Assessment, *Procedings of ESREL 2010: Reliability, Risk and Safety (Eds Ale B.J.M., Papazoglou, I.A., and Zio, E.), Rhodes, Greece, 5–9 September 2010, Taylor & Francis*, [CD-ROM ISBN: 978-0-415-60427-7].

Prescott, D.R., Remenyte-Prescottt, R., Reed, S., Andrew, J.D. & Downes, C.G. 2009. A reliability analysis method using binary decision diagrams in phased mission planning. *Proc. instn mech. engrs part O: j. risk and reliability* 223: 133–143.

Remenyte-Prescott, R., Andrews, J.D. & Chung, P.W.H. An Efficient Phased Mission Reliability Analysis for Autonomous Vehicles, Reliability Engineering & System Safety, Volume 95, Issue 3, March 2010, Pages 226–235.

Zang, X., Sun, H. & Trivedi, K.S. 1999. A BDD-based algorithm for reliability analysis of phased mission systems. *IEEE trans. Reliability* 48: 50–60.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

How IEC 61508 can be used to design safe offshore wind turbines

L. Dai & I.B. Utne
Department of Marine Technology, Norwegian University of Science and Technology, Trondheim, Norway

M. Rausand
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

Offshore wind energy is today an emerging industry with relatively small margins for profit. A number of studies are currently carried out on the reliability analysis of different subassemblies or components in Offshore Wind Turbines (OWTs). However, the protection systems are generally overlooked.

IEC 61508 is a generic standard which is applied on safety related systems in a range of different sectors. Its application starts with risk analysis of the system, and identification of the criteria related to the risk reduction and the tolerability of risk. Most of the time, the operation of offshore wind farms is unmanned. Thus, damage to the OWTs is the primary concern for safety, and financial losses are the main consequences. Several cost elements may contribute to financial losses, including the direct turbine damage cost, the follow-on cost on production interruption and repair/dismantlement, and the potential cost related to security of power supply, possibility of losing subsidies, and personnel injury/fatality.

Several common hazardous events in OWTs are introduced in this paper, which are rotor over-speed, generator overload or fault, excessive vibration, and abnormal cable twist. The performance of OWTs is significantly influenced by the system configuration and environmental conditions. Therefore, practical experience is of great importance to analyze the initiating causes of the hazardous events and the initiation likelihood. In practical application, more hazardous events might be identified with the techniques suggested in IEC 61508. These hazardous events should be investigated to improve learning and reduce the probability of future events. Learning from experience should also be used to define safety requirements, which are further allocated to the various protection layers.

An OWT is equipped with control and protection systems. They define an envelope of possible operational and environmental situations the OWT will experience. The OWT operating parameters are maintained within their normal limits by the control system. When a critical operating parameter exceeds its normal limits, the protection system is triggered to restore the turbine to a safe condition. Besides the control system and the protection system, improved design features and additional mitigation are commonly used protection layers.

According to IEC 61508, each protection function must comply with a specific safety integrity level (SIL). A number of techniques are listed in IEC 61508 for the determination of SIL requirements. In the current paper, a simplified application of the Layer Of Protection Analysis (LOPA) method in OWTs is demonstrated.

IEC 61508 provides a safety life cycle as a framework for specification, design, implementation, construction, operation, maintenance, and modifications of safety related systems. Based on this principle, this paper also suggests measures for implementation and verification of SIL requirements following the design phase. The current paper is the starting point for further work on gathering and structuring relevant data, and for getting more insight into relevant causes and consequences of potential hazardous events that can be used as basis for a detailed case study on the protection system.

REFERENCES

[1] Burton, T., Sharpe, D., Jenkins, N. & Bossanyi, E., 2001. Wind Energy Handbook. Wiley, Chichester.
[2] IEC 61508, 2010. Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, Geneva.
[3] Lundteigen, M.A. 2009. Safety Instrumented Systems in the Oil and Gas Industry: Concept and Methods for Safety and Reliability Assessment in Design and Operation. Ph.D. thesis, Norwegian University of Science and Technology.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Impact of different minimal path set selection methods on efficiency of fault tree decomposition

V. Matuzas & S. Contini
European Commission, Joint Research Centre, Ispra Establishment, Italy

ABSTRACT

The Level-1 PSA analysis of a nuclear power plant is based on ET and FT techniques. The analysis of ET accident sequences implies the analysis of very complex fault trees. The main factor that prevents the exact analysis of such large fault trees is insufficient computational resources (mainly insufficient working memory to store the BDD or the MCS depending on the approach). Current FT analysis methods use several efficient algorithms to reduce the complexity of the FT model in order to be able to determine at least an approximated result. The problem however is that the approximation may be an under estimation of the accident frequency and there is no method able to determine the truncation error on complex trees. Hence, new methods are needed to improve the quantification procedures.

In recent papers (Contini & Matuzas 2011a, Contini & Matuzas 2011b) a new method to analyse complex fault trees was proposed by the authors. The fault tree is decomposed into a set of mutually exclusive simpler fault trees up to their dimensions are compatible with the available computational resources. Then, the results of the exact analysis (using the BDD approach) of all simpler trees are composed to obtain the exact results for the original un-decomposed complex fault tree.

The decomposition is based on the events making up a Minimal Path Set (MPS). An MPS is a set of components such that if they are all working the Top event is not verified. Therefore Minimal Cut Set (MCS) contains at least one event of the MPS. This means that it is possible to partition all MCSs into a given number of sets. In the method described the complex fault tree is decomposed into a set of simpler trees equal to the order of the MPS. In general, complex tree can be decomposed in as many ways as the number of its MPSs.

The efficiency of the decomposition method is sensitive to the composition of the MPS. Hence, the problem is the determination of the MPS that minimises the analysis time.

Due to the heuristic nature of this problem it is necessary to experimentally test a number of algorithms in order to draw indications on the relatively "best" method(s).

The paper describes different MPS selection strategies and provides test results of their application for the analysis of complex fault trees.

REFERENCES

Contini, S. & Matuzas, V. 2011a. Analysis of large fault trees based on functional decomposition. *Reliability Engineering and System Safety* 96: 383–390.

Contini, S. & Matuzas, V. 2011b. Coupling decomposition and truncation for the analysis of complex fault trees, Accepted for publication in *Journal of Risk and Reliability*, (2011).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Issues of reliability in mobile working machines—inquiry study

Antti-Ville Itäsalo & Asko Ellman
TUT, Tampere University of Technology, Tampere, Finland

Tero Välisalo
VTT Technical Research Centre of Finland, Tampere, Finland

ABSTRACT

This paper deals with issues of reliability of the mobile work machines. Mobile work machines need to operate very reliably so that the working operation and the delivery of the products won't be disturbed. For this reason the work machine buyers have begun to require more exact reliability and maintenance information and possibly out-of-service times about the work machines. They also want to know the overall lifetime cost of the machine.

Another interesting thing is the transformation of manufacturers to maintenance services providers. The profitability of the maintenance services depends on the ability to arrange the maintenance operations in order to avoid additional maintenance operations due to unexpected failures or minimize the time consumed for them. In other words the malfunctioning of devices should be able to be controlled. The management of the reliability issues of the work machines is difficult due to the special characteristics of their use which are varying loads, demanding operating conditions and small manufactured series.

The study is based on the inquiry for which 11 Finnish companies have corresponded. The variety of the work machines concerned is wide: from forest machines to lifts. The operating environments of the machines are also quite different. For the inquiry a wide representation of persons that are involved in the different stages of the design and manufacturing process was needed. The interviewed workers included engineers, product managers, maintenance managers or the experts of the reliability.

The focus at the inquiry is to determine the main problem areas from the reliability point of view such as frame, actuators and the control system. Also, a more detailed investigation on the component level factors of these reliability areas such as a diesel engine and axels has been performed. Causes of the failures are divided in categories like using against instructions, difficult operating conditions and poor manufacturing or design quality.

The results show the reliability bottlenecks during and after the warranty period in the mobile work machines. The results indicate that more than 40% of the failures of work machines are found in the control systems. The most common causes of failure in control systems are caused by sensors and computer software. The faults in the software cause about 10% of all the faults of the machine during the warranty. After the warranty the situation, however, improves as the software is updated during the machine lifecycle.

The components of the work machines are usually produced by some big international companies and they are used around the world. Therefore the same problems are probably general around the world. As the significance of co-operation among work machine manufacturers concerning e.g., reliability testing is realized, more information will be obtained from different environments and different parts.

REFERENCES

Jerry Lawles, (2000). "Statistics in Reliability", Journal of the American Statistical association, Vol. 95, No. 451, Vignettes.

Standard IEC 60300-1. Dependability management. 2003.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Management of factors that influence common cause failures of safety instrumented system in the operational phase

M. Rahimi, M. Rausand & M.A. Lundteigen
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

Common Cause Failures (CCFs) are serious threats to the reliability of Safety Instrumented Systems (SIS). System vulnerabilities to CCFs may be introduced in all phases of the system life cycle, and especially in design, installation. Many of these vulnerabilities are the results of inadequate decisions and acts by the SIS designers, the installation crew, the operation and maintenance personnel, and the plant management. In the design phase, a significant effort is often devoted to avoid CCFs, for example, by implementing diversity.

This paper is focused on the operational phase. At the start of this phase, the hardware architecture and the components are settled and will usually remain unchanged in the whole operational phase, unless there is a call for modification. During the operational phase, the SIS reliability will mainly be influenced by the (i) environmental conditions, (ii) the operational and maintenance/testing procedures, and (iii) the actual human interactions with the systems. These influences may have impact on both random hardware failures and systematic failures. For CCFs, the influences on systematic failures are the most important.

This paper focuses on the third type, i.e., the CCF vulnerabilities influenced by the actual human interactions and the possible human errors committed during these interactions. The human errors will again be influenced by organizational factors. The link between human and organizational factors and CCFs in SISs is undeniable and has been documented in a range of investigations.

A high number of CCF models have been proposed to incorporate the effects of CCFs into quantitative risk and reliability assessments. Most industries, however, suffice with the simple beta-factor model, which was introduced by Fleming (1975).

The beta-factor model is preferred mainly due it's simplicity. This model has only one extra parameter, the beta-factor, β, which is the fraction of CCFs among all failures of a component. The parameter β may also be interpreted as the conditional probability that a component failure is a CCF, given that the component has failed.

In lack of supporting data, the beta-factor is often estimated by checklists, such as those given in Humphreys (1987), IEC 61508 (2010), and Brand (1996). These checklists, however, mainly focus on technical issues, rather than human-related issues. In the checklist questions in IEC 61508 (2010), only 20% of the questions concern human and organizational factors. Such a low focus on human and organizational factors is not in line with the lessons learnt from the ICDE project.

The objectives of the paper are to:

- Identify and discuss the main human and organizational factors that are contributing to changes of the CCF vulnerability in the operational phase.
- Establish a Bayesian network illustrating how the likelihood of CCFs is influenced by human and organizational factors.
- Discuss how the influence of human and organizational factors can be incorporated into the beta factor models.
- Discuss on how to use the insights from human and organizational factors to come up with a more realistic estimate of the parameter beta in the operational phase.

REFERENCES

Brand, P. 1996. A pragmatic approach to dependent failures assessment for standard systems. AEA Technology plc.

Fleming, K.N. 1975. A reliability model for common mode failures in redundant safety systems. Report GAA13284, General Atomic Company, San Diego, CA.

Humphreys, R.A. 1987. Assigning a numerical value to the beta factor for common cause evaluation. In Proceedings of the Sixth Conference, Birmingham, UK, pp. 2C/5/1–C/5/8.

IEC 61508, 2010. Functional Safety of Electrical/ Electronic/Programmable Electronic Safety- Related Systems. Genva: International Electro technical Commission.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Modelling of dynamical dependability by using stochastic processes

J. Chudoba
Technical University of Liberec, Liberec, Czech Republic

ABSTRACT

This paper on the topic of "Modelling of dynamical dependability by using stochastic processes" has the main aim of expanding the Markov analysis (in dependability) by adding an instrument, which allows learning and describing time and performance dynamics of complicated systems, especially network structure. The base hypothesis of the Markov analysis is that failure and repair rates between two postures are constant.

The instrument for time dynamics can solve tasks whose failure and repair rates are not constant and also solve repairs in predetermined maintenance. Mathematical solving of this problem is based on a construction of differential equations with non-constant parameters and their solution. The Runge-Kutta method is used for components, which are as "good as old". The Monte Carlo method is usually used for components of a system, which are as "good as new".

Performance dynamics can be described as systems with multiple counts of the same items. Resultant dependability of these items depends on the production volume and the combination of items, which are in use, or in active and passive redundancy.

An example can be mentioned as modelling of dependability of an electrical network and systems for railways and roads. Practical solving of this project was shown on the modelling of a compressor station and adjacent lines of the gas pipeline RWE Transgas. After instantaneous unavailability, a solution is possible to determine the probability that this gas pipeline system is not able to provide gas distribution to customers in required amounts. This could mean that the provider can't provide gas distribution in the required qualities or another example can be that gas pipeline becomes overloaded etc. Conventional software engines in dependability didn't solve these problems at that time. This dissertation thesis may help on a large scale by an efficient evaluation of probability of the creation on catastrophic failures by the modelling of complicated systems.

Thanks to the revaluation of modelled causes of dependability it is possible to decrease the probability of cataleptic failure. This can be achieved, for example, by more efficient maintenance, or multiple component redundancy. If the probability of cataleptic failure is effectively decreased, it would bring a reduction of cost resulting from the frequency of gas distribution failure and also the total time of failure.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Qualitative analysis of a BDMP by finite automaton

Pierre-Yves Chaux
LURPA, Cachan Cedex, France
EDF R&D, Clamart, France

Jean-Marc Roussel & Jean-Jacques Lesage
LURPA, Cachan Cedex, France

Gilles Deleuze
EDF R&D, Clamart, France

Marc Bouissou
EDF R&D, Clamart, France
École Centrale Paris, Chateney-Malabry Cedex, France

ABSTRACT

Many studies which have been carried out on predictive risk modelling and assessment target two complementary objectives (Henley and Kumamoto 1981). On the one hand, quantitative analyses aim at calculting the failure rate of the modelled system or of one of its subsystems. On the other hand the qualitative analyses aim at determining the scenarios which lead to the failure of the whole system. While those scenarios are in most cases only constituted by basic components failures, they may also include repairs of these components.

The Boolean Driven Markov Processes (BDMP) were created to include all the Electricite De Francé expertise in the construction and analysis of reliability models (Bouissou and Bon 2003). While staying close to Static Fault Tree models (Stamatelatos, Vesely, Dugan, Fragola, Minarick, and Railsback 2002), BDMPs extend the fault tree capacities by allowing to model both the failures and repairs of basic components. This extension also enables the description of the redundancies between components and between complex subsystems constituted by a number of components, which can be redundant one from another.

The main goal of this study is to conduct a qualitative analysis of a BDMP while setting aside all its capacities to model and conduct quantitative analysis on the reliability of a system. The qualitative analysis consists in enumerating all the sequences of repair and failure events that are implicitly described by a BDMP. To explicitly describe those combinations, this study is conducted within the languages and Finite Automata (FA) theories. For that, each scenario of failures and repairs is translated into a sequence of events. The set constituted by those sequences (or words) is a language.

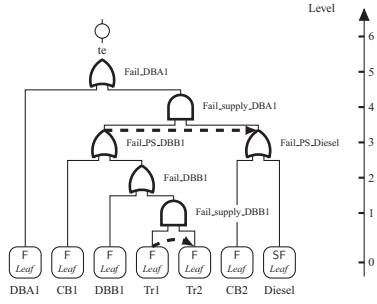


Figure 1. The BDMP of the studied system.

This paper describes an algorithm which is used to construct the FA "equivalent" to a BDMP in the away that this FA generates the same language as the one which is implicitly described in the BDMP. The qualitative studies can now be conducted on the FA rather than on the BDMP itself. This allows us to gain all the benefits of handling a formal model on which many results were published. This paper illustrates the given semantics and the usage of the algorithm on a system which supplies the components which support the cooling and the control functions of a nuclear reactor core. The BDMP which models the safety of this system is shown in Figure 1.

REFERENCES

Bouissou, M. & Bon, J. (2003). A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov Processes. *Reliability Engineering and System Safety 82*(2), 149–163.

Henley, E. & Kumamoto, H. (1981). *Reliability engineering and risk assessment*. Prentice-Hall Englewood Cliffs (NJ).

Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J. & Railsback, J. (2002). Fault tree handbook with aerospace applications.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability analysis of phased-mission systems with phase mission backup

Xiaoyue Wu & Qi Liu
College of Information Systems and Management, National University of Defense Technology, Changsha, Hunan, China

ABSTRACT

This paper proposes a Continuous Time Markov Chain (CTMC) model approach for the reliability analysis of Phased-Mission Systems (PMS) with phase mission backup. The spaceflight Tracking, Telemetry and Command (TT&C) system is an important technological supporting system providing services for spaceflight mission in consecutive phases. Sometimes, the mission success of TT&C depends not only on the success of each phase, but also depends on the redundancy of mission implementation between phases. For example, the mission failure during current phase can also be completed during the following phase. Therefore, there exists PMS that has phase mission backup for a given mission phase. To the best of our knowledge, this kind of PMS has not been investigated by researchers.

For the reliability analysis of such kind of PMS, we build a CTMC model for each mission phase as for conventional PMS. For each $i \in N$, let $\pi_i(t) = P\{X(t) = i\}$ represent the probability that the system is in state i, at time t, and $\pi(t) = (\pi_1(t), \ldots, \pi_n(t))$. Then, the state probability vector of the system after time t can be given as

$$\pi(t) = \pi(0)e^{Qt}$$

Assume there is only one critical mission phase Ph_i with phase mission backup (Figure 1). Let Ph_j be the mission backup phase for Ph_i. Both phases Ph_i and Ph_j have their own missions, denoted as M_i and M_j respectively. If M_i is failed during the mission time of Ph_i, then it is arranged to be executed again during the mission time of Ph_j If M_i is failed again in Ph_j, then it is said that mission M_i is failed for the PMS, that is, the whole mission of PMS fails since one of its mission failed.

For the mission phase which provide mission backup for other phase, if the mission of its backuped phase fails, then it will be decomposed into two subphases. The success of one subphase requires the success of its original mission and the failed mission of the previous phase. The mission success of another subphase only needs the accomplishment of its own original mission. Regarding the success or failure of the backuped mission phase as the initial states condition with different probabilities, the mission reliability of the backup phase can be found by solving the CTMC. By combination of all these results with different probabilities, the total mission reliability can be calculated.

Let the whole mission of PMS be denoted as M, then the mission reliability of the PMS R_{PMS} is the sum of the reliabilities of the two exclusive cases as follows

$$\begin{aligned} R_{PMS} &= R_{PMS1} + R_{PMS2} \\ &= \Pr\{M \text{ successful} \cap M_i \text{ successful in } Ph_i\} \\ &\quad + \Pr\{\boldsymbol{M} \text{ successful} \cap M_i \text{ fail in } Ph_i\} \end{aligned}$$

A simplified PMS with three phases is used to illustrate the application of our approach. The numerical results shows that by phase mission backup, the mission reliability of the PMS is increased by 0.0064 from 0.9559.

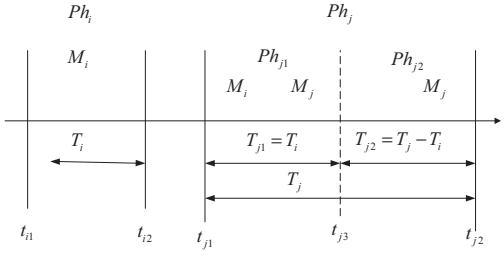


Figure 1. Mission phase and its backup phase.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability analysis of the electronic protection systems with mixed m—branches reliability structure

A. Rosiński
Warsaw University of Technology, Warsaw, Poland

ABSTRACT

In the article are presented questions connected with the electronic protection systems.

Into the group of the electronic protection systems we can include:

- Intruder alarm system,
- System Control Access,
- Closed Circuit TeleVision,
- Fire alarm systems,
- Systems of external terrains' protection.

Projecting the electronic safety protection systems it should be considered the stage of the threat (according to valid standards) stepping out in the protected object, particularly when this objects relates to the special objects (e.g., the protection of airport, railway stations). Than having the directives defines the minimum number of units from what the system has to composed, we can approach to the choice of the type of alarm central station and co-operating with it devices. The use on this stage of the presented in the article method of the analysis of reliability structures makes possible the formation of the values of the probabilities of staying in the respective states: full ability, the impendency over safety and unreliability of safety. It should be however considered the fact, that applying of the surplus results in enlargement of the financial value of the system.

The introduced method can also be used to the modernization already existing and the exploited electronic protection safety systems. If there occur the necessity of enlargement of the value of the probabilities of the staying in the states of full ability and the impendency over safety, the designer has the possibility of their determination. This is particularly essential is in the case of the growth of the stage of the threat stepping out in the protected object.

REFERENCES

Będkowski, L. & Dąbrowski, T. 2006. *The basis of exploitation, part II: The basis of exploational reliability*. Warszawa: Wojskowa Akademia Techniczna.

European standard EN 50131-1:2006. Alarm systems – Intrusion and hold-up systems – Part 1: System requirements. Brussels: European Committee for Electrotechnical Standardization CENELEC.

Jaźwiński, J. & Ważyńska-Fiok, K. 1993. *System safety*. Warszawa: PWN.

Rosiński, A. 2005. Reliability of monitoring systems. *Proc. 6-th European Conference of Young Research and Science Workers in Transport and Telecommunications (TRANSCOM 2005)*, Żilina, Slovak Republic, 27–29 June 2005.

Rosiński, A. 2008. Design of the electronic protection systems with utilization of the method of analysis of reliebility structures. *Proc. Nineteenth International Conference On Systems Engineering (ICSEng 2008)*, Las Vegas, USA, 19–21 August 2008.

Rosiński, A. 2009. Reliability analysis of the electronic protection systems with mixed – three branches reliability structure. *Proc. International Conference European Safety and Reliability (ESREL 2009)*. Prague, Czech Republic, 7–10 September 2009.

Ważyńska-Fiok, K. & Jaźwiński, J. 1990. *Reliability of technical systems*. Warszawa: PWN.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reliability analysis of vacuum sewerage systems using the total probability theorem

Katarzyna Miszta-Kruk
Warsaw University of Technology, Poland

ABSTRACT

Small towns having a flat terrain topology decide to introduce unconventional solutions to wastewater systems in relation to gravity sewers. Those solutions include inter alia vacuum sewerage systems which according to the carried out sociological studies are acceptable systems by end users. It is believed that those systems are more reliable than conventional ones; however it has not been yet in any way confirmed by reliability research or dissertations.

The research methodology and the reliability model of the vacuum sewerage system, using the theorem of the total probability, have been developed and gave rise to the quantitative evaluation of the reliability of the system individual components. As a consequence, it enables the quantitative estimation of values of reliability indices of the entire vacuum sewerage system. It also allows using the term reliability to quantify its specific values.

Reliability analysis of network systems, which include sewerage systems, consisted of describing the structure of the system with its division into III subsystems, defining elements in each subsystem, defining reliability states and determining probabilities of staying in those states using the theorem of total probability. Reliability structures of isolated subsystems represent interconnections of the system elements from the viewpoint of their failures impact on the reliability of the subsystems. It is assumed that elements forming subsystems are two-state elements. Reliability of the vacuum sewerage system was defined for two cases i.e., when the system is able to take sewage from the entire area (full suitability), and when it is only possible to discharge sewage from part of the area (partial suitability). The key input to the model are failure intensity values gathered from operational reliability research of 4 sewage systems that was carried out over a period of 2 years. System reliability expressed by probability of full suitability was estimated through determination of probabilities of individual elements suitability and of conditional probabilities.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Requirements for dependability management and ICT tools in early stages of the system design

P. Valkokari, T. Ahonen & O. Venho-Ahonen
VTT Technical Research Centre of Finland, Tampere, Finland

H. Franssila
University of Tampere, Tampere, Finland

A. Ellman
Tampere University of Technology, Tampere, Finland

ABSTRACT

The findings of our paper are results of an on-going research project which has its focus on dependability management in design process and from a pre-study which was used for defining the objectives of the research project. Our paper focuses on the practical needs of companies for methods and tools for reliability management at various stages of product development processes. The pre-study revealed that there has not been a major investment to the research dedicated to dependability management for a decade at European level. However, at the same time there has been a change in companies' strategies because of an ongoing change in the business environment. System providers are currently facing severe global competition. In order to maintain their competitiveness, system providers are transforming into life cycle service providers. Therefore, actors, that are willing to carry out this transformation, need to expand their understanding on their products' lifecycle. The transformation also sets new requirements for the dependability management processes and for tools and methods used to support that process.

We specifically focus on the machine industry sector in Finland and the needs of manufacturers in that sector, while they are transforming into providers of the life cycle services. The management of the dependability issues of this industry sector is quite challenging due to, for instance, the special characteristics of the working machine use environment. Machines need to be designed for varying loads and demanding operating conditions. At the same time manufactured series are small which limits the sources of reliability data.

In our paper, we address the needs identified in a survey conducted in our research project. Based on the survey, we recognize the perspectives of persons that are representing different organizational positions in the dependability management process. Based on the results of the survey and the complementary industrial interviews, we are able to propose next steps for defining the dependability management processes inside the machine industry sector. Especially these processes are required for the early stages of the system design.

The survey reached 35 professionals from 11 companies. The 35 experienced professionals, chosen by the contact persons of each company, represented the design function (12), product management (5), maintenance and services (9) and reliability management expertise (9). The results indicated that further information is needed regarding certain important perspectives. Therefore an interview study was initiated in order to further explore the current and future challenges related to dependability management at practical level. The interview study was carried out by interviewing 22 persons from four different organizations.

The results of the survey and the interviews should support companies when selecting appropriate reliability management tools needed during the different phases of the system design. Based on the results of our research, we find it important to be able to define the process descriptions and practical approaches for dependability management. Thereafter, we are able to focus on the following development steps identified:

- *Clarification of operational reliability data collection and its usage at various levels of organization*
- *Methods to compare the effects of operating conditions on the machine's reliability performance*
- *Enhanced maintenance program planning*
- *The ability of the component provider to deliver data on component reliability*
- *Development of practical LCC/LCP calculation models for measuring economic effects of dependability.*

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Safety and Reliability Decision Support System

K. Kolowrocki & J. Soszynska-Budny
Gdynia Maritime University, Poland

ABSTRACT

The contents of the Safety and Reliability Decision Support System—S&RDSS is presented. The S&RDSS is composed of the methods of complex technical systems operation processes modeling, the methods of unknown parameters of complex technical systems operation, reliability, availability, safety models identification, the methods of complex technical systems reliability, availability and safety evaluation and prediction, the methods of complex technical systems reliability, availability and safety improvement and the methods of complex technical systems operation, reliability, availability, safety and cost optimization. The procedure of S&RDSS usage in reliability analysis, prediction and optimization of an exemplary system is illustrated as well.

The aim of this paper is to present and to apply a guide-book recently developed by the authors and including the general reliability, availability and safety analytical models of complex non-repairable and repairable multi-state technical systems related to their operation processes (Kolowrocki & Soszynska 2010).

Presented in the paper the guide-book Safety and Reliability Decision Support System—S&RDSS (Kolowrocki & Soszynska 2010) is based on the results given in the monograph (Kolowrocki & Soszynska-Budny 2011) concerned with the methods of complex technical systems operation processes modelling, the methods of complex technical systems reliability, availability and safety evaluation and prediction, the methods of unknown parameters of complex technical systems operation, reliability, availability, safety models evaluation, the methods of complex technical systems reliability, availability and safety improvement and the methods of complex technical systems operation, reliability, availability, safety and cost optimization.

The procedure of the S&RDSS usage should start from the scheme-algorithm item S&RDSS 0, and next either to study if it is necessary or to omit its introductory item S&RDSS 1 and to continue with the items S&RDSS 2–15. The user should follow the successive steps of the scheme using the support given in the forms of practical instructions and theoretical backgrounds placed at the further parts of the guide-book (Kolowrocki & Soszynska 2010).

To make the use of the S&RDSS easy and fluent, it is suggested to study its practical applications to the reliability analysis of the exemplary complex technical system presented in this paper and its wide and detailed practical applications in maritime and coastal transport industry performed in (Kolowrocki & Soszynska-Budny 2011).

In this paper, the comprehensive approach to the analysis, identification, evaluation, prediction and optimization of the complex technical systems operation, reliability, availability and safety is presented. The presented algorithm may play the role of an easy-to-use guide necessary in reliability and safety evaluations of real complex technical systems, as well as during their operation and when they are designed. The general analytical reliability, availability and safety models together with the linear programming are very useful in the complex technical systems operation, reliability, availability and safety prediction, improvement, optimization and their operation cost analysis. Those all tools are useful in reliability, availability and safety optimization and operation cost analysis of a very wide class of real technical systems operating at the varying conditions that have an influence on changing their reliability and safety structures and their components reliability and safety characteristics.

REFERENCES

Kołowrocki, K. & Soszyńska, J. 2010. Integrated Safety and Reliability Decision Support System – IS&RDSS. Tasks 10.0–10.15 in WP10: Safety and Reliability Decision Support Systems for Various Maritime and Coastal Transport Sectors. Poland-Singapore Joint Research Project. MSHE Decision No. 63/N-Singapore/2007/0. Gdynia Maritime University.

Kołowrocki, K. & Soszyńska-Budny, J. 2011. Reliability and Safety of Complex Technical Systems and Processes: Modeling – Identification – Prediction – Optimization. Springer, (*to appear*).

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

The model of reusability of multi-component product

A. Jodejko-Pietruczuk & M. Plewa
Wrocław University of Technology, Wroclaw, Poland

ABSTRACT

Reverse logistics understood as the process of managing reverse flow of materials, in-process inventory, finished goods and related information has become one of the logicians' key areas of interest.

Literature survey that has been done around the theme of the reverse logistics area, allowed to set out this article aims and objectives. The model presented in this paper refers to the theme ofreusing of returned product components inmanufacturing of new products. Great majority of models deal with single—element system or with the assumption that reused elements are as good as new. Proposed model develops the previous ones by releasing both assumptions and gives the base to determine some of reusing policy parameters such as: threshold work time of returned element that can be used again, warranty period for the product containing elements which have some history of work, the size of new elements' stock necessary to fulfil production planes. The model is presented and tested for two-element series system, but it is very simple to be developed to the case of x-element, series system.Effects of analytical calculations of the presented model are confirmed and fulfilled by simulation results.

The usage of recovered components in a production decreases production costs but also increases the risk that additional costs occur because of larger amount of returns during warranty period. The objective of the model is to find the threshold work time T for returned elements that equalises potential cost and profits of the reusing policy:

$$[E(C_{WO}(T_W,T))-E(C_{WN}(T_W))]C_O = C_B - C_R - C_M$$

$$E\left(C_{WO}\left(T_W,T\right)\right)=\left[1-\frac{R_B\left(T_W+T\right)R_A\left(T_W\right)}{R_B\left(T\right)}\right]C_0$$

$$E(C_{WO}(T_W,T)) = [1-R_B(T_W)R_A(T_W)]C_O$$

$$n = (1 - R_A(\min(T,T_W)))R_B(\min(T,T_W))$$

$$[E(C_{WO}(T_W,T))-E(C_{WN}(T_W))]\cdot n\cdot C_O = (C_B - C_R)n - C_M$$

whereC_{WO} = the cost of warranty services if an "old" element is used in a new production; T_W = the warranty period of a product; T = the threshold age of the element B, after that the further exploitation isn't continued; C_{WN} = the cost of warranty services if a "new" element is used in production; C_B = the purchase cost of a new element B; C_R = the total cost of all activities of: decomposition, cleaning, preparing of returned B element to reusing in a production; C_O = penalty cost resulting from a product failure during warranty period (e.g., the total cost of production of a new object); $R_A(t)$ = reliability of the element A in t moment; $R_B(t)$ = reliability of the element B in t moment; n = production batch percent of reusable B elements, that return during warranty period; E(x) = expected value of variable x.

REFERENCES

Murayama, T. & Shu, L.H. 2001. Treatment of Reliability for Reuse and Remanufacture, Proceedings of the 2nd International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'01), Tokyo, Japan.

Murayama, T., Yoda, M., Eguchi, T. & Oba, F. 2005. Adaptive Production Planning by Information Sharing for Reverse supply Chain, Proceedings of the 4th International Symposium on Environmentally Conscious Design and Inverse Manufacturing (EcoDesign'05), Tokyo, Japan.

Murayama, T., Yoda, M. & Eguchi, T. 2006. Oba, F., Production Planning and Simulation for Reverse Supply Chain, Japan Society Mechanical Engineering International Journal, Series C, Vol. 49, No. 2.

Plewa, M. & Jodejko-Pietruczuk, A. 2011. The reverse logistics model of single-component product recovery. European Safety and Reliability Conference, Troyes, France – in prep.

This page intentionally left blank

Uncertainty and sensitivity analysis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A methodology to study complex biophysical systems with global sensitivity analysis

Q.-L. Wu & P.-H. Cournède
INRIA Saclay Ile-de-France, EPI DigiPlante, France
Ecole Centrale Paris, LabMAS, France

J. Bertheloot
INRA, UMR 0462 SAGAH, Beaucouzé Cedex, France

ABSTRACT

Functional-structural models of plant growth (FSPM) aim at describing the structural development of individual plants combined with their eco-physiological functioning (photosynthesis, biomass allocation, in interaction with the environment). The multi-biophysical processes described in FSPMs and their complex interactions make it difficult to identify the key processes, control variables and parameters. The objective of this study is to explore how global Sensitivity Analysis (SA) can help the design of such complex models in two aspects: first, quite classically, in the parameterization process and secondly by providing new biological insights and diagnosis.

We consider a complex functional-structural model, NEMA (Bertheloot, Cournède, & Andrieu 2009), describing Carbon (C) and nitrogen (N) acquisition by a wheat plant as well as C and N distributions between plant organs after flowering. This model has the specificity to integrate physiological processes governing N economy within plants: root N uptake is modeled following: High Affinity Transport System (HATS) and Low Affinity Transport System (LATS), and N is distributed between plant organs according to the turnover of the proteins associated to the photosynthetic apparatus. C assimilation is predicted from the N content of each photosynthetic organ. Inputs of Nitrogen fertilizers are fundamental to get high-yielding crops and a production of high quality with the required protein content. This required a proper understanding of root N uptake regulation and of N determinism on yield and production. Complex interactions exist between root N uptake, N remobilization to grains, and photosynthesis, whose regulatory mechanisms remain far from clear. In our application, analyses are conducted using Sobol's method and an efficient computation technique derived from (Saltelli, 2002), and several outputs of interest are considered. Moreover, since we consider a dynamic system, the evolution of the sensitivity indices is computed. The methodology developed is inspired by (Ruget, Brisson, Delécolle, & Faivre 2002) and first implies a module by module analysis. Basic biological modules are identified firstly. The full model involves around 80 parameters, and each module between 12 to 25 parameters. For each module and each output, the most important parameters (with the highest first-order Sobol indices) are identified. The interactions between parameters within the module also need to be identified. At this step, the least important parameters are then fixed in each module. The second step compares sensitivity produced by each module on the overall model outputs. The parameters for the SA are the ones selected as the most important from each module in the first step. The variance decomposition given by Sobol's method allows: ranking the effects of each module, but also the level of interactions between modules, regarding the output of interest. The consequences of this study are crucial in several aspects: for parameterization, stressing on which module and within each module on which parameter more care should be taken, but also on whether each module can be parameterized independently (from different experiments for example). Moreover, studying carefully the interactions between parameters and modules, dynamically, may reveal some biological phenomena of interests, non visible through simple simulations. In this regards, SA offers new tools in integrative biology.

REFERENCES

Bertheloot, J., Cournède, P.-H. & Andrieu, B. (2009). Nitrogen acquisition and utilization by crops: Review of different approaches and proposition of a mechanistic modeling. *International Symposium on Plant Growth Modeling and Applications 0*, 149–156.

Ruget, F., Brisson, N. Delécolle, R. & Faivre, R. (2002). Sensitivity analysis of a crop simulation model, stics, in order to choose the main parameters to be estimated. *Agronomie 22*, 133–158.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

A study of uncertainties in active load carrying systems due to scatter in specifications of piezoelectric actuators

S. Ondoua & H. Hanselka
System Reliability and Machine Acoustics SzM, Technische Universität Darmstadt, Darmstadt, Germany

R. Platz & J. Nuffer
Fraunhofer Institute for Structural Durability and System Reliability LBF, Darmstadt, Germany

ABSTRACT

In this paper, uncertainty in an active load-carrying system with an inserted single piezoelectric stack actuator presented in Enß et al. (2010) is investigated. The piezoelectric pre-stressed stack actuator exerts a controlled lateral force on a beam column critical to buckling to stabilize it against a short time acting lateral disturbance force.

Generally, mechanical loading, the system's ambient temperature and components specifications such as actuator maximum free stroke $\Delta l_{\max}$, actuator blocking force F_B, beam stiffness C_S and beam geometry are typical influences that affect the system performance. If these influences are subject to greater scatter, uncertainty occurs and the system's performance deviates from its predefined manner. Especially uncertainty in controlled active components like sensitive piezoelectric stack actuators may lead to the above deviations.

In this work, the focus of investigation lies on the statistical determination of the influence of scatter of the piezoelectric actuator's assumed blocking force, maximum free stroke, maximum electric driving voltage capabilities and stiffness of column on actuator's force-stroke-performance. For that, the actuator's dynamic behavior due to scatter of actuator's force F_a and stroke Δl_A capability is described with the actuator's force-stroke diagram, see Figure 1.

Stochastic and estimated uncertainty in the configuration process of the active system due to normally and uniformly distributed scatter in the actuator's blocking force and maximum free stroke capability will be determined by Worst-Case analyses and Monte Carlo simulations.

On the basis of Worst-Case analyses and Monte-Carlo simulations, the effect of uncertain actuator's specifications like blocking force F_B and maximum free stroke $\Delta l_{\max}$ on the force-stroke-performance of the piezoelectric actuator is investigated numerically.

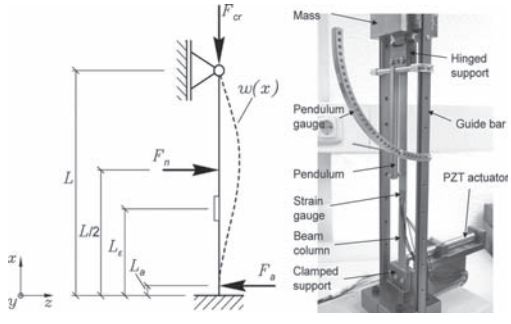


Figure 1. Force-stroke diagram of the PZT actuator used for active stabilisation, Piezomechanik (2003).

REFERENCES

Enß, G.C., Platz, R. & Hanselka, H. (2010). An approach to control the stability in an active load-carrying beam-column by one single piezoelectric stack actuator. *Proceedings of ISMA 2010, Leuven, Belgium, September 20–22*, 535–546.

Piezomechanik (2003). Piezomechanics: an introduction, booklet, september 2003. Technical report.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An environmental risk assessment of a contaminated site based on extended uncertainty analyses

M.F. Milazzo
University of Messina, Messina, Italy

T. Aven
University of Stavanger, Stavanger, Norway

ABSTRACT

In the context of contaminated sites, risk assessments have a dual purpose: to determine the level of contamination and to assess the effectiveness of remediation measures. Risk assessment is often defined as the process that estimates the likelihood of occurrence of adverse effects to humans and ecological receptors as a result of exposure to hazardous chemicals, physical and/or biological agents (US EPA 1989).

The commonly used risk assessments for such problems are based on dose-response curves producing probabilities and expected values. Typically best estimates are produced, and sometimes also (subjective) probabilities are used to describe the uncertainties. In the paper we have pointed to the need for extending these assessments to place stronger emphasis on uncertainties. The key challenge is to address uncertainties hidden in the background knowledge (assumptions) that the probabilities are based on.

A recently developed risk framework (Aven 2010) designed to better reflect such uncertainties is presented and applied to the case study, a site whose contamination is due to both past (related to the handling of chemical fertilisers) and current activities (related to the existence of a landfill of mercury sludge). Following this approach, a set of uncertainty factors are identified and assessed. The assessments of uncertainty factors for the case study have been executed in line with Flage & Aven (2009). The method includes the assessment and categorisation of the uncertainty factors with respect to both the degree of uncertainty and the degree of sensitivity.

In practice a full probability of frequency approach is difficult to carry out, as probability distributions of all parameters have to be assigned and assumptions made about independencies. The best estimate approach is quicker to carry out but lacks a proper uncertainty treatment. However, by adding the suggested assessment of uncertainty factors, the overall analysis is easier to justify. For many types of applications such an approach would be our recommended procedure. Following such a recommendation the main calculation schemes used today can be kept. What is new is the uncertainty assessment.

REFERENCES

Aven, T. 2010. *Misconceptions of risk*. Chichester: Wiley.

Flage, R. & Aven, T. 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability, Risk and Safety: Theory and Applications, Proc. intern. symp., Prague 7–10 September 2009*. Leiden: CRC Press, Taylor & Francis Group Proceeding.

US EPA 1989. *Risk assessment guidance for superfund: volume I Human health evaluation manual* (Part A, Baseline Risk Assessment). EPA/540/1–89/022. Washington, DC: United States Environmental Protection Agency.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Comparing Ordered Weighted Averaging (OWA) and Copeland score for composite indicators in the field of security of energy supply

Claudio M. Rocco S.
Universidad Central de Venezuela, Caracas, Venezuela

Stefano Tarantola
Institute of the Protection and Security of the Citizen, JRC, European Commission, Ispra, Italy

Anca Costescu Badea
Ecole Nationale Supérieure de Mines de Saint-Etienne, France

Ricardo Bolado
Institute of Energy, JRC, European Commission, ES Petten—The Netherlands

ABSTRACT

Composite indicators have been used in several fields as a practical way to synthesize different attributes or indicators of objects. The basic idea is to find a proper form of combination or aggregation rule for the individual indicators using, in some cases, additional information. In general, different performance measures based on different definitions may lead to different rankings of the countries. This situation could be controversial for a Decision-Maker (DM), whose responsibility is, for example, to achieve a better performance level.

In this paper we compare two procedures to define composite indicators for the security of energy supply in the European Member States (MS), obtained by two different aggregation rules derived from the Group Decision Theory.

In [Badea et al., 2011], the authors proposed a procedure, based on Ordered Weighted Averaging (OWA) to rank MS using PMs derived from an energy model, assessing different aspects of the security of supply. OWA is a parametric aggregation rule, which allows to test both compensatory and non-compensatory aggregations, and to embed expert preferences in the set up of importance weights. PMs are also aggregated by using a simple but efficient procedure, the Copeland Score (CS), a non-parametric ranking technique that does not require any information from the DM.

The security of energy supply is defined as the availability of reliable and affordable supplies of energy. Eight indicators are selected. The data are based on the results obtained with the PRIMES model and published in [EU 2007]. The comparison is made using a data set related to performance measures for the security of energy supply in the European Member States, for years 2010 and 2030.

The results show that the composite ranks from CS have a high correlation with the ranks produced by OWA for a risk neutral DM preference ($\alpha = 1$).

Figure 1 shows simultaneously the comparison between CS and OWA for alpha = 0, 1 and 1000 [Badea et al., 2011]. A simple sensitivity analysis

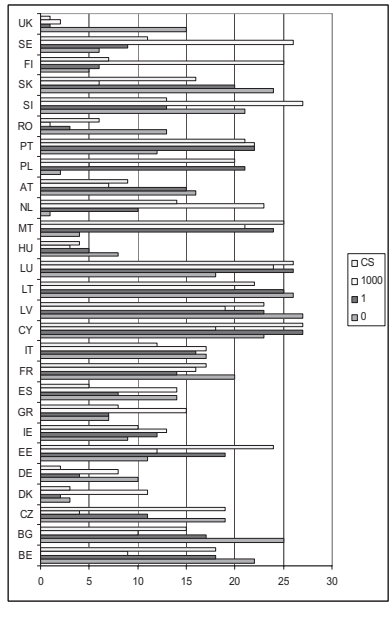


Figure 1. Comparison between countries ranking in 2010: CS vs. OWA: using the optimistic preference ($\alpha = 0$); the risk neutral preference ($\alpha = 1$) and using the pessimistic preference ($\alpha = 1000$).

shows that CS and OWA with $\alpha = 1$ have also a similar behavior when there is uncertainty in the input data. Finally CS and OWA with $\alpha = 1$ give ranking of countries that are more stable.

REFERENCES

Badea, AC., Rocco, C.M., Tarantola, S. & Bolado, R.: Composite indicators for security of energy supply using ordered weighted averaging. Reliability Engineering and System Safety (2011) doi:10.1016/j.ress.2010.12.025.

EU 2007: European Energy and Transport, Trends to 2030 – Update 2007, European Commission, DG TREN.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Generalized expressions of reliability of series-parallel and parallel-series systems using the Transferable Belief Model

Felipe Aguirre, Mohamed Sallak & Walter Schön
Laboratoire Heudiasyc, UMR CNRS 6599, Université de Technologie de Compiègne, France

ABSTRACT

Probability theory is well suited to treat uncertainties when their origin comes only from the natural variability of components' failure (aleatory uncertainty). On the other hand, if the uncertainties are due to incompleteness, imprecision or ignorance of the reliability data (epistemic uncertainty), several other theories can be used. The Transferable Belief Model (TBM) (Smets & Kennes 1994) which is an interpretation of the Dempster Shafer theory has been proven as a well suited theory for the treatment of aleatory and epistemic uncertainty in the reliability analysis (Sallak, Schön, & Aguirre 2010, Aguirre, Sallak, & Schön 2010). Nevertheless, past experiences have proven that the computational cost of the TBM based model grows exponentially with the size of the system. Actually, the computational time depends greatly on the size of the system. In the paper it is shown that a system of 8 components takes $\simeq 10$ *min*, a system of 9 components takes $\simeq 1$ *hr* and a system of 10 components takes $\simeq 5$ *hr*. A TBM Matlab Toolbox has been created to implement the TBM reliability model. The calculations were launched in a server with 32 Gb of RAM and an octo dual core Opteron 8218.

To overcome this situation, generalized expressions are introduced on the paper so as to have a more efficient way to study the reliability of series-parallel, parallel-series and combinations of series-parallel and parallel-series systems. The expressions were obtained using the method of minimal cuts and the general expressions of reliability of series and parallel systems presented in (Sallak, Schön, & Aguirre 2010). Compared to the TBM Matlab toolbox, using the presented generalized expressions, the computational limit is significantly higher. For example, a parallel-series system of 10 million components can still be studied in a fraction of a second.

However, even if the TBM reliability model has a higher computational cost, it still represents a formal framework to continue the advances in the application of the TBM theory in the reliability analysis.

Table 1. Generalized reliability belief functions through the use of minimal cuts and minimal paths.

Minimal cuts
$Bel(W_S) \quad \prod_{i=1}^{N_c}\left(\prod_{j=1}^{n(C_i)}\left(1-m\left\{W_{C_i(j)}\right\}\right)\right)$
$Pl(W_S) \quad \prod_{i=1}^{N_C}\left(1-\prod_{j=1}^{n(C_i)} m\left\{F_{C_i(j)}\right\}\right)$
Minimal paths
$Bel(W_S) \quad 1-\prod_{i=1}^{N_T}\left(1-\prod_{j=1}^{n(T_i)} m\left\{W_{T_i(j)}\right\}\right)$
$Pl(W_S) \quad 1-\prod_{i=1}^{N_T}\left(1-\prod_{j=1}^{n(T_i)}\left(1-m\left\{F_{T_i(j)}\right\}\right)\right)$

The generalized expressions are presented in table 1 and use the following notation:

N_T	Nb. of minimal paths in the system
N_C	Nb. of minimal cuts in the system
$n(T_i)$	Nb. of components in the i_{th} minimal path
$n(C_i)$	Nb. of components in the i_{th} minimal cut
T_i	Index set of the i_{th} minimal path
C_i	Index set of the i_{th} minimal cut

REFERENCES

Aguirre, F., Sallak, M. & Schön, W. (2010). Transferable belief model for incorporating failure dependencies in reliability analysis under data uncertainties. In *Workshop on the Theory of Belief Functions. Brest, France*.

Sallak, M., Schön, W. & Aguirre, F. (2010). The Transferable Belief Model for reliability analysis of systems with data uncertainties and failure dependencies. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 4*, 266–278.

Smets, P. & Kennes, R. (1994). The transferable belief model. *Artificial Intelligence 66*, 191–243.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Importance analysis in risk-informed decision-making of changes to Allowed Outage Times addressing uncertainties

S. Martorell, M. Villamizar, J.F. Villanueva & S. Carlos
Department of Chemical and Nuclear Engineering, Universidad Politécnica de Valencia, Valencia, Spain

A.I. Sánchez
Department of Statistics and Operational Research, Universidad Politécnica de Valencia, Valencia, Spain

ABSTRACT

A number of problems have been identified connected to TS that can jeopardize plant safety (Bizzak et al., 1987). The development of PRA (Probabilistic Risk Assessment) and its application since the early 80's to analyze TS changes has brought the opportunity to review TS consistency from a risk viewpoint, i.e., addressing the impact of the changes on plant safety on the basis of the risk information provided by the PRA, with particular attention to the role of the STI (Surveillance Test Intervals) included within the SR (Surveillance Requirements), and of the AOT (Allowed Outage Times) included within the LCO (Limiting Conditions for Operation).

Nowadays, regulatory bodies are encouraging the use or PRA where practical, consistent with the state-of-the-art, to support a risk-informed regulatory framework. The US Nuclear Regulatory Commission (NRC) issued RG 1.174 (2002), which is a key element in this framework to support risk informed decisions on changes to LB, which particularizes to analyze TS changes in RG 1.177 (1998). In this context, original PRA models and data need to be adapted and even extended for analyzing TS changes, depending on the particular requirement under study, e.g., STI, AOT.

RG 1.174 and RG 1.177 require that all sources of uncertainty be indentified and analyzed such that their impacts are understood at the technical element level. Guidance is being proposed on the systematic treatment of uncertainties associated with the use of the PRA in risk-informed decision making of LB changes, see references EPRI-1016737 (2009) and NUREG-1855 (2009). In addition, specific guidance has been proposed for the treatment of uncertainties in analyzing TS changes (Martorel et al., 2010).

In ref. (Martorel et al., 2010), it is proposed an approach and it is also provided an example of application for the treatment of uncertainties within a risk-informed decision-making framework to support the analysis of changes to Allowed Outage Times (AOT) using a level I PRA (see Figure 1). This paper focuses on the use of importance analysis, adopting both traditional and uncertainty importance measures (Aven 2010), within the approach proposed. A case study that focuses on an AOT change of the Accumulators System of a Nuclear Power Plant using a level I PRA is provided.

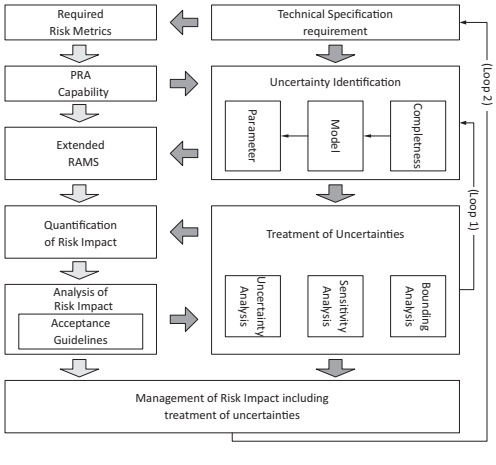


Figure 1. PRA based approach.

ACKNOWLEDGMENTS

Authors are grateful to the Spanish Ministry of Science and Innovation for the financial support of this work (Research Project ENE2010-17449).

REFERENCES

Aven, T. & Nokland, T.E. (2010). On the use of uncertainty importance measures in reliability and risk analysis. *Reliability Engineering and System Safety*, 95, 127–133.

Bizzak, D.J., Stella, M.E. & Stukus, J.R. (1987). "Identification and Classification of Technical Specification Problems", EPRI NP-54–75. Electric Power Research Institute.

EPRI 1016737 (2008). Electric Power Research Institute, "Treatment of Parameter and Model Uncertainty for Probabilistic Risk Assessments".

Martorell, S., Villamizar, M., Villanueva, J.F., Carlos, S. & Sanchez, A.I. (2010). Risk-Informed decision-making on changes to Allowed Outage Times addressing uncertainties. European Safety and Reliability Conference (ESREL), Rhodes.

RG 1.174 (2002). "An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis", USNRC.

RG 1.177 (1998). "An Approach For Plant-Specific, Risk-Informed Decision making: Technical Specifications", USNRC.

NUREG 1855 Vol. 1 (2009). "Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making", USNRC.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Importance analysis of multi-state system based on structural function methods

E. Zaitseva & V. Levashenko
University of Žilina, Žilina, Slovakia

ABSTRACT

Binary-State System (BSS) and Multi-State System (MSS) are basic mathematical model in reliability analysis. BSS is used allow description of initial system as system with two state: reliable and unreliable or functioning and failure. There are a lot of methods for estimation system based on this representation. MSS is mathematical model in reliability analysis that is used for description system with some (more than two) levels of performance (availability, reliability). MSS allows present the analyzable system in more detail than traditional Binary-State System. The MSS has been used for representation and reliability analysis of systems, such as, the manufacturing, production, water distribution, power generation and gas and oil transportation.

There are different directions for estimation of MSS behaviour. One of them is importance analysis. Importance analysis is used for MSS reliability estimation depending on the system structure and its components states. Quantification of this is indicated by *Importance Measure* (IM). They have been widely used as tools for identifying system weaknesses, and to prioritise reliability improvement activities.

Authors of the paper (Levitin et al., 2003) have been considered basic IM for system with two performance level and multi-state components and their definitions by output performance measure. The principal approach for calculation in (Levitin et al., 2003) is universal generating function methods. In paper (Ramirez-Marquez & Coit 2005) have been generalized this result for MSS and have been proposed new type of IM that is named as composite importance measures. New methods based on Logical Differential Calculus for importance analysis of MSS have been considered in paper (Zaitseva 2010) and new type of IM has been proposed. These measures have been named as *Dynamic Reliability Indices* (DRIs).

The mathematical tool of *Multiple-Valued Logic* (MVL) as Logical Differential Calculus is used for calculation of DRIs. The Logical Differential Calculus is mathematical tool that permits to analysis changes in function depending of changes of its variables. Therefore evaluate influence of every system component state change to level of MSS reliability by Direct Partial Logic Derivative (this approach is part of Logical Differential Calculus). Direct Partial Logic Derivative reflects the change in the value of the MVL function when the values of variables change.

There is one more mathematical approach of MVL that is used for MSS estimation (Zaitseva & Levashenko 2007). It is *Multi-Valued Decision Diagram* (MDD). MDD is natural extension of Binary Decision Diagram (BDD) to the multi-state case (Zaitseva & Levashenko 2007, Xing and Dai 2009). New methodology for MSS importance analysis based on Logical Differential Calculus and MDD is proposed.

REFERENCES

Levitin, G. et al. 2003. Generalised Importance Measures for Multi-State Elements Based on Performance Level Restrictions. *Reliability Engineering and System Safety* 82(3): 287–298.

Ramirez-Marquez, J.E. & Coit, D.W. 2005. Composite Importance Measures for Multi-State Systems with Multi-State Components. *IEEE Trans. on Reliability* 54(3): 517–529.

Xing, L. & Dai, Y. 2009. A New Decision-Diagram-Based Method for Efficient Analysis on Multistate Systems. *IEEE Trans Depenable Sec Comput* 6(3): 161–174.

Zaitseva E. 2010. Importance Analysis of Multi-State System by tools of Differential Logical Calculus. In: Bris, R., Guedes, C., Martorell, S. (eds) *Reliability, Risk and Safety. Theory and Applications*: 1579–1584. CRC Press.

Zaitseva, E. & Levashenko, V. 2007. Investigation Multi-State System Reliability by Structure Function. In *Dependability of Computer System (DepCoS-RELCOMEX'07)*; *Proc. intern. conf., 14–16 Jun 2007*, Szklarska Poreba, Poland: 81–88.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Integrated approach to assessment of risks from VCE's using phast risk and FLACS

N.J. Cavanagh & G. Morale
DNV Software, London, UK

ABSTRACT

Accidents like Buncefield and Texas City have put the risks from explosions high on the agenda of both regulators and operators. Models like TNO Multi-Energy and Baker-Strehlow-Tang have been used extensively in assessing the risks associated with such facilities. Over recent years, a number of projects have been completed to provide guidance on the application of these models including the GAME, GAMES and RIGOS joint industry projects (see for example Cavanagh et al., 2009, Cavanagh 2010).

However, the calculated overpressure when using these models as part of a QRA has been seen to be highly dependent on the assumptions made when breaking a plant up into a number of regions of congestion and confinement. For example, the well known GAME correlations for the Multi-Energy model (Eggen, 1998) relate peak side-on overpressure to specific geometric properties of the congested region and material properties of the flammable gas within the region. These have been seen to be very sensitive to the assumptions made when defining regions of congestion.

CFD sub-models can be used to assess maximum peak side-on overpressure or maximum flame speed for particular congested regions within your plant, as well as evaluating the extent of the region more accurately. Then, using the Multi-Energy or Baker-Strehlow-Tang correlations directly within your QRA based on these 3D sub-models reduces the uncertainty associated with these parameterised models without introducing the full complexity or time overhead associated with building a complete 3D CFD model. This paper describes a methodology we have developed where the Phast Risk QRA software model is used in conjunction with the FLACS CFD code to reduce the uncertainty associated with using simplified explosion models such as Multi-Energy and Baker Strehlow Tang, both of which are widely used in QRA. A case study is used to illustrate this approach and to highlight some of its advantages and disadvantages.

REFERENCES

Cavanagh, N.J. (2010). Recent advances in software for modelling the risks associated with gas explosions in congested spaces using the Multi Energy Method, 13th International Symposium on Loss Prevention and Safety Promotion in the Process Industry, June 6th–9th, Bruges, Belgium, 2010.

Cavanagh, N.J., Xu, Y. and Worthington, D.R.E. (2009). A Software Model for Assessing Fatality Risk from Explosion Hazards using the Multi Energy Method and Baker Strehlow Tang Approach, Hazards XXI Symposium, November 10th–12th 2009, Manchester, UK.

Eggen, J.B.M.M. (1998). GAME: Development of guidance for the application of the multi-energy method, TNO Prins Maurits Laboratory, ISBN 0717616517.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Monte Carlo and fuzzy interval propagation of hybrid uncertainties on a risk model for the design of a flood protection dike

P. Baraldi, N. Pedroni, E. Zio & E. Ferrario
Politecnico di Milano, Milan, Italy

A. Pasanisi & M. Couplet
Electricité de France, Chatou, France

ABSTRACT

In risk analysis, uncertainty is conveniently distinguished into two different types: randomness due to inherent variability in the system behavior (aleatory uncertainty) and imprecision due to lack of knowledge and information on the system (epistemic uncertainty) (Helton 2004).

Traditionally, probabilistic distributions have been used to characterize both types of uncertainty. However, resorting to a probabilistic representation of epistemic uncertainty may not be possible when sufficient data is not available for statistical analysis or information is of qualitative nature (Helton 2004). As a result of the potential limitations associated to a probabilistic representation of epistemic uncertainty under limited information, a number of alternative representation frameworks have been proposed (Aven & Zio 2010). Possibility theory, in particular, may be attractive for risk assessment, because of its representation power and its relative mathematical simplicity. The rationale for using possibility (instead of probability) distributions to describe epistemic uncertainty lies in the fact that a possibility distribution defines a *family* of probability distributions (bounded above and below by the so called possibility and necessity functions, respectively), which account for the expert's inability to select a *single* probability distribution and, thus, the imprecision in his/her knowledge of the epistemically uncertain parameters/variables (Baudrit et al., 2006).

In this paper, four methods for constructing possibility distributions are taken into account and a hybrid method, that jointly propagates probabilistic and possibilistic uncertainties combining the Monte Carlo technique with the extension principle of fuzzy set theory (Baudrit et al., 2006), is considered and compared with a pure probabilistic method for uncertainty propagation. The comparison is carried out with reference to a risk model concerning the design of a protection dike in a residential area closely located to a river with potential risk of floods. Two issues of concern are: i) high construction and annual maintenance costs of the dike; ii) uncertainty in the natural phenomenon of flooding. Then, the different design options must be evaluated in the face of uncertainty (Pasanisi et al., 2009).

In the paper, it is shown that the application of the pure probabilistic approach results in the estimation of one cumulative distribution of the model output that does not fully catch the *imprecision* typically affecting the poorly known variables subject to epistemic uncertainty. On the contrary, the hybrid approach is shown capable of *explicitly separating* the contributions coming from aleatory and epistemic uncertainties. In particular, in the application of the method to the case study of interest, in the estimation of the upper (plausibility) and lower (belief) cumulative distributions of the model output allows effectively distinguishing between the components of uncertainty due to variability and imprecision: the former is reflected by the *slope* of the belief and plausibility functions while the latter is pictured in the *gap* between the two functions. The larger gap between the belief and plausibility functions is explained by the larger area contained under the corresponding possibility distribution functions.

REFERENCES

Aven, T. & Zio, E. 2010. Some considerations on the treatment of uncertainties in risk assessment for practical decision making. Reliability Engineering and System Safety, 96 (1): 64–74.

Baudrit, C., Dubois, D. & Guyonnet, D. 2006. Joint Propagation of Probabilistic and Possibilistic Information in Risk Assessment. *IEEE Transactions on Fuzzy Systems*, 14 (5): 593–608.

Helton, J.C. 2004. Alternative Representations of Epistemic Uncertainty. *Special Issue of Reliability Engineering and System Safety*, 85 (1–3): 1–10.

Pasanisi, A., de Rocquigny, E., Bousquet, N. & Parent, E. 2009. Some useful features of the Bayesian setting while dealing with uncertainties in industrial practice. Proceedings of the ESREL 2009 Conference, Prague, Czech Republic: 1795–1802.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Procedures for aggregating experts' knowledge and group decision model approaches

T.V. Garcez, A.T. de Almeida-Filho & A.T. de Almeida
Federal University of Pernambuco, UFPE, Recife, Brazil

ABSTRACT

When objective information is complete, when there is sufficient historical data or when the stability of the process of generating such data is guaranteed, it is possible to generate probabilities or probability distributions from these data. But generally, in decision making and risk assessment (Zio, 1996), such information is not always complete or available, or when there is a need to consider uncertainty, experts must quantify their judgments and generate a subjective probability distribution.

In the event that the decision maker wants to acquire as much information as possible, he/she can consult other subjects who have more information or knowledge, preferably someone who is skilled in the area of interest (expert), and thus he/she can make use of multiple experts. Therefore making use of an expert in the decision-making process is of fundamental importance.

Winkler et al. (1992) list several reasons why the knowledge of multiple experts must be combined, (i) where the combined distribution produces a better evaluation than an individual distribution from both the psychological perspective (when it is expressed that more heads are better than one) or from the statistical perspective (when the average of the samples is better than one sample), (ii) the combined distribution can be thought of as a form of consensus, (iii) it is more reasonable and practical to use a single distribution probability when a more thorough analysis is needed.

When the probability distributions represent the respective judgments of several experts, one of the resulting distributions can be "thought" as a consensus of experts' decisions. Thus, the problem of determining this distribution can only be dealt with as a probability distribution consensus/ aggregation /combining problem. (Hampton et al., 1973; Winkler & Cummings, 1972; Kaplan, 1992).

In the area of Group Decision Making, some research has set out to achieve a solution based on inputs and feedback from multiple experts, given that this solution is the most acceptable to the group as a whole (Ekel et al., 2009).

Having shown the importance of various approaches to aggregating experts' knowledge, this paper proposes to investigate the use of Group Decision Making to aggregate expert opinions. First, a literature overview on aggregation methods already used will be made, which will be deemed the traditional approach, as will a conceptual review of Group Decision Making in order to seek features that justify its use as a new approach to aggregating experts' knowledge.

REFERENCES

Ekel, P., Queiroz, J., Parreiras, R. & Palhares, R. 2009. Fuzzy set based models and methods of multicriteria group decision making. *Nonlinear Analysis 71: e409–e419.*

Hampton, J.M., Moore, P.G. & Thomas, H. 1973. Subjective Probability and Its Measurement. *Journal of the Royal Statistical Society. Series A (General), 136(1): 21–42.*

Kaplan, S. 1992. 'Expert information' versus 'expert opinions.' Another approach to the problem of eliciting/ combining/using expert knowledge in PRA. *Reliability Engineering and System Safety 35: 61–72.*

Winkler, R.L. & Cummings, L.L. 1972. On the Choice of a Consensus Distribution in Bayesian Analysis. *Organizational Behavior and Human Performance, 7: 63–76.*

Winkler, R.L., Hora, S.C. & Baca, R.G. 1992. *The quality of expert judgment elicitations*. Nuclear Regulatory Commision Contract NRC-02-88-005. San Antonio, TX: Center for Nuclear Waste Regulatory Analyses.

Zio, E. 1996. On the use of the analytic hierarchy process in the aggregation of expert judgments. *Reliability Engineering and System Safety, 53: 127–138.*

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Sensitivity analysis of repetitive shock machine's vibration energy

J. Wan, B. Chen & Q.T. Wang
College of Basic Education of Command Officer, National University of Defense Technology, Changsha, China

ABSTRACT

The Repetitive Shock (RS) machine is one of main vibration testing equipments in the fields of Reliability Enhancement Testing (RET) in recent days. However, the middle and low frequency vibration energy of the RS machine is usually lower, which limits its applications. The sandwich vibration plate is one main part of the RS machine. It is significant to study the influence of vibration plate's material parameters on the transform characteristic of the middle and low frequency energy of pneumatic vibrators, and then choose the proper material parameters to improve the middle and low frequency vibration energy of the RS machine.

The sandwich vibration plate is made up of four layers from up to down: the first layer is a polymer plate; the second layer is an aluminum alloy plate; the third layer is made up of four aluminum bars fixed around the second plate; and the fourth layer is also an aluminum alloy plate. In this paper, the MSC.Patran and MSC.Nastran softwares are adopted to perform the sensitivity analysis of the middle and low frequency vibration energy on the material parameters of the first layer of the sandwich vibration plate.

Before the sensitivity analysis, the efficiency and precision of the MSC.Nastran software for the dynamic characteristic computation is validated by means of the comparisons of a single layer plate's computational results and the experimental results tested and analyzed by the Brüel & Kjær pulse system and ME's scope system.

The 3-D finite element model of the sandwich vibration plate is established by means of the MSC.Patran software. The sensitivity analysis of the RS machine's middle and low frequency vibration energy on the material parameters such as the structural damp coefficient, the elastic module, the density and the Poisson ratio of the first layer in the sandwich vibration plate is performed by means of the MSC. Patran and MSC.Nastran softwares.

The sensitivity analysis results indicate that the material parameters such as the elastic module and the density have apparent influence on the middle and low frequency vibration energy of the RS machine. Increasing the elastic module or decreasing the density of the first layer in the sandwich vibration plate can also be benefit to the enhancement of the middle and low frequency vibration energy of the RS machine. This work can provide some useful guides on the structural optimal design of the RS machine.

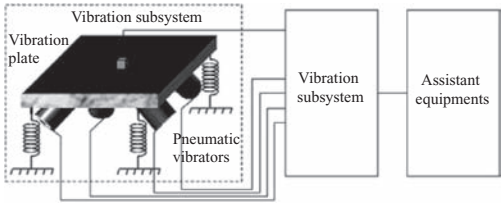


Figure 1. Composition of RS machine.

REFERENCES

Andonova, A.S. & Atanasova, N.G. 2004. Accelerated reliability growth of electronic devices. Proceeding of 27th international spring seminar on electronics technology: meeting the challenges of electronics technology progress: 242–246.

Kearney, M. & Marshall, J. 2003. Comparison of reliability enhancement tests for electronic equipment. Proceedings of the Annual Reliability and Maintainability Symposium: 435–440.

Lagattolla W. 2005. The next generation of environmental testing. Evaluation engineering 44(1): 44–47.

Polcawich, R.G., Feng, C. & Vanatta, P. 2000. Highly accelerated lifetime testing (HALT) of lead zirconate titanate (PZT) thin films. Proceeding of the 12th IEEE international symposium on applications of ferroelectrics: 357–360.

Wang, K. 2009. Research on energy spectrum optimization of vibration excitations produced by repetitive shock machine (PhD dissertation). Changsha: National University of Defense Technology.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Uncertainty analysis in probabilistic risk assessment: Comparison of probabilistic and non probabilistic approaches

Dominique Vasseur, Tu Duong Le Duy & Anne Dutfoy
Risk Management Department, Electricity of France R&D, Clamart cedex, France

Laurence Dieulle & Christophe Bérenguer
University of Technology of Troyes, UMR STMR, Institut Charles Delaunay/LM2S, Troyes Cedex, France

ABSTRACT

In order to better control the safety of its nuclear power plants, EDF developed Probabilistic Safety Assessments (PSA). Such studies involves the development of models that delineate the response of systems and of operators to initiating events that could lead to core damage or a release of radioactivity to the environment. The development of a PSA consists in building all the possible scenarios starting from an initiating event and calculating the probability of these scenarios. Each event of a scenario represents the failure (or the success) of a system mission or an operator mission. To allow the quantification of the scenarios, each mission system is modeled using a fault tree. PSA make it possible to evaluate the safety of the plants and to rank the plants components with regard to their risk contribution. PSA indicators are thus used to make decisions relative to plants design or procedures modifications, or to maintenance program optimization for example. To get robust decisions, it is necessary to take account of uncertainties in decision making process.

Uncertainties in PRA model are mainly epistemic ones and can be roughly split into two categories: parameter and model uncertainties. Epistemic uncertainty represents lack of knowledge with respect to the models or to the appropriate values to use for parameters that are assumed to be fixed but poorly known in the context of a particular analysis. The model uncertainties are due to different alternative assumptions that can impact the logical structures of event or fault trees of the PSA model. The treatment of these two types of uncertainty can be done in a probabilistic framework by Monte Carlo simulations for parametric uncertainties and by sensitivity studies for model uncertainties, such as proposed by Nuclear Regulatory Commission (Drouin 2009). But it can also be done in a non probabilistic framework called Dempster-Shafer Theory such as proposed in (Tu Duong *et al.,* 2011).

In this paper both approaches are used to assess the uncertainties associated to a case study related to a specific PSA application: the precursor events analysis. This application consists of studying the increment of a risk metric (core damage frequency) when an event challenging the safety occurs at the NPP. The results are compared in order to identify the advantages and the drawbacks of both approaches.

REFERENCES

Drouin, M., Parry, G., Lehner, J., Martinez-Guridi, G., LaChance, J. & Wheeler, T. 2009. Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-informed Decision making. NUREG-1855 Report, Vol. 1.

Tu Duong Le Duy, Dominique Vasseur, Laurence Dieulle, Christophe Bérenguer. Mathieu Couplet. Parameter and Model Uncertainty Analysis using Dempster-Shafer Theory in Nuclear Probabilistic Risk Assessment. PSA 2011 Conference, Wilmington NC USA.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty analysis of nanoparticles for cancer photothermal therapy

D. Barchiesi, S. Kessentini & T. Grosges
Université of Technology of Troyes, France

ABSTRACT

The treatment of diseases like cancer is a major societal issue. One of the ways to achieve this goal uses injected metallic nano-particles for burning the diseased tissue. This mode of therapy is known to be efficient, but remains currently in development. Some constraints have to be fulfilled for actual medical applications. First the particles have to be small enough to be renally eliminated and compatible for their use in tissues, while maintaining a sufficient thermal efficiency as well as a reproducible method of fabrication and control of their size. Despite a few papers devoted to their optimization, at our knowledge, neither sensitivity analysis nor study of the propagation of uncertainties, have been conduct to help to focus on the improvement of appropriate engineering process.

The basic operating principle of such metallic particles after embedment in cells, is based on their heating by an adequate illumination which passes through the biological tissues but is highly absorbed by the particles. The conversion of illumination in heating enables the local burning of the target cells. The model of this phenomenon is based initially on the resolution of Maxwell's equations which govern the interaction between light and matter, and the computation of the energy that is absorbed by the metallic particles (Mie's theory).

We propose an analysis of the propagation of uncertainties on the experimental parameters, through the model: the geometrical properties of the particles (radius and thickness of the metal coating if they are assumed to be spherical), and the material characteristics of the involved metals under illumination (complex optical index as a function of the illumination wavelength). For this, we use our former studies of optimization, giving the best parameters to get the highest temperature of the particles, and we consider a tolerance on its acceptable value. Then, we deduce a hypercube of acceptable parameters space, from realizations of a boundary adapted Monte-Carlo method. The principle of the method is to reduce the boundaries of the hypercube of parameters until stability, such they delimit a region where the absorbed energy is greater than a given fraction of its maximum, the maximum being determined by adapted heuristic optimization at each step. The proposed approach gives results in good agreement with those by SimLab (http://simlab.jrc.ec.europa.eu/). Moreover, the best performance of gold nano-shells is confirmed as well as the surprisingly low sensitivity of the temperature elevation to the material characteristics.

ACKNOWLEDGMENT

This work was supported by the "Conseil Régional de Champagne Ardenne", the "Conseil Général de l'Aube" and the *Nanoantenna* European Project (FP7 Health-F5-2009-241818).

REFERENCES

[1] Barchiesi, D. 2009. Adaptive non-uniform, hyper-elitist evolutionary method for the optimization of plasmonic biosensors. In *(IEEE) Proc. Int. Conf. Computers & Industrial Engineering CIE39*, pages 542–547.

[2] Kessentini, S., Barchiesi, D., Grosges, T., and Lamy de la Chapelle, M. 2011. Selective and collaborative optimization methods for plasmonics: A comparison. PIERS Online, 7(3):291–295.

[3] Barchiesi, D. 2011. Biosensors for Health, Environment and Biosecurity, volume 4, chapter Numerical Optimization of Plasmonic Biosensors. InTech - Open Access Publisher.

[4] Kessentini, S. and Barchiesi, D. 2010. A new strategy to improve particle swarm optimization exploration ability. In *IEEE 2010 Second WRI Global Congress on Intelligent Systems (GCIS)*, volume 1, pages 27–30, Wuhan, China.

[5] Kessentini, S., Barchiesi, D., Grosges, T., Giraud-Moreau, L., and Lamy de la Chapelle, M. 2011. Adaptive non-uniform particle swarm application to plasmonic design. International Journal of Applied Metaheuristic Computing, 2(1):18–28.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty analysis via failure domain characterization: Unrestricted requirement functions

L.G. Crespo
National Institute of Aerospace, VA, US

S.P. Kenny & D.P. Giesy
NASA Langley Research Center, Hampton, VA, US

ABSTRACT

This paper studies the reliability of a system for which a parametric mathematical model is available. The acceptability of the system depends upon its ability to satisfy several design requirements. These requirements, which are represented by a set of inequality constraints on selected output metrics, depend on the uncertain parameter vector $\boldsymbol{p}$. The system is deemed acceptable if all inequalities are satisfied. The constraints partition the uncertain parameter space into two sets, the failure domain, where at least one of them is violated, and the safe domain, where all of them are satisfied. The reliability analysis of a system consists of assessing its ability to satisfy the requirements when $\boldsymbol{p}$ can take on any value from a prescribed set. The most common practice in reliability analysis is to assume a probabilistic *uncertainty model* of $\boldsymbol{p}$ and estimate the corresponding probability of failure. Sampling-based approaches (Niederreiter 1992, Kall and Wallace 1994) and methods based on asymptotic approximations (Rackwitz 2001) are the engines of most (if not all) of the techniques used to estimate this probability.

Reliability assessments whose figure of merit is the probability of failure are strongly dependent on the uncertainty model assumed. Quite often this model is created using engineering judgment, expert opinion, and/or limited observations. The persistent incertitude in the model resulting from this process makes the soundness of the reliability analyses based on failure probabilities questionable. Furthermore, the failure probability fails to describe practically significant features of the geometry of the failure event. Some of these features are the separation between any given point and the failure domain, the location of worst-case uncertainty combinations, and the geometry of the failure domain boundary.

This paper proposes an uncertainty analysis framework based on the characterization of the uncertain parameter space. This characterization enables the evaluation of the features listed above, the approximation of the failure and safe domains and the calculation of arbitrarily tight upper and lower bounds to the failure probability. A significant thrust of this research is the generation of sequences of inner approximations to the safe and failure domains by subsets of readily computable probability. These sequences are chosen such that they almost surely fill up the region of interest. The methods developed herein, which are based on nonlinear constrained optimization, are applicable to requirement functions whose functional dependency on the uncertainty is arbitrary. Some of the most prominent features of the methodology are the substantial desensitization of the calculations from the uncertainty model assumed as well as the accommodation for changes in such a model with a practically insignificant amount of computational effort. The companion paper (Crespo et al., 2011) proposes strategies with the same goal but restricted to polynomial requirement functions.

REFERENCES

Crespo, L.G., Munoz, C.A. Narkawicz, A.J. Kenny, S.P. and Giesy, D.P. (2011, 18–22 September). Uncertainty analysis via failure domain characterization: Polynomial requirement functions. In *ESREL 2011*, Number 1, Trojes, France.

Kall, P. and Wallace, S. (1994). *Stochastic Programming*. New York: Wiley.

Niederreiter, H. (1992). *Random Number Generation and Quasi-Monte Carlo Methods*. Philadelphia, PA: Society for Industrial and Applied Mathematics.

Rackwitz, R. (2001). Reliability analysis, a review and some perspectives. *Structural Safety 23*, 365–395.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty assessment of reliability estimates for safety instrumented systems

H. Jin, M.A. Lundteigen & M. Rausand
Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

ABSTRACT

Reliability estimates play a crucial role in decision-making related to design and operation of safety instrumented systems (SISs). Unfortunately, the SIS is a highly complex system whose performance can seldom be fully understood. A reliability estimate is highly influenced by the simplifications and assumptions about the SIS as well as its operating environment, and therefore always subject to uncertainty. If the decision-makers are not aware of the level of uncertainty, they may misinterpret the results and select a SIS design that is either too complex or too simple to provide the necessary risk reduction.

In the context of decision-making related to a SIS, we define uncertainty as a measure of the decisionmaker's lack of confidence in SIS reliability performance. The paper is limited to so-called low-demand systems where the SIS reliability is judged based on its Probability of Failure on Demand (PFD). The PFD is subject to both aleatory and epistemic uncertainty. The focus is given to epistemic part in this paper.

This paper aims to elucidate the issue of uncertainties in relation to the estimation of SIS reliability. A new approach is proposed for (i) how to determine the level of uncertainty and (ii) how to take the uncertainty into account for SIS related decision-making.

Based on its sources, epistemic uncertainty is further divided into completeness, model, and parameter uncertainty. Methods are proposed to account for uncertainty caused by each of these categories. Qualitative assessment is suggested to determine the unknown and known completeness uncertainty level, and their contributions are combined to obtain the overall completeness uncertainty. This uncertainty is given as one out of five uncertainty levels. Model uncertainty is controlled by using prescribed consensus models. When using such models, the model uncertainty is considered to be broadly acceptable and this uncertainty is therefore not further considered in the decision-making process. The uncertainty associated with various input parameters are propagated into the reliability estimate by means of Monte Carlo simulation.

In the proposed approach, the inputs to SIS related decisions are changed from PFD_{avg} to a situation as shown in Fig. 1: A completeness uncertainty level and a uncertainty distribution of the reliability estimate. In order to ease the decision process, we still use a single PFD value for decisions. But it takes into account the epistemic uncertainty. This is achieved by basing the PFD value selection on the completeness uncertainty level. The basic principle is that the higher the uncertainty is, the more conservative the decisions should be, hence more confidence in the selected PFD value. A detailed PFD selection strategy is suggested in Table 1.

The proposed approach is illustrated by a case study of a High Integrity Pressure Protection System (HIPPS). The results show that the PFD value for decisions in a very high completeness uncertainty situation is about three times the value when the completeness uncertainty is very low. It is evident that SIS related decisions would be influenced. Therefore we conclude that an uncertainty assessment of the SIS reliability estimates is a valuable additional input in the SIS related decision-making process.

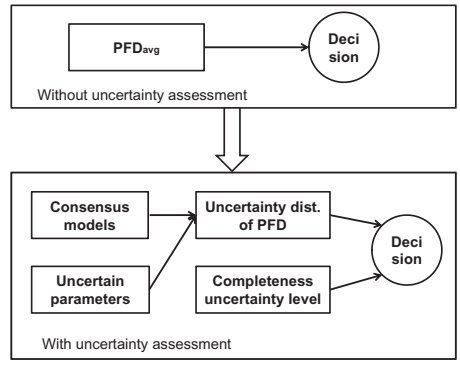


Figure 1. Inputs to SIS related decisions.

Table 1. Selection of PFD value for decisions.

Completeness uncertainty	LL	L	M	H	HH
Percentile in PFD dist.	50	60	70	80	90

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty propagation methods in dioxin/furans emission estimation models

G. Ripamonti & G. Lonati
DIIAR-Environmental Section—Politecnico di Milano, Milan, Italy

P. Baraldi & F. Cadini
Dipartimento di Energia—Politecnico di Milano, Milan, Italy

E. Zio
Ecole Centrale Paris and Supelec, Paris, France & Dipartimento di Energia—Politecnico di Milano, Milan, Italy

ABSTRACT

Environmental Impact Assessment (EIA) is required for public and private projects likely to have significant impacts on the environment. Due to its important role as decision-aiding and informative tool, the EIA procedure must be an open and transparent process leading to robust and reproducible outputs.

In this context, the EIA of waste incineration plants is usually developed with particular regards to the potential impacts on air quality by means of the following three main step: i) estimation of the source atmospheric emissions, ii) estimation of pollutant dispersion in the atmosphere, and iii) assessment of pollutant concentrations at the receptors. Unfortunately, uncertainties affect all these three steps due to the complexity of the environmental issue, in which scarcity of data and lack of knowledge are common practice. In particular, the final EIA outputs are seriously affected by the uncertainty of the values of the source emission estimation.

This work, focused on the emission assessment of a planned new waste gasification plant, has been conceived as a preliminary study to understand the applicability of the methods developed to describe uncertain variables to the whole EIA procedure, in order to provide a more realistic and objective description of the environmental impacts.

Probabilistic Methods (PMC) have been developed to describe uncertain variables by Probability Distribution Functions (PDFs) that are then propagated through the model by Monte-Carlo (MC) simulation. However, due to the scarcity of data typical of the environmental context, the analyst is often obliged to force statistically unjustified PDF on data on the basis of his subjective judgement. This subjective and arbitrary view of probability adds not declared assumptions in the analysis, causing a loss of transparency in the procedure.

Recently, various studies have brought evidence that under limited information availability uncertainty may be better described by possibilistic distributions and propagated by fuzzy interval analysis. Hybrid probabilistic-possibilistic Monte-Carlo methods (HMC) have been developed to propagate both probabilistic and possibilistic uncertainty representations.

In this work both a standard PMC and a HMC method are applied to an uncertainty propagation analysis in an emission estimation model for dioxins and furans (PCDD/Fs) for the new gasification plant. The emission model computes the emitted PCDD/F mass flow Q based on the PCDD/F concentration C_D in the emitted flue gas, and on the flue gas production V_F. The PMC method describes the uncertainty in both C_D and V_F in terms of PDFs and propagates it by a MC sampling simulation. The HMC method combines a MC sampling of the PDF of C_D and a fuzzy interval analysis of V_F, whose uncertainty is described in terms of a possibilistic distribution due to data scarcity.

The analysis shows that the HMC method allows separating the contributions to the output uncertainty due to C_D (probabilistic) and V_F (possibilistic). In particular, the HMC results define for the PCDD/F mass flow a belief-plausibility band extending by a roughly ±20% around the output distribution provided by the PMC method. The HMC method seems to process and communicate uncertainty more "transparently", clearly highlighting the contributions that, conversely, are hidden in the single PDF resulting from the PMC method. Furthermore, the information provided by the HMC outputs is more consistent with that available for the input parameters.

The satisfactory outcomes of this first study foster future works towards the extension of the HMC method to the remaining stages of the EIA procedure, and in particular to the assessment of the environmental fate of the pollutants and to the human health risk assessment for both carcinogenic and non-carcinogenic pollutants.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Variance based sensitivity analysis of interactive buckling

Z. Kala
Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT

Steel is a material with high resistance, and therefore it is made possible for designers to design light, slender structure. The more a member is slender, the more its load-carrying capacity influences buckling. In systems, it is necessary to solve the stability of the whole structure. The frame structures represent a typical example of a system consisting of more members.

The frame structure is characterized by the fact that members influence each other mutually. Interactions among input random imperfections and the influence of both of them on the ultimate limit state of steel frame structures are analyzed in the present paper. The interactions are studied on behalf of the global sensitivity analysis. The objective of these studies is to find how change of boundary conditions becomes evident in the influence of input imperfections on the load-carrying capacity. The variance-based method due to Sobol was applied.

In the paper, there is elaborated an analysis of the influence of boundary conditions on the results of sensitivity analysis of I-section symmetric portal steel plane frames. To be able to study the clear stability problem of systems, frames loaded on the top of columns were solved. Two types of boundary conditions were solved. The first steel frame has rotation and translation fixed boundary conditions of both column ends. The second steel plane frame is similar to previous frame with the exception that there is no rotation restrain at the column ends.

The geometrical beam nonlinear finite element solution of the load-carrying capacity was applied. The sensitivity indices were evaluated applying the LHS method. The sensitivity analysis results show that the proportion of factors influencing the load-carrying capacity is strongly dependent on boundary conditions.

The frames are typical lean-on systems. For the first frame, load-carrying capacity is significantly influenced by yield strength of the left column and the right one. The interaction between yield strength of the left column and the right one has the greatest signification. In case of the second frame, the interaction between the sway imperfection of the left and the right columns is the most significant. Therefore, it does not hold automatically that the imperfections with dominant influence of first order sensitivity indices have the most important interactions between themselves. Another important finding is the fact that the influence of bow imperfections is relatively low in comparison with the other quantities.

The abstract was elaborated within the framework of projects of TAČR TA01020307 and AVČR IAA201720901 and MSM0021630519.

REFERENCES

Kala, Z. 2005. Sensitivity analysis of the stability problems of thin–walled structures. Journal of Constructional Steel Research, 61(3): 415–422. doi:10.1016/j.jcsr.2004.08.005

Kala, Z. 2011. Sensitivity analysis of stability problems of steel plane frames. Thin-Walled Structures, 49(5): 645–651.

Kala, Z., Melcher, J. and Puklický, L. 2009. Material and geometrical characteristics of structural steels based on statistical analysis of metallurgical products. Journal of Civil Engineering and Management, 15(3): 299–307.

Saltelli, A. and Annoni, P. 2010. How to avoid a perfunctory sensitivity analysis. Environmental Modelling and Software, 25(12):1508–1517.

Saltelli, A., Chan, K. and Scott, E.M. 2004. Sensitivity analysis. Wiley series in probability and statistics. New York: John Wiley and Sons, p. 475.

Sobol' I.M. 1990. Sensitivity estimates for nonlinear mathematical models, Matematicheskoe Modelirovanie, 2: 112–118.

Sobol' I.M. 1993. Sensitivity analysis for non-linear mathematical models. Mathematical Modelling and Computational Experiment 1: 407–414; Translated from Russian.

This page intentionally left blank

Special topics: Risk and reliability importance measures

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Differential importance measures estimation through Monte Carlo and importance sampling techniques

S. La Rovere
NIER Ingegneria, Bologna, Italy

P. Vestrucci & M. Sperandii
DIENCA, University of Bologna, Bologna, Italy

ABSTRACT

The assessment of the RAMS (Reliability, Availability, Maintainability and Safety) performances of systems generally includes the evaluation of the "importance" of its components and/or of their "basic parameters". The computation of the Importance measures requires the evaluations of the system performances for different values of the input variables. It can be seriously time-consuming if the solution of the model requires the application of simulation techniques. Specifically, we refer to the estimation of the time-dependent unavailability of systems made up of repairable components, through an Indirect MonteCarlo simulation.

We propose the use of the Importance sampling techniques for the estimation of Differential Importance Measures, through one simulation of the model. All the output variables (system unavailability for different values of the input variables) are computed contemporaneously, on the basis of the same sequence of the components which cause the system state transitions, events type (failure/repair) and transition times for each trial.

The "basic procedure" requires the adoption of the "Forced specific transition" and "Forced transition rate" techniques. A number of analytical calculations substitute a number of simulations, reducing the computational time. A preliminary reduction of the variance on the output variables is obtained.

The presence of redundant components and the typical values of the failure and repair probabilities generally lead to the "rare events" condition. In this case, the "Forced System Transition technique" can be applied, assuring the occurrence of at least a system failure within the (residual) mission time.

Without lose of generality, we refer to a Networked system. We describe the procedure to be applied for the changes in the components (edges) transition rates, in order to estimate the first order Differential Importance Measure for components (edge and user node) and parameters and the Total order finite change sensitivity index for parameters.

The results coming from the application of the procedure to a simple network are compared with the analytical solutions. The effectiveness of the "Forced System transition" technique is verified in "rare events" condition. The relationship between the Total order sensitivity index for parameters and the Total order Differential Importance measures for components is currently under investigation.

REFERENCES

Borgonovo, E. 2009. Sensitivity analysis with finite change: An application to modified EOQ models, European journal of Operational research. 200: 127–138.

Borgonovo, E. 2010. The reliability importance of components and prime implicants in coherent and non-coherent system including total-order interactions. European Journal of Operational Research 204: 485–495.

Borgonovo, E. & Apostolakis, G.E. 2001. A new importance measure for risk-informed decision making. Reliab Eng Syst Safety 72: 193–212.

Dubi. 2000. A MonteCarlo application in system engineering. John Wiles and Sons.

La Rovere, S. & Vestrucci, P. 2010. Investigation of the Structure of a Networked System. Proc. SAMO10. Milan.

La Rovere, S. & Vestrucci, P. 2010. On influence of the structure of a Networked System on its performances. Proc. PSAM10. Seattle.

La Rovere, S., Vestrucci, P. & Sperandii, M. 2008. Risk significance importance measures for a networked system. Proc. PSAM9. New Orleans.

Labeau, P.E. & Zio, E. 2002. Procedures of Monte Carlo transport simulation for applications in system engineering. Reliab Eng Syst Safety 77: 217–228.

Marseguerra, M. & Zio, E. 2002. Basic of Monte Carlo method with application to system reliability. LiLoLe-Verlag GmbH.

Marseguerra, M. & Zio, E. & Podofillini, L. 2005. First-order differential sensitivity analysis of a nuclear safety system by Monte Carlo simulation. Reliab Eng Syst Safety 90: 162–166.

Rocco, C.M. & Moreno, J.A. 2002. Network reliability assessment using a cellular automata approach. Reliab Eng Syst Safety 78: 289–295.

Zio, E. et al. 2006. A combination of Monte Carlo simulation and cellular automata for computing the availability of complex system. Reliab Eng Syst Safety 91: 181–190.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Importance measures with finite changes: The relationship between Fussell-Vesely and total order reliability importance

E. Borgonovo
Department of Decision Sciences and ELEUSI, Bocconi University, Milan, Italy
Bocconi University, Italy

C.L. Smith
Department of Risk, Safety and Reliability, Idaho National Laboratory, Idaho Falls, ID, US

ABSTRACT

Importance measures are usually conceived either for extreme or for small changes. Risk achievement worth or risk reduction worth provide information on the effect of a component being always failed or always working. Fussell-Vesely (FV) quantifies the fractional contribution to risk of a component and is, therefore, a status quo risk measure (Cheok et al.1998). The Birnbaum (Birnbaum 1969) differential (DIM) (Borgonovo and Apostolakis 2001) and criticality importance measures (Borgonovo 2007) rely on small changes. However, in some applications, components are subjected to finite changes (ageing, inspection and maintenance plans etc.) and one needs to account for interactions (Borgonovo and Smith 2011). The problem of incorporating interactions in importance measures has been addressed in a stream of research extending the Birnbaum and differential importance measures for including interactions (Armstrong 1995, Zio and Podofillini 2006, Do Van et al. 2008, Borgonovo 2010, Do Van et al. 2010).

In this work, we study the relationship between FV and the total order reliability importance measure (D^T). We look for conditions under which these two importance measure coincide. Findings indicate FV is fractional contribution to risk (status quo), while D^T is a fractional contribution to risk-change. They coincide if a system is initially in a state of perfect reliability.

REFERENCES

Armstrong, M. (1995). Joint reliability-importance of elements. *IEEE Transactions on Reliability 44 (3)*, 408–12.

Birnbaum, L. (1969). On the importance of different elements in a multielement system. *Multivariate analysis, New York: Academic Press 2.*

Borgonovo, E. (2007). Differential, criticality and birnbaum importance measures: An application to basic event, groups and sscs in event trees and binary decision diagrams. *Reliability Engineering & System Safety 92*(10), 1458–1467.

Borgonovo, E. (2010). The reliability importance of components and prime implicants in coherent and non-coherent systems including total-order interactions. *European Journal of Operational Research 204*(3), 485–495.

Borgonovo, E. and Apostolakis, G. (2001). A new importance measure for risk-informed decision making. *Reliability Engineering & System Safety 72*(2), 193–212.

Borgonovo, E. and Smith, C. (2011). A study of interactions in the risk assessment of complex engineering systems: An application to space psa. *Operati forthcoming*.

Cheok, M.C., Parry, G.W. and Sherry, R.R. (1998). Use of importance measures in risk-informed regulatory applications. *Reliability Engineering & System Safety 60*(3), 213–226.

Do Van, P., Barros, A. and Berenguer, C. (2008). Reliability importance analysis of markovian systems at steady state using perturbation analysis. *Reliability Engineering and Systems Safety 93(1)*, 1605–1615.

Do Van, P., Barros, A. and Berenguer, C. (2010). From differential to difference importance measures for markov reliability models. *European Journal of Operational Research 204(3)*, 513–521.

Zio, E. and Podofillini, L. (2006). Accounting for components interactions in the differential importance measure. *Reliability Engineering and System Safety 91*, 1163–1174.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

On imprecision in relation to uncertainty importance measures

R. Flage & T. Aven
University of Stavanger, Norway

P. Baraldi
Polytechnic of Milan, Italy

E. Zio
Ecole Centrale Paris and Supelec, France
Polytechnic of Milan, Italy

ABSTRACT

A number of Uncertainty Importance Measures (UIMs) have been proposed in the literature to extend classical risk and reliability importance measures in the presence of epistemic uncertainty; ref. e.g. Aven & Nøkland (2010) and Borgonovo (2006). Uncertainty importance measures typically reflect to what degree uncertainty about risk and reliability parameters at the component level influences uncertainty about parameters at the system level. The definition of these measures is typically founded on a Bayesian perspective where subjective probabilities are used to express epistemic uncertainty; hence, they do not reflect the effect of imprecision in probability assignments, as captured by alternative uncertainty representation frameworks such as imprecise probability, possibility theory and evidence theory. In the present paper we consider the issue of imprecision in relation to uncertainty importance measures. We define a (Relative) Imprecision Removal Importance Measure ((R)IRIM) to evaluate the effect of removing imprecision. Two extents of imprecision removal are indicated: reduction to a probabilistic representation (type I) and removal of epistemic uncertainty (type II), the latter a special case of the former. In the present paper focus is put on type II imprecision removal; as further work we suggest to also consider type I imprecision removal. In a numerical example we consider a system consisting of three independent components, where component 1 and 2 are connected in a parallel configuration which is again connected to component 3 in a series configuration. Epistemic uncertainty about the availability of each component is described possibilistically as shown in Figure 1. Table 1 shows that the suggested Imprecision Importance Measure (IIM) ranks component 3 as the most important component in terms of imprecision removal, contributing to between 83.5 and 85.3 per cent (depending on which value the component 3 availability is fixed at) of the imprecision associated with the system availability.

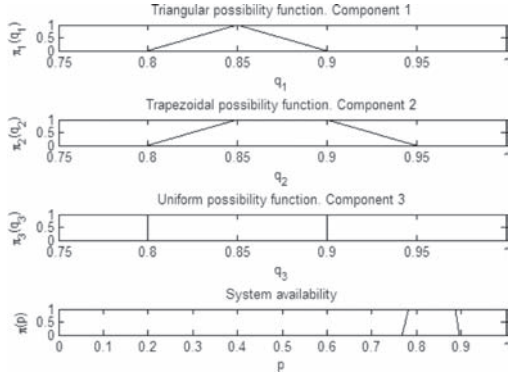


Figure 1. Input distribution functions on component availabilities and resulting system availability.

Table 1. Type II (R)IRIM value ranges.

i	$\text{IRIM}_i^{\text{II}}$	$\text{RIRIM}_i^{\text{II}}$
1	[0.0015, 0.0087]	[1.29%, 7.54%]
2	[0.0105, 0.0146]	[9.05%, 12.6%]
3	[0.0969, 0.0990]	[83.5%, 85.3%]

REFERENCES

Aven, T. & Nøkland, T.E. 2010. On the use of uncertainty importance measures in reliability and risk analysis. *Reliability Engineering and System Safety* 95(2): 127–133.

Borgonovo, E. 2006. Measuring uncertainty importance: Investigation and comparison of alternative approaches. *Risk Analysis* 26(5): 1349–1361.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Uncertainty in importance measures: Developing the Epistemic Risk Achievement Worth

E. Borgonovo
Bocconi University, Italy

C.L. Smith
Idaho National Laboratory, ID, US

ABSTRACT

Reliability importance measures are essential tools to support decision-making in several operational applications (Cheok et al., 1998, Borgonovo and Apostolakis 2001, Borgonovo and Smith 2011, Ramirez-Marquez and Coit 2005).

Risk or Reliability Achievement Worth (RAW) is one of the most widely employed importance measures. RAW is defined as the ratio of the reliability (or risk metric) value attained when a component is failed over the base case value of the reliability. Both the numerator and denominator are typically point estimates. Thus, the current definition of RAW is not reflective of a decision-maker's degree of belief (state of information) in the problem at hand, when epistemic uncertainty (Apostolakis 1990, Apostolakis 1995, Patè-Cornell 1996) is present.

Epistemic uncertainty can, however, be considered in two ways. In Modarres and Aggarwal (1996) and Borgonovo (2008) the variability in importance measure results generated by epistemic uncertainty is analyzed. Specifically, in Modarres and Aggarwal (1996) the distribution of importance measures is studied. In Borgonovo (2008) the influence of epistemic uncertainty in the safety categorization of SSCs is studied. In these works, uncertainty analysis is conducted on both the importance measure values and ranking in a Monte Carlo propagation. In other words, one computes the importance measure values for different possible realizations $\underline{x}^1, \underline{x}^2, ..., \underline{x}^M$ of the probabilities. In so doing, one is informed about her/his uncertainty in the ranking.

In this work, we propose an extension of RAW to the case in which epistemic uncertainty is taken into consideration. We call the new importance measure Epistemic RAW (ERAW). ERAW considers the effect of the component being down not only on the reliability point estimate but on its distribution generated by epistemic uncertainty. We discuss the properties of the new measure for series and parallel systems. In particular, for series systems, we show that aleatory uncertainty makes the value of ERAW independent of epistemic uncertainty. We then study how ERAW is linked to RAW for generic systems. Findings indicate that under the assumptions of

– aleatory and epistemic independence
– all point values

REFERENCES

Apostolakis, G.E. 1990: The concept of Probability in Safety Assessment of Technological Systems. *Science*, 250:1359–1364.

Apostolakis, G.E. 1995: A commentary on model uncertainty. 1995, In "Model uncertainty: its characterization and quantification," Center for Reliability Engineering, University of Maryland, Annapolis, MD, USA, October 20–22, 1993.

Borgonovo, E. 2008: "Epistemic Uncertainty in the Ranking and Categorization of Probabilistic Safety Assessment Model Elements: Issues and Findings," *Risk Analysis*, 28 (4), pp. 983–1001.

Borgonovo, E. and Apostolakis, G.E. 2001: A New Importance Measure for Risk-Informed Decision-Making, *Reliability Engineering and System Safety*, 72 (2), 193–212.

Borgonovo, E. and Smith, C.L. 2011: "A Study of Interactions in the Risk Assessment of Complex Engineering Systems: An Application to Space PSA," *Operations Research*, forthcoming.

Cheok, M.C., Parry, G.W. and Sherry, R.R. 1998: Use of Importance Measures in Risk-Informed Regulatory Applications, Reliability Engineering and System Safety, 60, 213–226.

Modarres, M. and Agarwal, M. 1996: "Consideration of Probabilistic uncertainty in Risk-Based Importance Measures," Proceeding PSA 96, Park City, Utah, September 29–October 3, 1996, published by the American Nuclear Society, La Grange Park, Illinois.

Paté-Cornell, M.E. Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and System Safety, 1996; 54:95–111.

Ramirez-Marquez, J.E. and Coit, D.W. 2005: Composite Importance Measures for Multi-State Systems with Multi-State Components, *IEEE Transactions on Reliability*, 54 (3), 517–529.

Special topics: Deterioration modelling with covariates

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Adaptive residual-based maintenance policy for a deteriorating system in dynamic environment

Xuejing Zhao
School of mathematics and statistics, Lanzhou University, Lanzhou, Gansu, China

Mitra Fouladirad & Christophe Bérenguer
Université de Technologie de Troyes, Institut Charles Delaunay, UMR CNRS 6279, STMR, Troyes, France

ABSTRACT

Optimal replacement problems for deteriorating systems have been intensively studied in the past decades (Wang 2002). Many models are developed for systems with increasing degradation evolving in a stationary environment. However in most industrial applications, the system is influenced by different risk factors, which are called explanatory variables (covariates). These variables describe the dynamical environment in the experiments of life science and engineering Singpurwalla (1995). An extensive literature on identification and application of covariates model, including theory and practical application, has addressed, e.g. Makis & Jardine (1992), Bagdonavicius & Nikulin (2000), Zhao et al. (2010).

This paper investigates the adaptive residual-based maintenance policy to utilize the information of the observed covariates state for a monotone deteriorating system. The increments of the degradation are modeled by a stochastic Gamma process. The covariates process is supposed to be a time-discrete homogeneous Markov chain with finite state space and the covariates effect on the deterioration is modeled by a multiplicative exponential function.

It is supposed that the system can only be observed by inspections. In this framework, the system is correctively replaced if the deterioration level exceeds a fixed level called failure threshold. To avoid the failure the system is preventively replaced if the deterioration level is higher than the preventive threshold but still lower than the corrective threshold. Replacements take place only in inspection times and a non-periodic inspection scheme is proposed as follows: at each inspection time the mean residual lifetime of the system is calculated and based on this value the next inspection time is scheduled.

We propose two types of residual-based inspection/replacement policy for the considered system: global maintenance and adaptive maintenance policy. The global maintenance policy doesn't take into account the covariates and in the framework of an adaptive maintenance the state of covariates is taken into account in the maintenance decision rule. For each policy we derive maintenance parameters (the preventive threshold and the inter-inspection function) which lead to a minimal long run average cost. By Monte Carlo numerical simulations the efficiency of the two maintenance policies is studied and the different inspection/replacement maintenance policies are compared.

REFERENCES

Bagdonavičius, V. & Nikulin, M. (2000). Estimation in degradation models with explanatory variables. *Lifetime Data Analysis 7*(1), 85–103.

Makis, V. & Jardine, A. (1992). Optimal replacement in the proportional hazards model. *INFOR 30*, 172–183.

Singpurwalla, N.D. (1995). Survival in dynamic environements. *Statistical Science 10*(1), 86–103.

Wang, H. (2002). A survey of maintenance policies of deteriorating systems. *European Journal of Operational Research 139*(3), 469–489.

Zhao, X., Fouladirad, M., Bérenguer, C. & Bordes, L. (2010). Condition-based inspection/replacement policies for non-monotone deteriorating systems with environmental covariates. *Reliability Engineering and System Safety 95*(8), 921–934.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

An adaptive sequential maintenance decision for a deteriorating system with covariates and maintenance constraints

Elias Khoury, Estelle Deloux, Antoine Grall & Christophe Bérenguer
Institut Charles Delaunay and STMR UMR CNRS 6279—Université de Technologie de Troyes, Troyes, France

ABSTRACT

In the last decades, the interest of decision making in maintenance has increased in order to reduce the associated costs and/or improve the durability and the reliability of a system. Intensive research activity on maintenance modeling has produced a lot of models for optimizing its scheduling. Condition-based maintenance (Wang 2002) is particulary efficient in terms of economical benefits and also in terms of system safety performance for a gradually deteriorating system when a condition variable is measurable. Actually, the pronostic is the prediction about the future state of the system. The most used pronostic is to predict how much time is left before a failure occurs (Jardine et al., 2006). This time is usually called Residual Useful Lifetime (RUL). The information about the actual condition of the system and the environment in which it evolves can be both used in pronostic. The condition-based maintenance combined to the pronostic leads to the predictive maintenance approach that would be more efficient, however, research about it is still limited (You et al., 2010). The main objective of this paper is to develop a predictive maintenance policy based on all the available information on the system and its environment.

In this context, we consider a gradually deteriorating system operating under an uncertain environment that impacts the degradation. The system is continuously monitored and it is assumed that its degradation level is always available. The system is subject to constraints, maintenance actions cannot be planned at any time (Dekker and Dijkstra 1992), it is possible only at fixed times called "maintenance opportunities". This corresponds to several cases for example aeronautic field, nuclear facilities, off-shore firms, etc. The information on the future environment and the upcoming maintenance opportunities is available, it should be then integrated in the maintenance decision model to provide better performance. However, it is only available on a limited period of time to which we refer by the "visibility horizon". As the system evolves, more information is available, it is then a "rolling visibility horizon". The objective is to use this sequential information to schedule the maintenance actions in the maintenance opportunities, in a way to reduce the costs. Therefore, we consider the RUL of the system given the available information and we use it in a cost-based indicator for maintenance decision support.

A case study is done to show the interest of the proposed maintenance policy. We consider a two-stages environment: "normal" and "stressed" usages. For each of the usage we assume that the deterioration follow an homogenous Gamma process (van Noortwijk 2009). To assess the performance of the proposed policy we compare it with a more classical policy on the basis of long-run cost rate. Numerical results show that the proposed policy is efficient in terms of cost reduction. The gain vary according to the model parameters. This dependance is investigated considering several parameters sets.

REFERENCES

Dekker, R. & Dijkstra, M. (1992). Opportunity-based age replacement: exponentially distributed times between opportunities. *Naval Research Logistics 39*(2), 175–190.

Jardine, A., Lin, D. & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical systems and signal processing 20*(7), 1483–1510.

van Noortwijk, J. (2009). A survey of the application of Gamma processes in maintenance. *Reliability Engineering and System Safety 94*, 2–21.

Wang, H. (2002). A survey of maintenance policies of deteriorating systems. *European Journal of Operational Research 139*(3), 469–489.

You, M., Liu, F., Wang, W. & Meng, G. (2010). Statistically Planned and Individually Improved Predictive Maintenance Management for Continuously Monitored Degrading Systems. *IEEE Transactions on Reliability 59*(4), 744–753.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Condition-based maintenance strategies for a partially observable deteriorating system

E. Deloux, M. Fouladirad & C. Bérenguer
Université de Technologie de Troyes, Institut Charles Delaunay, UMR CNRS 6279 STMR, Troyes, France

EXTENDED ABSTRACT

In this paper the aim is to propose a condition-based maintenance policy for a deteriorating system in uenced by the environment in which its is evolving. The term Condition-Based Maintenance (CBM) is used to signify the monitoring of a system for the purpose of maintenance. Information through monitoring is used to determine the current health status of a system and based on this information maintenance actions are performed to avoid failure. CBM has the potential to greatly reduce costs by helping to avoid catastrophic failures and by more efficiently determining maintenance action times.

One method for performing CBM is by using measurements on the deterioration level of the system. For a system subjected to CBM program, inspections are performed to obtain proper information about the deterioration state of the system. In order to avoid a failure occurrence hence a resulting period of inactivity of the system (duration between the instant of failure and the following inspection) a preventive replacement takes place when the system state enters in a particular state (or when the deterioration level exceeds a predefined threshold).

Most of works concerning the problem of decision making about monitoring and maintenance consider monotically deteriorating systems in a statical environment, see (Wang (2002), Abdel-Hameed (1975), Bérenguer et al., (2003), van Noortwijk (2009), Dieulle et al., (2003)). Recently more interest and attention are given to deterioration models including explanatory variables (covariates). These variables describe the dynamical environment in the experiments of life science and engineering and they are often expressed by the proportional hazards model, see (Singpur-walla (1995)). These variables can be some times monitored by inspections and some times they are completely unknown. If in the monitoring process the covariates can be observed it would be worthwhile to use these variables in the maintenance decision rule. Some times it is much cheaper to monitor these explanatory variables than the deterioration level. In this case it could be sensible to build a maintenance decision rule based only on covariates.

The structure of the paper is as follows. We model the deterioration process by a stochastic univariate process where the influence of the covariates is modelled by a multiplicative exponential function in section 2. In Section 3 we propose three optimal maintenance decision rules for the system under the consideration. Finally, in section 4 the performences of the proposed maintenance policies are studied through Monte Carlo simulation methods. For future works it would be interesting to study the impact of the preventive replacement cost variation and consider also other cox model parameters which translate more difficultly the deterioration state.

REFERENCES

Abdel-Hameed, M. (1975). A gamma wear process. *IEEE Transaction on Reliability 24*(2), 152–153.

Bérenguer, C., Grall, A., Dieulle, L. & Roussignol, M. (2003). Maintenance policy for a continuously monitored deteriorating system. Probability in the Engineering and Informational Sciences 17(2), 235–250.

Dieulle, L., Bérenguer, C., Grall, A. & Roussignol, M. (2003). Sequential condition-based maintenance scheduling for a deteriorating system. European Journal of Operational Research 150(2), 451–461.

Singpurwalla, N.D. (1995). Survival in dynamic environnements. Statistical Science 1(10), 86–103.

van Noortwijk, J.M. (2009). A survey of the application of gamma processes in maintenance. Reliability Engineering and System Safety 94(1), 2–21.

Wang, H. (2002). A survey of maintenance policies of deteriorating systems. European Journal of Operational Research 139(3), 469–489.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

On the gamma process modulated by a Markov jump process

Christian Paroissin
Université de Pau et des Pays de l'Adour, Pau, France

Landy Rabehasaina
Universite de de Franche-Comté, Besanon, France

ABSTRACT

Gamma process is one of the most popular stochastic process to model degradation of device in reliability theory (see the review by van Noortwijk). Here we propose and study a gamma process integrating covariates which evolves according to a Markov jump process (which is assumed to be independent of the underlying gamma processes). For lack of simplicity we restrict ourselves to a two-states Markov process (or binary Markov process), but it can be extended to a multi-state Markov process. This Markov process with two states 0 and 1 such that transition rates between 0 and 1 (resp. 1 and 0) is λ (resp. μ), and represents the environment in which the device is used. For instance assume that the device could be used under nominal stress (state 0) or accelerated stress (state 1).

The degradation process ($D(t)$) is described through the increments of two independent gamma processes whose parameters depend on the state of covariates. If the covariates are in state 0, then the degradation process will be governed by a gamma process with parameter (ξ, α_0) and if the covariates are in state 1, then the degradation process will be governed by a gamma process with parameter (ξ, α_1) with $\alpha_0 \leqslant \alpha_1$ (the average degradation is larger under higher solicitation use than under nominal condition).

The first problem we consider is the distribution of the hitting time T_c of a fixed level c by a such Markov modulated gamma process. Since (D_t) has increasing paths, it follows that it is sufficient to study the distribution of $D(t)$ for any $t \geqslant 0$. We have obtained an integral representation of the cumulative distribution function F_{T_c} of T_c by conditioning on the occupation time $\Delta_0(t)$ of state 0 between the interval $[0, t]$ (see the papers by Sericola for a study of this random variable).

Then we have deduced a stochastic order (in the usual sense) between hitting times. Indeed let us denote by $T_c^{(0)}$ the hitting time when $\mu = 0$ and by $T_c^{(1)}$ the hitting time when $\lambda = 0$. We proved that $T_c^{(1)} \preceq_{st} T_c \preceq_{st} T_c^{(0)}$.

At least we discuss about a simple problem of optimal maintenance. Assume that the degradation level of a device can be measured only during inspections (i.e. no continuous monitoring). We also assume that at each replacement the device is replaced by a new one or is perfectly repaired (AGAN) and that the replacement/repair duration is negligible. At least replacement occurs only after an inspection (in particular there is no replacement at failure times). Such maintenance scheme is a case of the so-called block replacement policy. Hence one can be interested in determining the optimal inter-inspection delay δ_*. To do it, consider the two following different costs: the cost c_r for replacing the device and the unavailability cost c_u. The asymptotic cost per unit of time is given by:

$$C_\infty(\delta) = \frac{c_r + c_u \int_0^\delta F_{T_c}(du(u))}{\delta}.$$

Let us denote δ_* the minimum of this cost function. It has been proved that δ_* is finite if $\mathbb{E}[T_c] > c_r/c_u$ and is infinite otherwise. We provide a numerical illustration of this problem which leads to conjecture that:

$$\delta_*^{(1)} \leqslant \delta_* \leqslant \delta_*^{(0)}.$$

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Preventive maintenance optimization for a degrading system subject to shocks with degradation-dependent maintenance costs

M.C. Segovia & P.E. Labeau
Service de Métrologie Nucléaire, Université Libre de Bruxelles, Belgium

ABSTRACT

Systems deteriorate due to continuous usage and aging, and they might be subject to random shocks that accelerate their deterioration.

The deterioration of a system entails a reduction of its global performances and eventually leads to its failure. A system working in a deteriorated condition might increase operational costs (because of larger energy consumption, delays in the production, reduction in productivity …), and an unplanned replacement also turns out to be quite costly. To limit the consequences of a system working in a deteriorated condition, preventive maintenance is performed.

Classical preventive maintenance policies (Barlow and Proschan (1996)) are considered in the study of a system subject to shocks and wear-out studied by Segovia and Labeau (2010). In the latter model, shocks cause damage to the system, influencing the wear-out process and accelerating its degradation. The study of the system is achieved by means of phase-type distributions (Neuts (1981)). Shocks occur with inter-arrival times following phase-type distributions and the lifetime of the system between shocks is also phase-type distributed, its phases referring to the different levels of degradation of the system. These degradation levels are associated to thresholds on the cumulated damage caused by the successive shocks undergone by the system. The magnitude of the different shocks follows a phase-type distribution too. The system can stand a limited number of shocks: following the arrival of the nth one, the system fails. The system also can fail due to wear-out before the arrival of the nth shock. Under these assumptions, the analytical expression of the survival probability function of the system was obtained.

The present paper extends the previous model by introducing classical as-good-as-new maintenance policies for the system rejuvenation. Corrective maintenance actions are performed when the system fails due to the wear-out process or to the shocks. In both cases the system is replaced by a new and identical one with an associated cost. In order to avoid the cost of such an unplanned replacement, different preventive maintenance actions are carried out and compared: First, a preventive maintenance action is performed when the age of the system is T, secondly a preventive maintenance action is performed when either the age is T or the degradation in the system reaches a determined level, whatever comes first. After a maintenance action the system goes back to an as-good-as-new state.

These classical maintenance policies are however adapted to the specificities of the our degrading system subject to shocks, by introducing two different criteria on which the preventive maintenance cost can depend: either the number of shocks that have occurred to the system or the level of degradation reached in the system.

A numerical application is performed in order to compare the different preventive maintenance actions and the different cost models.

REFERENCES

Barlow, R. & Proschan, F. (1996). *Mathematical theory of reliability,* 1965, SIAM, Philadelphia.

Neuts, M.F. (1981). *Matrix-Geometric Solutions in Stochastic Models-An Algorithm Approach*. John Hopkins University Press, Baltimore.

Segovia, M.C. & Labeau. (2010). Reliability estimation of a degrading system subject to shocks using phase-type distributions. Proceedings of the European Safety and Reliability Conference 2010 (ESREL 2010), Rhodes, Greece, 5–9 September 2010.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Statistical modelling of aeronautical turboshaft engines ageing from field and repair data feedback including preventive maintenance

A. Billon, P. Darfeuil & S. Humbert
Turbomeca, Bordes, France

L. Bordes & C. Paroissin
Université de Pau et des Pays de l'Adour, Pau, France

ABSTRACT

The aim of our studies is to propose a statistical model of turboshaft engines ageing behaviour in order to improve the reliability level assessment. Field and repair data feedback are used to fit our model. This model takes into account components whose failure mechanisms are in competition with respect to a final event and preventive maintenance policy. We want to estimate reliability of the main engine components and, for instance, optimize the preventive maintenance policy.

This article proposes a methodology in order to study the impact of a scheduled maintenance policy on one component reliability. First we present the model of one component ageing behaviour whose parameters are estimated from field and repair data feedback. Because these data account preventive maintenance policy, we will propose a method in order to estimate the component ageing behaviour without scheduled maintenance.

We consider a system with a single component whose several failure mechanisms compete with respect to the component failure. The following is the global methodology proposed to estimate the preventive maintenance policy impact.

First we estimate the component ageing model from field and repair data feedback. As a consequence, we estimate the ageing model including the preventive maintenance policy applied in service (the information about the maintenance operations is implicitly included in field and repair data feedback). This model put in competition two Markov processes whose parameters are estimated with the maximum likelihood method. Then we define an ageing model which takes into account a preventive maintenance policy. In this new model, the maintenance is explicitly modelled. To fit parameters of this new model, we minimize the distance (e.g., Cramèr-von Mises distance) between the new model and the model fitted using field and repair data feedback for the same scheduled maintenance policy (the one that is applied in service). Then we obtain a component ageing model without preventive maintenance that can be used to test several maintenance periodicities or to optimize a preventive maintenance policy.

In conclusion this article proposes a method to study the preventive maintenance policy impact on one component reliability. The main difficulty is to estimate the component ageing behaviour independently of the scheduled maintenance policy from field and repair data feedback (i.e., data including the maintenance effects). We also apply the proposed method to an example study that we present in this article. In an incoming work, we plan to take into account randomness of maintenance inspections (instead of a fixed periodic maintenance). This maintenance will take into account the removals due to the scheduled maintenances but also those due to the unscheduled maintenance. The final goal of this work is to set up a preventive maintenance optimization algorithm by fixing beforehand some optimal reliability criteria. It will make possible to choose the preventive maintenance policy guarantying an *a priori* reliability criterion.

REFERENCES

Billon, A. *et al.* (2010). Modélisation statistique des dégradations des moteurs aéronautiques à partir des données de retour d'expérience. Lambda Mu 17, 5–7 octobre 2010, La Rochelle (France).

Bocchetti, D. *et al.* (2009). A competing risk model for the reliability of cylinder liners in marine Diesel engines. Reliability Engineering and System Safety, vol. 94, issue 8, pp. 1299–1307.

Cook, R.J. & Lawless, J.F. (2007). The Statistical Analysis of Reccurent Events. Springer.

Special topics: Multiple Criteria Decision Aid (MCDA) and risk analysis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Assessing sustainability and risks: About using a Multi-Criteria Decision Aid methodology within an organization

M. Merad
INERIS, Verneuil-en-Halatte, France

N. Dechy
IRSN, Fontenay aux Roses, France

F. Marcel
INERIS, Verneuil-en-Halatte, France

ABSTRACT

The Sustainable Development (SD) principle is difficult to implement within the Organization. There is rarely an optimal solution in SD but most frequently a need to build compromises between conflicting aspects and risks such as economic, social and environmental ones. Moreover, information is rarely available and precise. In this paper we have used a Multi-Criteria Decision Aid (MCDA) methodology to cope with these difficulties. MCDA methodology offers the opportunity to avoid monetization of the different dimensions of the SD. These dimensions are not substitutable for one another and all have a role to play. MCDA is a branch of decision theory where actions or alternatives are chosen considering several points of view or criteria, assuming that the Decision Maker (DM) has all the information at his/her disposal concerning the alternatives, i.e., they are fully described by a vector of attributes which is supposed to be known without uncertainty. Two main features of this kind of problem make it difficult to solve. The first one is that attributes describing alternatives are heterogeneous, i.e., they represent different physical (or economical, subjective …) entities like price, size, color, weight, etc. and may be numerical or not. Hence a first difficulty is to make them commensurable in some sense. The second feature is that points of view or criteria are more or less important to make a decision, and most often they are conflicting or interacting in some way, so that it is not obvious to find how to combine them for reaching a final overall opinion.

There are several possible aggregation procedures in MCDA methodology. We have proposed a method to choose an adequate aggregation procedure for SD problems. Outranking approach (i.e., ELECTRE) easily solve the commensurateness problem by making pair wise comparisons. Mono-criterion synthesis approaches (i.e., MAUT approaches) rely on the construction of utility functions, which can be fairly difficult because of commensurateness problems, but then easily reach a final decision by combining utilities or scores of all criteria.

In this paper we have implemented two aggregation procedures to rank SD actions: ELECTRE III at a strategical level of decision and MAUT method based on the Choquet integral at an operational level of decision within an expertise Institute. Both methods present advantages and difficulties in a real life situation. The implementation of the ELECTRE III method for the ranking of 22 SD actions offer the opportunity to discuss incomparability situations where the actors involved can discuss their different visions and opinions about the implementation of the SD actions. Let us note that this method is easy to understand and communicate, perhaps due to the fact that the actors involved were familiar with this method that was used in daily situations for risk management and risk analysis problems (i.e., pesticide ranking, industrial accident scenario ranking, etc.). The implementation of the MAUT method based on Choquet integral was very helpful at an operational level. First, the engineer culture within the Institute is familiar with numbers and they appreciate the results of this method that offer the possibility of having a final score on actions that respect the incommensurability between the criteria. Second, this method offers the possibility of building a real interaction between the Analyst and the DM and testing the coherence on the action ranking.

REFERENCE

Merad, M. 2010. Aide à la decision et expertise en gestion des risques, ISBN: 978-2-7430-1265-6. Lavoisier.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)

Expertise and decision-aiding in safety and environment domains: What are the risks?

Myriam Merad
INERIS-BP 2, Verneuil-en-Halatte, France

Wassila Ouerdane
Ecole Centrale Paris—Département Génie Industriel, Châtenay-Malabry Cedex, France

Nicolas Dechy
IRSN, Fontenay aux Roses, France

ABSTRACT

Should the Analyst/Expert consider the impacts of his final recommendations in risk analysis and risk management processes? What are the risks induced by the practice of a decision aid activity in risk analysis and risk management processes? Is it possible to assess the quality of a decision aid activity? How can we do that and who has the legitimacy to do that? Such questions were raised by looking at the experience feedback after catastrophe of Texas City 2005, Toulouse 2001, Challenger 1986, Katrina 2005, … where for each major accident, we can notice that some analysts have provided to some Decision-Maker the necessary information, but these information was considered only after the disaster (*see* Llory and Montmayeul, 2010).

On one hand, in the decision aiding literature, the analyst has, in general, the aim to support the Decision Maker (DM) in order to: express his preferences, to structure the decision problem and to frame the final decision. Moreover, the role of the analyst is clearly distinguished from the DM by the fact that the former is involved neither in the decision situation nor in the implementation of the corresponding recommendations. His main objective is to help or aid in constructing the criteria of decision and the recommendations and at least to adapt them to the need of the DM, who has the responsibility of the final decision (ex. choosing a propertied mitigation measure).

On the other hand, the safety and environmental scientific and expertise community is often facing tricky and strategic decision situations. Therefore, the necessity to take into account and to reply to such question has been raised. Different answers were distinguished, depending on the discipline, the role played by the Analyst (s) in risk management process and to his (their) institutional position (s). For instance, many social scientists, especially those who work on experience feedback and accident investigation have argued in favor of the independency of the Analyst or Board of Investigators (Analysts) (ESReDA, 2009, Dechy and Dien, 2007; Dien et al., 2007) and have pointed the exemplary investigation done by the CAIB[1] about the accident of the space shuttle Columbia in February 1st, 2003. Some others, working in the field of risk perception and risk governance have insisted on the need of a more transparent and democratic process of expertise and decision-making in risk analysis and risk management processes and also on the problem of validation (Renn, 1998; Reid, 1999; Assmuth and Hilde, 2008; Rosqvist, 2010). Indeed, since stakeholders are impacted and affected by the decisions and the conclusions of the expertise, they should be consulted and involved in the decision aid and in the decision processes. Others scientists have focused on the difficulties of coping with the complexity of a decision aid context and situation and choosing the right model (Gertman et al., 1996; Horlick-Jones, 1998; Lagergren, 1998; Amendola, 2001; Fairbrother et al., 2007).

This paper will discuss the difficulties of being an Analyst in risk analysis and in risk management processes and proposes new concepts and discussions based on MCDA literature and practices.

[1] Columbia Accident Investigation Board.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

MCDA tools and risk analysis: The decision deck project

B. Mayag, O. Cailloux & V. Mousseau
Laboratoire de Génie Industriel, École Centrale Paris, Chatenay-Malabry, France

ABSTRACT

MultiCriteria Decision Aid aims at helping one or more Decision Makers (DMs), guided by one or more analysts, to prepare and make a decision where more than one point of view has to be considered. Its objective being not to force a decision at any cost, MCDA can range from a rational structuring of the decision problem to the elaboration of a decision recommendation. In this context, many methods and algorithms have been proposed in the literature. These methods can be schematically divided into two classes of methodologies:

- The outranking methods proposed by the European methodological school. Their objective is to build, using pairwise comparisons, a relation on a set of alternatives called the outranking relation, and to exploit it in order to solve MCDA problems (choice, sorting or ranking). To this category belong the ELECTRE methods (Figueira, Mousseau, and Roy 2005) and PROMETHE (Brans, Mareschal, and Vincke 1984).
- Methods based on the multi-attribute utility theory proposed by the American methodological school (Keeney and Raiffa 1976). The goal of these methods is to build a numerical representation of the preferences of the DM on the set of alternatives. Methods from this category include MAUT (Dyer 2005), MACBETH (Bana e Costa, Corte, and Vansnick 2005).

The interconnexion between MCDA and risk analysis has been proved. MCDA methods can be used to solve risk analysis problems such as:

- Computation of a risk scale: it can be done by using MCDA methods as ELECTRE TRI or by MACBETH methodology when the scale is quantitative;
- The evaluation of remediation solutions after an accident.

We present in this paper the Decision Deck (D2) project (http://www.decision-deck.org/) which aims at collaboratively developing Open Source software tools implementing MCDA. Roughly speaking, the Decision Deck project's objective is to provide an open source software, composed of various modular components, pertaining to the field of Multiple Criteria Decision Analysis (MCDA). It should give a user the possibility to add, modify or simply use existing plugged-in functionalities (plugins). These constituents can either be complete MCDA methods or elements common to a large range of procedures. The typical end-user of the Decision Deck platform is an MCDA researcher, an MCDA consultant or a teacher in an academical institution. These tools constitute an open source platform available for all communities, not only for MCDA community.

We show how MCDA methods implemented in Decision Deck can be useful for risk analysis, especially in risk assessment and remediation risk management. Thus, Decision Deck can be interpreted as a bridge between MCDA and risk analysis.

REFERENCES

Bana e Costa, C.A., Corte, J.-M.D. and Vansnick, J.-C. (2005). On the mathematical foundations of MACBETH. In J. Figueira, S. Greco, and M. Ehrgott (Eds.), *Multiple Criteria Decision Analysis: State of the Art Surveys*, pp. 409–437. Springer.

Brans, J.-P., Mareschal, B. and Vincke, P. (1984). Promethee: a new family of outranking methods in multicriteria analysis. In J.-P. Brans (Ed.), *Operational Research'84*. North Holland.

Dyer, J. (2005). MAUT - multiattribute utility theory. In Figueira, J., Greco, S. and M. Ehrgott (Eds.), *Multiple Criteria Decision Analysis: State of the Art Surveys*, pp. 265–285. Boston, Dordrecht, London: Springer Verlag.

Figueira, J., Mousseau, V. and Roy, B. (2005). ELECTRE methods. In J. Figueira, S. Greco, and M. Ehrgott (Eds.), *Multiple Criteria Decision Analysis: State of the Art Surveys*, pp. 133–162. Springer.

Keeney, R.L. and Raiffa, H. (1976). *Decision with Multiple Objectives: Preferences and Value Tradeoffs*. New York: John Wiley and Sons.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Parametrize a territorial risk evaluation scale using multiple experts knowledge through risk assessment examples

Olivier Cailloux & Vincent Mousseau
Laboratoire Génie Industriel, École Centrale Paris, Châtenay-Malabry, France

ABSTRACT

Assessing the risk levels associated with geographical zones involves multiple, and often conflicting, point of views, relevant for a Decision Maker (DM), or expert (who is either a single person or a collegial body): a zone may have a low risk according to one criterion while being exposed to a critical risk according to an other one. Examples of such criteria include the presence of a school or the percentage of vulnerable persons in the zone. Associating a risk level to a zone involves aggregating these point of views. This article suggests to use the tools developed in the domain of multicriteria decision aiding, which enable a formal approach to that aggregation problem when assessing risk. Multicriteria (MC) decision aiding aims at recommending a decision which is consistent with the value system of the DM.

Various methodologies have been proposed to support DMs facing a MC decision problem (Keeney and Raiffa 1976, Roy 1996, Bouyssou et al., 2006). In this paper, we consider the multicriteria (MC) sorting problematic to represent qualitative risk assessment models. The MC sorting problematic concerns ordinal classification of alternatives, here, zones, and consists in assigning each alternative to one of some pre-defined categories, here, risk levels ordered from the worst risk level to the less serious one. They can be e.g.: {Critical risk, Medium risk, Low risk}. The MC sorting method used here is a simplified version of ELECTRE TRI.

The assignment of a zone to an appropriate risk level relies on the zone's intrinsic value, i.e. a vector of risk factors associated with the point of views involved in the problem, and a set of subjective data representing the preferences of the considered DM and known as a MC sorting model. These preferential parameters may be elicited in a direct way, but this is often difficult as it requires the DM to undertand the fine details of their use in the considered MC sorting method. That is why it has been suggested to deduce the preferential parameters in an inverse way, by asking the DM examples of alternatives, or zones, and the category, or risk level, they would consider appropriate for these.

A supplementary difficulty arises when the evaluation method to be defined involve multiple DMs, as different stakeholders may favor different subjective parameter values. Applying inverse elicitation in a multiple DMs context amounts to ask each DM for a set of examples, which may be conflicting, and deduce preferential parameter values that may be either entirely shared by the DMs, or shared for a part of the parameters, and individual for other values. This is the approach we use in this article.

Previous works aiming to infer preferential parameters for the ELECTRE TRI procedure on the basis of assignment examples involve a single DM or suppose that a part of the preferential model is known beforehand. The method we propose enables a consensus to be approached by eliciting a subset of the parameters of the preference model shared by all DMs while leaving other parameters possibly different for each DM.

We detail a decision aiding process combining the proposed approach and existing ones to help building a risk evaluation scale on the basis of zone examples. The method is illustrated on an hypothetical example, and the details of the algorithm to infer the parameters are given.

REFERENCES

Bouyssou, D., Marchant, T. Pirlot, M. Tsoukiàs, A. and Vincke, P. (2006). *Evaluation and decision models with multiple criteria: Stepping stones for the analyst* (1st ed.). International Series in Operations Research and Management Science, Volume 86. Boston: Springer.

Keeney, R. and Raiffa, H. (1976). *Decisions with multiple objectives: Preferences and value tradeoffs*. Wiley, J. New York.

Roy, B. (1996). *Multicriteria Methodology for Decision Aiding*. Dordrecht: Kluwer Academic.

Special topics: Function-oriented monitoring and diagnosis

This page intentionally left blank

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Generating quantitative cause-consequence explanation for operator support systems

Akio Gofuku & Masahiro Yonemura
Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan

ABSTRACT

It is important to generate operator support information for taking a suitable counter action depending on a plant condition. This study proposes a technique to explain quantitatively the effect of a counter action by combining a qualitative causality propagation technique [Gofuku 2004] based on a functional model and a numerical simulation.

The reasoning process of a qualitative reasoning is basically to trace the influence of a cause along the connections of symbols in the model. This process is similar to that of human when he/she considers and explains how a cause influences. The qualitative reasoning can generate all possible paths to be influenced by a cause. On the other hand, a numerical simulation can predict a future condition of a plant when an anomaly happens or an operator action is taken. Considering the advantages and disadvantages of both a qualitative reasoning and a numerical simulation, this study combines complementally a qualitative reasoning based on an MFM model [Lind 1990, Lind 1994] and a static numerical simulation.

There are several steps in the proposed technique to generate quantitative explanation information of the effects of a counter action. By converting the information of a counter action into suitable formats, a numerical simulation and a qualitative reasoning based on an MFM model are conducted in parallel. The numerical values predicted by a numerical simulator are used to select correct influence propagation paths from the generated paths by the qualitative reasoning based on an MFM model. Then, the numerical values are incorporated into the linguistic explanation on the effect of the counter action along the selected paths.

The applicability of the proposed technique is examined by applying the technique to an oil refinery plant. A static numerical simulator is developed based on the simple mathematical models of components. An MFM model is constructed for the oil refinery plant. Quantitative explanations are generated to show the effects of several counter actions for an anomaly. As the results, it is confirmed that this technique can generate suitable explanation sentences including quantitative information of causal relations of the effects of a counter action.

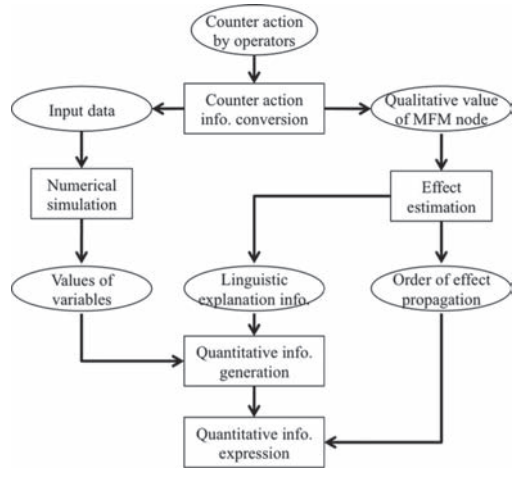


Figure 1. Flow of quantitative explanation information generation of the effects of a counter action.

REFERENCES

Gofuku, A., Ohi, T. & Ito, K. 2004. Qualitative reasoning of the effects of counter action based on a functional model, *Proc. CSEPC2004*, *Sendai, November 2004*, 43–48.

Lind, M. 1990. Representing goals and functions of complex systems - an introduction to multilevel flow modeling, *Institute of Automatic Control Systems, Technical University of Denmark*, Report No. 90-D-381.

Lind, M. 1994. Modeling goals and functions of complex industrial plants, *Applied Artificial Intelligence*, 8 (2): 259–283.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Multilevel flow modeling for nuclear power plant diagnostics

G. Gola
Institute for Energy Technology, Halden, Norway

M. Lind
Technical University of Denmark, Department of Electrical Engineering, Elektrovej, Lyngby, Denmark

H.P.-J. Thunem, A.P.-J. Thunem, E. Wingstedt & D. Roverso
Institute for Energy Technology, Halden, Norway

ABSTRACT

Innovative modeling approaches, techniques, and solutions are needed to support the monitoring and diagnostic requirements of current and future nuclear power plant designs. Longer fuel cycles, reduced staffing, higher intrinsic safety and other related factors are all likely to play an important role in shaping these requirements in the direction of additional flexibility, robustness and automation when compared to the systems and techniques that are currently used or being developed today.

Online monitoring techniques based on data reconciliation are currently available for early fault detection, i.e., for identifying abnormal residuals between measured and estimated parameters. Nevertheless, the actual analysis and interpretation of these results is typically a manual process. If one envisions the likely centralization of condition monitoring functions in fleet-wide monitoring centers, then it becomes evident that supporting functions such as automated diagnosis would become an all-important requisite.

In this paper, a modeling technique known as Multilevel Flow Modeling (MFM) is used within an innovative diagnostic scheme for automating residual analysis in nuclear power plants. MFM-based approaches have been successfully applied to diagnostics and to modeling of power systems.

The goal-and-function orientation of MFM exploits the principles of qualitative reasoning. MFM presents the plant at different levels of abstraction by defining the functions performed by the components toward the achievement of specific goals. Functions and goals are connected via causal relations. The propagation (backwards for fault diagnosis, forwards for prognostic purposes) of the information (e.g., related to system or sensor faults) is carried on by resorting to a model-based reasoning approach. Once the goal-and-function representation is defined, evidence about the plant state is collected and processed by a rule-based causal reasoning (i.e., a system which combines a number of generic rules with the actual casual relationships between functions specified in the MFM model) eventually resulting in the identification of abnormal states of some functions. The physical meaning of the MFM reasoning provides the diagnostic response.

Within the novel diagnostic scheme hereby proposed, a plant monitoring system called TEMPO developed at the Norwegian Institute for Energy Technology based on physical modeling and data reconciliation is used to analyze process measurements and possibly detect abnormal residuals. This information is translated into functional evidence for the MFM model and is used to trigger the reasoning process which eventually leads to the identification of the possible causal paths and associated root causes.

The TEMPO-MFM scheme has been applied to diagnosing faults in the secondary loop of the Loviisa-2 Pressurized Water Reactor (PWR) located in Finland. Evidence concerning residuals of different types is collected and translated into the corresponding states of the MFM functions. The reasoning system is triggered by one single abnormal residual and one causal path is identified and physically interpreted.

Overall, the on-line diagnostic scheme hereby proposed has indeed proved considerable potential advantages. In fact, the qualitative, linguistic-oriented representation of the plant coupled with the description in terms of goals and functions makes the approach very powerful to handle the diagnosis of complex systems and facilitates the operator communication.

Furthermore, the MFM representation of the system can be also used as an off-line tool to analyze faulty scenarios. In this view, triggering events can be manually inserted in the MFM causal reasoning and the resulting cause paths can be investigated for diagnostic purposes.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Reasoning about causes and consequences in Multilevel Flow Models

M. Lind
Department of Electrical Engineering, Technical University of Denmark, Kongens Lyngby, Denmark

ABSTRACT

The paper describes the use of Multilevel Flow Models (MFM) for reasoning about causes and consequences in complex dynamic processes. Reasoning in MFM models derives its power from representation of process knowledge on several levels of specification. The principles described in the paper have been used in the implemented in a model based reasoning system.

The basic ideas of MFM have been developed by the author and his research group and by research groups in several other countries. The research originated in problems of representing complex systems in Human Machine Interfaces for supervisory control but has developed into a broader research field dealing with modeling for design and operation of automation systems for safety critical complex plants. An up to date introduction to MFM is presented in (Lind, 2011).

MFM has been exploited for solving various diagnosis and control problems (Lind 1981, Fang & Lind 1995, Gofuku & Tanaka 1999, Petersen 2001) and for on-line alarm analysis (Larsson 2002). Applications for fault tree generation and risk analysis have been investigated by (Yang & Zhang & Peng & Yan 2007, Rossing & Lind & Jensen & Jørgensen 2009). MFM has been used for a range of industrial processes. Gola et al. (2011) describe an application of MFM for nuclear power plant diagnosis and Rossing et al. (2009) describe an MFM model of a distillation column in a study on risk analysis.

The paper presents novel results showing how process knowledge is efficiently represented and used in MFM for reasoning about events. It is shown that MFM represents process knowledge on four levels of specification. Three of the levels are discussed in detail in the paper and it is shown that the knowledge encoded on these levels is efficient for formulation of strategies for reasoning about causes and consequences of events. It is also demonstrated that the knowledge which is expressed by the means-end and functional topology of MFM models can be visualized and therefore used in human computer interaction to support diagrammatic reasoning in supervisory control.

REFERENCES

Fang, M. & Lind, M. 1995. Model Based Reasoning using MFM. Proc. Pacific Asian Conference on Expert Systems (PACES), May 16–18, Huangshan China.

Gofuku, A. & Tanaka, Y. 1999. Application of derivation technique of possible counter actions to an oil refinery plant. In Proc. 4´th IJCAI Workshop on Engineering Problems for Qualitative Reasoning, Stockholm Sweden: 77–83.

Gola, G., Lind, M., Thunem, H., Thunem, A., Wingstedt, E. & Roverso, D. 2011, Multilevel Flow Modeling for Nuclear Power Plant Diagnostics, Submitted to ESREL 2011, September 18–22, Troyes, France.

Larsson, J.E. 2002. Diagnostic reasoning based on means-end models: Experiences and future prospects. Knowledge-Based Systems, 15(1–2):103–110.

Lind, M. 1981. The Use of Flow Models for Automated Plant Diagnosis. In J. Rasmussen and W.B. Rouse (ed), Human Detection and Diagnosis of System Failures. Plenum Publishing Corporation: 411–432.

Lind, M. 2011. An Introduction to Multilevel Flow Modeling. Journal of Nuclear Safety and Simulation, 2(1):22–32.

Petersen, J. 2000. Causal Reasoning based on MFM. Proc. of CSEPC 2000 Cognitive Systems Engineering in Process Control, Taejon Korea, November 22–25 2000: 36–43.

Rossing, N, L., Lind, M., Jensen, N. & Jørgensen, S.B. 2010. A Functional Hazop Methodology. Computers in Chemical Engineeering, 34(2): 244–253.

Yang, M., Zhang, Z., Peng, M. & Yan, S. 2007. Modeling nuclear power plant with multilevel flow models and its applications in reliability analysis.In Proc. Intern. Symp. on Symbiotic Nuclear Power Systems for the 21´th Century (ISSNP), July 9–11, Tsuruga Japan.

Advances in Safety, Reliability and Risk Management – Bérenguer, Grall & Guedes Soares (eds)
© 2012 Taylor & Francis Group, London, ISBN 978-0-415-68379-1

Using an agent-oriented framework for supervision, diagnosis and prognosis applications in advanced automation environments

H.P.-J. Thunem & A.P.-J. Thunem
Institute for Energy Technology, OECD Halden Reactor Project, Norway

M. Lind
Technical University of Denmark, Denmark

ABSTRACT

Building and managing advanced automation environments for current and future nuclear reactor generations requires a full understanding of the risks and benefits associated with the increased complexity of dealing with all activities that in one way or another involve the automated process. In that regard, the usability aspects of the associated techniques and their contribution to increased (or decreased) situation awareness for various human-automation constellations during the modernization of reactor plants or engineering of new ones need to be investigated and clarified. Equally, a variety of deficiency modes as well as emergency scenarios must be carefully assessed.

Available and emerging techniques and tools for advanced supervision and control are based on a wide range of different methods for qualitative and quantitative engineering and analysis purposes. Different categories of these methods target different problem areas. Furthermore, even methods within the same category can be mutually distinct, as they might assume certain properties about the systems on which they are developed to operate. Thus, the methods and their supporting techniques and tools need to be applied in combination. To find their most suitable combinations, it is necessary to investigate their strengths and weaknesses.

This paper describes how an agent-oriented framework as a common supporting base for various methodologies and their tools can be used for Supervision, Diagnosis and Prognosis (SDP) applications in advanced automation environments. The framework itself is developed on the basis of a theory assuming that all socio-technical systems are multi-purpose and made of human, organizational and technical *agents* that together with their *assets* can fulfill various purposes, depending on their different manners of interrelations and interactions.

The framework, called ShapeShifter, was for the first time described in a paper published in the ESREL2010 proceedings (Thunem, 2010). The present paper briefly describes ShapeShifter's background and main application areas, the latter by means of its different supported tools TRACE (Thunem, 2009) and MímirBuilder (Thunem et al., 2010). It then proceeds to describe recent enhancements in terms of features for function-oriented fault-tolerant design and early fault detection, as a part of the framework's support for SDP-related activities.

The paper also provides a description of the main features of a tool, the MFM Editor, for function-oriented modeling and qualitative analysis, based on ShapeShifter and communicating with a qualitative reasoning tool that itself utilizes the function-oriented method Multilevel Flow Modeling (MFM) and its reasoning mechanisms (Lind, 2011). MFM has proven strength in qualitative planning, modeling and diagnosis activities in process control applications, particularly involving mass-, energy-, and control-related functions. The paper includes a brief introduction to the MFM method and its reasoning mechanisms.

REFERENCES

Lind, Morten (2011), An Introduction to Multilevel Flow Modeling, *International Journal of Nuclear Safety and Simulation*, 2(1), pp. 22–32.

Thunem, Harald P.-J. (2009), TRACE: A Generic Tool for Dependable Requirements Engineering, *Proceedings of ESREL 2009*, ISBN 978-0-415-55509-8, Vol. 1, pp. 137–142, September 7–10, Prague, Czech Republic.

Thunem, Harald P.-J. (2010), ShapeShifter: A Generic Framework for Identifying, Categorizing, Analyzing, Configuring and Managing Information Assets of Systems and Their Agents, *Proceedings of ESREL 2010*, ISBN 978-0-415-60427-7, pp. 390–396, September 5–9, 2010, Rhodes.

Thunem, Harald P.-J., Hoffmann, Mario, Bodal, Terje (2010), Mímir – Continued Work on a Modular Framework for Condition Monitoring and Diagnostics, *Proceedings of NPIC&HMIT 2010*, ISBN 978-0-89448-084-3, pp. 242–253, November 7–11, Las Vegas, Nevada.

References

Thematic areas

BBC. 2004. Scores die in Argentina club fire. BBC News,

December 31, 2004. Retrieved from http://news.bbc.

co.uk/2/hi/americas/4136625.stm Daamen W, Hoogendoom. 2003. Controlled experiments to derive walking behaviour. European Journal of Transport and Infrastructure Research SP; 3(1):39-59. Fang, Z., Lo, S.M. & Lu, J.A. 2003. On the relationship between crowd density and movement velocity, Fire Safety Journal, 38:271-283. Frei, R., Kingston, J., Koornneef, F., Van den Ruit, J. & Schallier, P. 2002. NRI MORT user's manual. For use with the management oversight and risk tree analytical logic diagram. Noordwijk Risk Initiative Foundation, 2002, AG Delft. Fruin, J. 2002. The cause and prevention of crowd disasters. In proceedings of the First International Conference on Engineering for Crowd Safety, http://www.crowdsafe.com/ Gupta, A.K. & Yadav, P.K. 2004. SAFE-R: a new model to study the evacuation profile of a building, Fire Safety Journal, 39: 539-556. Nelson, H.E. & MacLennan, H.A. 1988. Emergency movement. MA, USA:SFPE Handbook of fire protection engineering, NFPA Quincy. Pauls, J.L. 1980. Effective width model for evacuation flow in buildings. In Proceedings, Engineering Applications work-shop, Society of Fire Protection Engineers, 215-232. Perkins, L.B. 2004. Crowd Safety and Survival: Practical Event & Public Gathering Safety Tips. Lulu Press, 2004, USA. Retrieved from http://books.google.com.mx/bo oks?id=e8ThPTakU_0C&printsec=frontcover&sour ce=gbs_v2_summary_r&cad=0#v=onepage&q=&f= false Purser, D.A. & Bensilum, M. 2001. Quantification of behavior for engineering design standards and escape time calculations, Safety, 26: 157-182. The New York Times. 2000. Gas Attack in Lisbon Nightclub Leaves 7 Dead and 60 Injured. The New York Times, April 17, 2000. Retrieved from http://www.nytimes.com/2000/04/17/world/

Case study: Do activities and outcomes of the process safety

observations match?

Marko Gerbec

Jožef Stefan Institute, Department of Inorganic Chemistry and Technology, Ljubljana, Slovenia

ABSTRACT

Paper describes process of implementation of process safety incident investigation procedure in an SME company involved in LPG and technical gases storage and distribution. Realistic resources available at the SME size company were consid ered in the process of defining an incident inves tigation process, and main obstacles, approaches and solutions are briefly introduced. Further on, safety activities observations/monitoring in terms of SMS audit (EC, 1996), ARAMIS safety cul ture (ARAMIS, 2006) and violation motivation (Mason, 1997) surveys results were compared with three incident cases analyzed (safety outcomes) according to the 3CA (Kingston, 2002) and NRI MORT (Frei, 2002) methods.

Summaries of the results of the internal SMS audit carried out by the author, as well as results of both questionnaire surveys on multiple company sites among 58 workers/supervisors are presented. It was found that there is an issue related to the relationships between safety activities top ics categorizations compared to the categoriza tions selected for safety outcomes and author’s interpretations/reflections were needed.

However, generally, deficiencies revealed in activities monitoring were correspondingly found also in incidents caused (and vice versa), subject to suitable categorizations both using 3CA and NRI MORT methods/approaches.

Using 3CA method, from a total 20 Generic Organizational Systems (GOS) 11 were found somehow deficient by at least one incident, six by all three incidents, and four by at least two incidents analyzed. Comparison of the activities (using all three methods/approaches) to the outcomes categories for all three incidents analyzed, revealed that the deficient GOS could be "anticipated" by at least one activity monitoring approach, and eight of eleven by at least two or three approaches.

Using NRI MORT method, similar conclusions

Definition of an algorithm for accident identification

M. Nombela & E. Boix

Applus+ IDIADA, Santa Oliva, Tarragona, Spain

ABSTRACT

Worldwide, 1.2 million people die in road crashes yearly; 43,000 in Europe alone. This implies a cost to European society of approximately 160 billion euros, and takes up 10% of all healthcare resources. To reduce these rates, new active and passive safety

technologies which help to minimize the severity of injuries to vehicle occupants have been developed. However, studies have shown that most deaths due to road accidents occur in the time between the accident and the arrival of emergency medical services.

The aim of this study is to define an algorithm (and basically a methodology) which allows the vehicle to recognize when an accident has occurred and what kind of accident has taken place (frontal, side, roll-over or rear-end collision).

The project is based on the idea that each kind of impact shows a “typical” acceleration (lineal or angular) which is specific to each type of accident (frontal, lateral, roll-over, etc.). The methodology developed is based on the recording of the dam aged vehicle’s acceleration when a collision occurs.

To perform this study, a complete database includ ing information of the accelerations in different sorts of collisions is necessary. For each class of vehicle (supermini, small family car, large family car, small MPV, large MPV, executive, roadster sports, small off-road 4 × 4, large off-road 4 × 4, pick-up), accelerations corresponding to the same kind of collision were grouped, and studied in order to define same acceleration patterns. From those patterns, and for each type of vehicle and type of accident, an acceleration characteristic pulse and corresponding thresholds for each

scenario (severe/slight accident, no accident) were defined. The innovative aspects of this methodology are basically that, for each type of accident (frontal, side, rear-end) and for each class of vehicle, a maximum and minimum level of vehicle accelerations (linear or angular) are defined for the SEVERE ACCIDENT, SLIGHT ACCIDENT and NO ACCIDENT scenarios. A direct application of this algorithm could be to include it in an onboard unit on vehicles, and use it in emergency call applications (eCall). eCall devices have been developed to automatically notify emergency services in the event of an accident, in which a fast and efficient rescue operation can significantly increase the chances of survival of the severely injured. In order to reduce response time and improve the efficiency of the medical and technical services, fast and accurate accident identification is required. This on-board algorithm makes it possible to identify the type and severity of the accident allowing emergency services to respond accordingly; and as such could contribute to saving lives.

Feasibility of railway suicide prevention strategies: A focus group study

H. Rådbo, B. Renck & R. Andersson

Faculty of Social and Life Sciences, Karlstad University, Sweden

ABSTRACT

Suicide is a major public health concern, both

nationally and internationally. In Sweden, more

than 1200 people commit suicide every year,

amounting to about 25% of all injury deaths. Five

percent of these suicides occur on railways. From

a railway safety perspective, suicide constitutes a

clear majority (about 75%) of all Swedish railway

related fatalities. Several studies describe the fre

quency and characteristics of railway suicide in

different countries. Some of them also discuss vari

ous preventative possibilities. However, fewer studies, if any, analyze and evaluate such strategies in more detail. In Sweden, a comprehensive research program in this field is now underway. The ultimate goal is to develop a set of preventative strategies against railway suicide that can be used by the railway transportation providers themselves, as an integral part of their regular safety work.

The overall goal of this study is to explore preferences for preventative strategies against railway suicide among relevant professional groups.

For the above purpose, a focus group approach was chosen. Focus group interview is a qualitative method based on group dynamics intended to gain non-quantitative in-depth understanding of a certain phenomenon, not obtainable from individual interviews. In total, 22 interviewees were selected and divided into four groups. Each interview session began with a brief presentation of the results so far accumulated from the ongoing research programme. Thus, all participants were given a common platform for the discussion. The discussions were centred on railway suicide and possibilities for prevention, with special focus on possible environmental and technical changes in the railway system. The content analysis resulted in 16 categories, here structured and presented under themes identified through the analysis process. Theme 1: Measures

reducing the attractiveness of railway as a means of suicide. Theme 2: Measures obstructing the accessibility to the track area. Theme 3: Measures influencing the victim's determination while awaiting train. Theme 4: Early warning systems, enabling the train to brake sufficiently or the victim to be removed before collision. Theme 5: Measures to make the collision less violent and thereby less fatal and injurious. Our results show that there is general acceptance and understanding among practitioners of our proposed strategies to prevent railway suicide, although individual participants expressed some scepticism regarding how far one can reach in hindering individuals who are really determined to kill themselves in front of a train. Several concrete proposals were met with optimistic expectation and support. The results also support the validity of the proposed model for railway suicide prevention. All the principles encompassed by the model were considered relevant, although some of them were perceived to be more realistic than others as regards practical implementation. No major additional categories were identified from the interviews that were not already covered by the model.

Major accidents and their consequences for risk regulation

I.B. Dahle, G. Dybvig, G. Ersdal, T. Guldbrandsen, B.A. Hanson & J.E. Tharaldsen

Petroleum Safety Authority Norway, Stavanger, Norway

A.S. Wiig

Petroleum Safety Authority Norway, Stavanger, Norway

Department of Health Studies, Faculty of Social Sciences, University of Stavanger, Stavanger, Norway

ABSTRACT

The purpose of this paper is to study four major

accidents in the petroleum industry and their effects

on Health Safety and Environment (HSE) regula

tory regimes and lessons learnt at an industrial and

company level. Our cases are the following four

major accidents: Piper Alpha (1988), Texas City

refinery (2005), Montara (2009), and Deepwater Horizon (2010). Criteria for case selection: Accidents of major historical influence, new accidents with an assumed high influence on regulatory approaches and lessons learnt for the industry; Petroleum related accidents and accidents which we have the potential of gaining insights into development of regulatory regimes over time. Main aims of the paper are to examine implications for HSE regulatory regimes and industrial actors. In the paper we draw upon theories on risk regulation, systemic learning, safety culture and organizational reliability. Our methodological approach mainly relies on literature studies of accident investigation reports, but we have also applied other data material in our study such as written material, documents and documentaries. The results show that the examined major accidents have had and will most likely still have an impact on regulatory regimes. Changes are being made with regards to risk regulation practices and the organization of safety and energy departments, lessons are tried learnt across industrial sectors and shelves, safety management systems and technological solutions are improved, and higher degree of employee participation and involvement is often called for. Regulatory regimes are often changed from a prescriptive to a goal setting regime, the energy and safety division within the regulatory authority are being separated, safety case regime are being introduced, better formal and informal employee involvement is recommended, improvements of procedural and safety management systems and lessons are learnt with regards to improvement of barriers technical solutions.

Prevention of atypical accident scenarios through the use of resilience

based early warning indicators

N. Paltrinieri & V. Cozzani

Dipartimento di Ingegneria Chimica, Universita Bologna, Bologna, Italy

K. Øien & T.O. Grøtan

SINTEF Technology and Society, Safety Research, Trondheim, Norway

ABSTRACT

An “atypical” accident scenario is a scenario deviating from normal expectations and, thus, not deemed credible by common processes of risk assessment. Past experience shows that non identified accident scenarios as such represent a latent risk for industry and society and sometimes their occurrence can lead to consequences of unexpected extent. An evident example of an atypical accident was the major accident occurred at Buncefield on 11th December 2005. A detailed analysis of this and other cases in literature has shed some light on the complexity of their causal factors, demonstrating that an atypical major accident is not only the consequence of a single uncommon event, but rather the final result of deficient background conditions, such as the organizational failures represented in Figure 1.

Thus, it has been a big challenge to foresee

combinations of such failures and corresponding unidentified accident scenarios. Two complementary approaches to deal with this challenge are: i) improved identification of atypical scenarios, to reduce the occurrence of unforeseen events; ii) improved early detection, to reduce the possibility of remaining unforeseen events leading to an accident. For this reason the Resilience based Early Warning Indicator (REWI) (Øien et al., 2010) method has been considered in this contribution. In fact, the concept of resilience refers to the capability of recognizing, adapting to, and coping with the unexpected and one of its key characteristics is the interaction and interchange between different (organizational) system layers, levels, and focal points. The REWI method allows to establish a set of early warning indicators on the basis of issues of contributing success factors (CSFs) being attributes of resilience. The main aim of this work is to show the preliminary results of the application of this method to the site at Buncefield Table 1. Resilience based early warning indicators for a Buncefield-like oil depot referring to the CSF “Anticipation”. CSF Anticipation—Indicators 1 Portion of operating personnel participated in HAZID 2 Fraction of operational procedures that have been risk assessed 3 No. of reviews of safety reports in the last 5 years 4 Fraction of internal past events considered in safety report review 5 Fraction of external past events considered in safety report review Figure 1. Scheme of organizational

failures collected in the analysis of the accident at Buncefield (Paltrinieri et al., 2010). COMMUNICATION NEGLIGENCE POOR SUPERVISION & CONTROL KNOWLEDGE MANAGEMENT RISK AWARENESS Senior management Community Contractors Workforce

(Tab. 1), obtained by adapting the candidate set of

REWI indicators to the oil depot characteristics

and defining new indicators on the basis of the

accident causes. In this way it has been also pos

sible to understand the relevance of these resilience

based indicators as early warnings of the atypical

scenario and to demonstrate, by the correspond

ence of the defined indicators with the accident

causes, that this major accident would have been

likely prevented by the application of the REWI

method.

MIIB – Buncefield Major Incident Investigation Board

2008. The Buncefield Incident 11 December 2005,

Final Report, HSE Books. Øien K., Massaiu S., Tinmannsvik R.K. & Størseth F., 2010a, Development of Early Warning Indicators based on Resilience Engineering, PSAM 10, June 7–11 2010, Seattle, USA. Paltrinieri N., Wardman M., Dechy N., Salzano E. & Cozzani V., 2010, Atypical major hazard scenarios and their inclusion in risk analysis and safety assessments, Proceedings of the European Safety and Reliability Conference, ESREL 2010, Rhodes, Greece.

Suicide and the potential for suicide prevention on the Swedish rail

network: A qualitative multiple case study

H. Rådbo, I. Svedung & R. Andersson

Faculty of Social and Life Sciences, Karlstad University, Sweden

ABSTRACT

Suicide prevention deserves urgent attention. In Sweden, with a population of about 9 million, 1200–1400 individuals commit suicide annually, with about 5% of these events occurring on rail ways. Although the leading railway safety problem today (in terms of human loss) in many European and other countries, suicide is still a surprisingly neglected aspect of railway safety, and very little research is carried out on the problem. However, there is now a growing interest in the field and increasing attention is being paid to the suicide issue in railway safety circles. In Sweden, the Swed ish National Rail Administration, has initiated a research program to achieve a broader understand ing of the suicide problem in connection with the railway system and of the possibility of applying a systems-oriented approach to preventing railway suicide.

The aim of this study is to evaluate the content of existing reports on railway suicide incidents from a preventive perspective and to identify and cat egorise additional preventive-oriented information obtainable from independent site investigations.

This study is based on all police-reported

cases of railway suicide (22 cases in total) during

2003–2004 in a defined geographical area. Data on

each case were also collected from standard reports

by the Swedish National Rail Administration

(Banverket). In addition, all sites were visited for complementary data collection, resulting in both written and photographic documentation. There are both similarities and differences between the police and rail administration reports. The two organizations record information regarding background data on the victim and train involved, as well as the place and time of occurrence. Location characteristics are important for the identification of features favouring the choice of a certain place for suicide. Our analysis points to common traits in terms of conditions offering seclusion. Among our 22 cases, it is obvious that most victims sought seclusion for their final preparation. In summary, neither police, nor railway administration reports include many of the relevant details for the prevention of suicide on the Swedish Railways. There is major uncertainty regarding the exact time and place of the occurrence, and little or no information on victim behaviour and other circumstances preceding the collision is given, with the exception of the last few seconds as observed by train drivers. Structured in-depth investigations of railway suicide incidents may contribute considerably to the learning process regarding this phenomenon and how it can be prevented. To improve railway safety, more detailed information on the behavioural, technical and environmental circumstances characterising railway suicide incidents needs to be systematically collected and analysed on a regular basis. Bayesian methods This page intentionally left blank

An AHP-based approach of risk analysis in Bayesian belief networks

Bin Xie

Gexcon AS, Bergen, Norway

Jørn Vatn

Department of Production and Quality Engineering, Norwegian University of Science and Technology,

Trondheim, Norway

ABSTRACT

The aim of this paper is to present a new approach to integrate expert judgments into Bayesian Belief Networks. An approach is proposed for updating the conditional probability tables (CPT) when new soft evidence is obtained from expert judgment exercises. In the elicitation of beliefs from the experts, elements of the Analytic Hierarchy Process (AHP) are applied to reduce the work load.

A section of BBN is shown in Figure 1. CPT, for node X for the various combinations given parent nodes, will contain m columns and p rows.

Let Ci represent the ith combination of the parent vector of X. Element a ij , $1 \leq j \leq m$, $1 \leq i \leq p$, in the CPT is the probability that X takes the jth value given the ith combination of the parent vector. The objective is then for each combination, Ci, to use the expressed knowledge by the experts to update a ij .

Similar pairwise comparison in AHP is created in the following likelihood matrix. Let A 1 represents the situation that X takes the first value given C 1 , A 2 represents the situation that X takes the second value given C 1 and so on. Matrix A is denoted with

i as the row index, and j as the column index. Let b ij

represent Pr(X = A i |C 1)/Pr(X = A j |C 1), i,j ≤ m, i ≠ j.

Figure 1. Section of the BBN for demonstration of the

update in the CPT. A A A m A A A m b b m b 1 2 1 2 1 12 1 1 12 1 • • • • = • • • A ....1 .... 1 .... 1 1 1 b 1m ⎡ ⎣ ⎤ ⎦

An optimizational resource allocation method for series system

reliability life test

Qi Liu, Xiaoyue Wu & Jianrong Ding

College of Informational Systems and Management, National University of Defense Technology,

Changsha, P.R. China

ABSTRACT

Testing and demonstrating the system's reliability

is often a costly and difficult undertaking. And

sometimes, because of the constraints of cost and

available products, cannot reach at a desirable

target. To series system which all the subsystems

have life time and follow exponential distributions,

a Probability Constraint Programming Model

for Life System (PCPMLS) is proposed for the

verification of system failure rate. In PCPMLS,

a statistical hypothesis of system's failure rate is

constructed, the null hypothesis is that system's failure rate should be equal or greater than a given value. The objective of PCPMLS is to minimize the total reliability test cost. In PCPMLS, the total reliability test cost is supposed to be a linear function of subsystems' (system's) sample sizes and test durations. Considering the principle of small-probability event and reliability test requirement, the constraint conditions include posterior probability of null hypothesis should be equal or greater than a given confidence level, every subsystem (system) life test duration should be equal or greater than its given minimize test duration and be equal or less than another given maximum test duration, and single product's reliability test duration shouldn't be longer than its given longest test duration.

In order to make full use of the prior information of subsystems and system, the Bayesian Optimum Resource Allocation Model (BORAM) is developed to calculate the prior distribution of system's failure rate and posterior probability of null hypothesis. By BORAM, under the assumption of all subsystems are independent and exponential distributed, the expectation and variance

of system's failure rate are deduced. Under the assumption of subsystems' prior distributions and actual test results are the only sources of system's prior information, the moment method is used to calculate the hyper-parameters of the prior distribution of system's failure rate. And, to given actual system's reliability test result, the posterior probability calculation formula is given, and it is the function of subsystem's (system's) actual test results and hyper-parameters of subsystems' prior distribution. Because subsystems' (system's) reliability test durations are continuous variables, so it is impossible to list all the possible values of each variable and calculate all the possible posterior probability of null hypothesis, then find the optimum resource allocation plan. The grid based numerical algorithm (GBNA) for the solution of resource allocation plan is introduced to find the satisfactory solution. GBNA splits the solution space into small grids. The intersecting points of different grids are treated as temp feasible solutions. The purpose of GBNA is to find an optimum solution from all the temp feasible solutions, and based on the optimum solution, construct another solution space, and so on, the optimizational solution can be found out. Under the assumption that every subsystem (system) has no failure during its reliability test, the initial test plan calculation steps were given. And considering the possible failure during reliability test, the calculation method of sequential test plan was given. At last, considering a rocket engine, it consists of one thrust chamber (subsystem 1), one tank (subsystem 2), a feed mechanism (subsystem 3), a power source (subsystem 4), suitable plumbing or piping (subsystem 5), a structure (subsystem 6), and control devices (subsystem 7). The rocket engine is supposed to be series system, every subsystem (system) reliability test results are exponential distributed, and all subsystems are independent. For given constraint conditions, prior distributions of subsystems' failure rate, initial test costs, unit product test costs and unit time test costs of subsystems (system), the initial test plan calculation process is presented, and the optimizational initial test durations are carried out. Compare with other test plan, it is obvious that the optimizational test combination is the optimum test plan which satisfies the constraint

conditions and its test cost is the lowest one.

Assessing risk based on Bayesian networks and FMECA: A case study

L.M. Pedersen & M.H. Saltnes

Safetec Nordic, Norway

ABSTRACT

In this paper a Bayesian network-based method, used to assess the fire risk in relation to a product installed in houses, is presented. The paper uses a new approach where the Bayesian belief network (BBN) model is based on a failure mode, effect and criticality analysis (FMECA). The node probabilities in the BBN are determined from the frequency classes and consequence classes defined in the FMECA. The goal was to obtain knowledge of the risk affect of installing a product, as well as providing decision support on risk reducing measures.

Knowledge of the fire risk for a product for installation in or on houses was needed in order to minimise the risk of fire, fatalities and damage to property. Furthermore, if the product catches fire and the fire propagates to the house, the reputation of the product and the producer will be damaged and the producer may be held responsible for death of people. Hence, the producer had a request for

increased knowledge of the magnitude of the fire

risk and how the risk can be reduced before manu

facturing the product for sale. As the product is to

be integrated in houses, a larger amount of com

bustible material will be present than for earlier

products not integrated in houses. The complex

ity of the fire risk is due to where the fire arc and

heating may appear in addition to a wide variety

of combustible materials that may be present. The

method used for the original case is presented by

application on a simplified case. An FMECA was performed on the product to identify 1) where the ignition points could be and 2) where the combustible material may appear. Fire may appear when combustion material is close to ignition points. FMECA is not suitable for identification of combinations of failures, such as combinations of ignition and combustible material. A BBN model was therefore developed to explain the combinations between ignition sources and presence of combustible material that may initiate a fire. The frequency classes and severity classes from the FMECA were used to set the probability on each of the nodes in the Bayesian network. The model calculates the probability of initiated fire based on background knowledge and the assumptions made in the analysis by the specialists. FMECA is a systematic method to identify possible failure modes of a system and their effect on the system, but FMECA is not suitable for identification of combinations of failures. However BBN modelling is well suited for analysing the combinations between failures such as in this example. The method presented in this paper uses FMECA to identify possible failures and uses BBN to analyse the combinations of these failures. This method is useful when performing an FMECA and the analysis identifies combinations of failures that may be dangerous and must be further analysed. The method is also useful when performing a BBN without accurate input data. An FMECA could then be a good method to estimate classes of failure rates to use as input data.

Bayesian network for decision making on ageing facilities

P.A.P. Ramírez & I.B. Utne

Department of Marine Technology, Norwegian University of Science and Technology (NTNU),

Trondheim, Norway

ABSTRACT

Extension of the design lifetime of ageing installations has become a crucial issue for several oil and gas (O&G) companies. Even though large repairs and modifications may be required, keeping in operation the existing installations beyond the design lifetime will often be economically advantageous. A major concern regarding the life extension of the facilities is that safety and regularity should not be compromised. This can be achieved by implementing ageing management programmes to control and mitigate the degradation of the facilities (Brurok et al., 2010). Ageing management comprises physical ageing, obsolescence, and human and organisational issues (Petersson 2006). This paper focuses on physical ageing, which deals with degradation of systems, structures and components (SSCs).

An effective management of ageing includes assessing the actual condition of the SSC and deciding what actions must be taken for ensuring

safe and cost effective operation of the SSC. Usu
ally, four possible alternatives can be considered for
handling SSCs subject to ageing (Hokstad et al.,
2010): (i) use-up (i.e. using the equipment until
the end of service life), (ii) refurbishment (i.e. the
existing equipment is overhauled and restored with
old technology), (iii) replacement, and (iv) modi
fication. In addition to these alternatives, other
measures can be taken for controlling or mitigat
ing the ageing of the SSCs, such as increasing the
preventive maintenance, improving the condition
monitoring, and changing the operating condi
tions. Therefore, these measures may also affect
the final decision. The objective of this paper is
to introduce a procedure for applying Bayesian
Networks (BN) to support decision making about
equipment subject to physical ageing, taking into
account the factors that influence the safety, pro
duction assurance/availability and costs.

The paper describes the procedure for develop

Q. Mahboob
Pakistan Railways Lahore, Pakistan

D. Straub

Engineering Risk Analysis Group, TU München, Germany

ABSTRACT

Modern railway systems are equipped with automatic signaling as well as Train Protection and Warning Systems (TPWS) that control train movement and ensure the attention of the driver. In spite of reliable signaling and TPWS, trains are still passing red signals. These so-called SPAD events can lead to train derailment, head on collision with another train, collision with infrastructure and other adverse consequences. Investigations have been carried out to identify the critical components that lead to SPAD and subsequent train derailment. The classical way of modeling such events is by means of Fault Tree (FT) analysis. However, the FT methodology has limitations when modeling complex systems, which motivates the investigation of using Bayesian Networks (BN) for modeling and analyzing SPAD and other safety critical events in railway systems.

BN allows combining systematic, expert and factual knowledge about the system and is a flexible and compact form of system representation.

In this paper, it is studied whether the use of

BN provides significant advantages over the FT

methodology for the railway systems. The causes

of train derailment due to SPAD are analyzed

and the safety risk model for train derailment Figure 1. Bayesian Network for train derailment due to SPAD. due to SPAD is constructed using FT and then translated into the BN shown in Figure 1. The two methods are compared with respect to different modeling and analysis aspects that are relevant for railways.

Establishing prior probability distributions for probabilities that pairs

of software components fail simultaneously

M. Kristiansen

Østfold University College, Remmen, Halden, Norway

R. Winther

Risikokonsult, Oslo Area, Norway

B. Natvig

Department of Mathematics, University of Oslo, Norway

ABSTRACT

One possible way to assess and include depend

ency aspects in software reliability models is to

find upper bounds for probabilities that software

components fail simultaneously and then include

these into the reliability models. In Kristiansen,

Winther & Natvig 2011, a Bayesian hypothesis

testing approach for finding upper bounds for

probabilities that pairs of software components

fail simultaneously is described in detail. This

approach consists of two main steps: 1) establish
ing prior probability distributions for probabilities
that pairs of software components fail simultane
ously and 2) updating these prior probability dis
tributions by performing statistical testing. In this
paper, the focus is on the first step in the Bayesian
hypothesis testing approach, and two procedures
for establishing a prior probability distribution for
the simultaneous failure probability q ij are pro
posed. Both procedures consist of two main steps,
the first step being common for both of them.

1. Establish a starting point for q ij based on a
transformed beta distribution.
2. Adjust this starting point up or down by apply
ing expert judgement on relevant information
sources available prior to testing.

In the first procedure, the prior probability dis
tribution for q ij is determined by letting experts
adjust the initial mean and variance of q ij in the
transformed beta distribution based on relevant
information sources. In the second procedure,
the prior transformed beta distribution for q ij is
adjusted numerically by letting experts express
their belief in the total number of tests and the
number of simultaneous failures that all relevant

information sources correspond to. The main motivation for establishing a prior probability distribution for q ij is to utilise all relevant information sources available prior to testing in order to compensate for the enormous number of tests which is usually required to satisfy a predefined confidence level C 0,ij . In the case where reasonable prior information is available, the number of tests which mustbe run to achieve C 0,ij can be greatly reduced. Both procedures assume that relevant information sources can be assigned values in the interval [0, 1]. A value close to 0 can for example indicate substantial difference in development methodologies, great diversity between development teams or low complexity of the interface between the software components. On the other hand, a value close to 1 can for example indicate use of identical development methodologies, extreme complexity of the interface between the software components or that components are developed by the same development team. The idea is that the larger (closer to 1) the values of the relevant information sources I i are, the larger is the mean for the simultaneous failure probability in the first procedure and the number of simultaneous failures in the second procedure. REFERENCE Kristiansen, M., Winther, R. & Natvig B. (2011). A Bayesian Hypothesis Testing Approach for Finding Upper Bounds for Probabilities that Pairs of Software Components Fail Simultaneously. To appear in International Journal of Reliability, Quality and Safety Engineering (IJRQSE).

Parameter estimation in a reservoir engineering application

A.M. Hanea

Institute of Applied Mathematics, Delft University of Technology, The Netherlands

M. Gheorghe

iBMG / iMTA, Erasmus University Rotterdam, The Netherlands

ABSTRACT

Reservoir simulation models are used not only in

the development of new fields, but also in devel

oped fields where production forecasts are needed

to help make investment decisions. When simulat

ing a reservoir one must account for the physical and chemical processes taking place in the subsur face. Rock and fluid properties are very important when describing the flow in porous media.

In this paper the authors are concerned with estimating the permeability field of a reservoir. The problem of estimating model parameters such as permeability is often referred to as a history matching problem in reservoir engineering. Currently, one of the most widely used method ologies which address the history matching prob lem is the Ensemble Kalman filter (EnKF) (e.g. (Aanonsen, Naedval, Oliver, Reynolds & Valles 2009; ?)). EnKF represents the distribution of a system state using a collection of state vectors, called an ensemble. EnKF is a Monte-Carlo imple mentation of the Bayesian update problem. The Bayesian update is combined with advancing the model in time, incorporating new data when avail able. Traditional EnKF requires the assumption of joint normality. Moreover, when the size of the ensemble used is much smaller than the size of the state vector, unreal/spurious correlations between variables may be noticed. Given the dimension of the reservoir engineering applications, this is often

the case. The methods used to eliminate spurious correlations introduce other inconsistencies in the modelled system. Considering these limitations of the EnKF method, a new approach based on graphical models is proposed and studied. The graphical model chosen for this purpose is a non-parametric Bayesian network (NPBN) (Hanea 2008). A NPBN consists of nodes which represent random variables and arcs which represent direct dependencies among the variables. The

Reliability based design of engineering systems with monotonic models

M. Rajabalinejad & C. Spitas

Department of Engineering Design, Delft University of Technology, Delft, The Netherlands

ABSTRACT

A computationally efficient Bayesian Monte Carlo for Monotonic (BMCM) models for reliability based design of engineering systems is described in this paper. The model employs Gaussian dis tribution and monotonicity principles that have been implemented in the Dynamic Bounds (DB) method (Rajabalinejad 2009) integrated with a Bayesian Monte Carlo (BMC) technique. Signficant improvements in the computational speed of coupled DB and BMC methods are real

ized by incorporating a weighted logical depend
ence between neighboring points of the limit-state
equation (LSE) as prior information and global
uncertaintiy concept for quantifying variations of
the controlling input variables. The outcomes of
preceding simulations are factored in subsequent
calculations to accelerate computing efficiency
of the Monte Carlo method. The theory and
numerical algorithms of the BMCM are described
in this paper, and extension of the BMCM to
multi-dimensional problems is provided.
The DB and BMC techniques are combined
and used in this research to assess reliability of e
engineering systems. We investigate in this paper
potential merits of using Gaussian distribution
with monotonic models in reliability engineering.
The system parameters can be classified as con
trol and noise factors. The controlgroup includes
parameters that can be controlled by designer.
Those that are difficult or expensive to control are
the noise factors. In this paper, a statistical deci
sion theory is applied to increase the performance
by integrating different types of prior information.
This motivated the development of an approach
that could take advantages of DB and BMC

methodsusing monotonic models. Since the Gaus

sian distribution is widely used in engineering to

characterize variations of system parameters,

Towards a Bayesian Network methodology to improve maintenance

of complex semiconductor systems

M.F. Bouaziz & E. Zamaï

G-SCOP, Grenoble INP, Grenoble, France

S. Monot & F. Duvivier

PROBAYES, Montbonnot, France

S. Hubac

ST Microelectronics, Crolles, France

ABSTRACT

Today, it is a well-known fact that the evolution

of microelectronics is characterized by an intense

competitive environment between manufacturers

in different regions of the world. The semiconduc

tor industry must be able to produce Integrated

Circuit (IC) with reduced cycle time, improved yield

and enhanced equipment effectiveness. Besides

these challenges IC manufacturers are required to

address the products scrap and equipment drifts

in a complex and uncertain environment which

otherwise shall severely hamper the maximum

production capacity planned. The study presented

in this paper is supported by European project

IMPROVE (Implementing Manufacturing science solutions to increase equiPment pROductiVity and fab pErformance). This project includes several industrial partners such as ST Microelectronics, Austria Micro Systems, LFoundry; industrial solu tion providers as Probayes Company and academic partners such as G-SCOP laboratory, EMSE-CMP school … It aims to improve European semicon ductor fabs efficiency by providing methods and tools to act in complex and uncertain contexts. The objective of this paper is to propose a generic method to develop a model to predict the Equipment Health Factor (EHF) which will define decision support strategies on maintenance tasks to increase the semiconductor industry performance. Firstly, this paper presents a literature review about maintenance and risk analysis methods. Giving the system characteristics, Bayesian Network techniques are the special focus in this paper. BNs are capable of modeling causal dependency even if information are imperfect or missing and could incorporate the expert judgments (Murphy 2002). Then, a methodology (Figure 1) to develop a model is proposed. The EHF model is based on statistic and probabilistic calculations. Following

the proposed methodology, industrial case study

benchmarked on a semiconductor manufacturing

Work time loss prediction by exploiting occupational accident data

E.C. Marcoulaki, I.A. Papazoglou & M. Konstandinidou

System Reliability and Industrial Safety Laboratory, NCSR “Demokritos”, Athens, Greece

ABSTRACT

According to EUROSTAT (2007) 3.2% of workers

in the EU-27 had an accident at work during a one

year period, which corresponds to almost 7 mil

lion workers. Manufacturing, which covers a large

portion of industrial production, is third in the

ranking of occupational activities in what con

cerns the accidents rate. Among workers who had

an accident, 73% reported lost work days after the

most recent accident, and 22% reported time off

that lasted at least one month. Hence, due to an

accident at work, 0.7% of all workers in the EU-27

took sick leave for at least one month.

Some of these accidents require several days

leave before the worker recovers and can return to

work. Clearly, work time losses are directly related

to financial losses for the company. Work time loss

estimations cannot be based only on the number

of accidents, since the total loss is a function of

accident frequency as well as accident severity. For instance, accidents resulting to very minor injury may be dealt within the company premises with negligible loss of work time.

The present work considers Bayesian models for the prediction of work time losses due to occupational accidents occurring in an industrial work place. Meel & Seider (2006) developed a Bayesian approach to estimate the dynamic probabilities of accident sequences, tailored to chemical industries, and applied it on the analysis of incident databases. Marcoulaki et al. (2011) applied these tools to investigate the frequency of equipment failures and occupational accidents in Greek industrial sites. Bayesian inference methods are hereby used for the analysis of occupational accidents recorded in accident databases, to derive probability distributions for the prediction of:

i. the number of accidents occurring over a given time period in a company workplace

ii. the duration of the recovery period following an accident

iii. the percentage of time that the workers are recovering from accidents, so they are unavail

from individual and collective risk criteria

J.E. Kaufman & I. Häring

Fraunhofer Ernst-Mach-Institut, Efringen-Kirchen, Germany

ABSTRACT

Active protection systems are designed to protect vehicles against impact threat, e.g., from high speed armor-piercing kinetic energy projectiles, shaped charges, explosively formed projectiles or improvised devices. Active protection systems pro vide an essential addition to the protection spec trum, hitherto made up of passive and reactive protection (e.g., armor). Active protection systems can be classified into three categories according to the distance from the vehicle that the incom ing threat is physically intercepted and mitigated: close-in, middle-range and far-range. In any case, an active protection system intercepts an incoming threat prior to the threat is making contact with the outer surface of the vehicle platform.

Using an on-board computer system and sen sors, approaching threats are detected, tracked, classified and then mitigated if found to be a criti cal threat. In particular, in the event of intercep tion of close-in threats in an urban setting, the question arises which safety requirements have to

be fulfilled to avoid unintended functioning, pos

sibly resulting in casualties.

The paper presents a general approach that

applies to any hard-kill active protection system

that has to react in a very short time without

assuming specific technical system details. Figure 1

shows the top-view of a vehicle outfitted with an

active protection system consisting of n separately

deployable countermeasures (singular: CM, plu

ral: CMs). This two-dimensional representation

enables a quantitative risk assessment for persons

located within the dangerous area of one or more

CMs. The term countermeasure, CM, as used in the

paper, is a conceptual unit of the physical mecha

nism that intercepts an incoming threat. Each

CM i has a corresponding dangerous area, which is

depicted by a rectangle labeled DA i , 1 ≤ i ≤ n ∈ .

The CMs are assumed to be arranged on the vehi

cle, possibly with some spacing between adjacent

CMs or superposed. For the purposes of general

ity, the direction of action of the CMs is arbitrary

How the use of modelled scenarios can improve risk awareness

and risk control in complex environments

J.M. Hagen, B.O. Knutsen, T. Sandrup & M. Bjørnenak

Norwegian Defense Research Establishment, Norway

1 INTRODUCTION

Modelled scenarios depict how a variety of inci
dents occur and the ways in which preparedness
is challenged. In these scenarios, both security
and safety issues are addressed, and the timeline
is stretched through the phases “crisis preface”,
“crisis peak” and “post crisis normalization”. We
developed 20 modelled scenarios which can be fur
ther analysed and used for table top exercises and
for crisis management and emergency prepared
ness planning, including evaluation and exercises
with particular weight upon analysis of the latter.
The use of scenarios contributes to increased secu
rity and safety awareness, assisting researchers in
identifying mitigating measures and enhanced risk
control. The paper presents the applied method for
developing such modelled scenarios.

Systematizing the feedback received from senior
advisors at Norwegian Ministries of government
revealed a low awareness of rare disasters. First we
found that risk awareness varies among the differ
ent Ministries. Common threats are perceived to be
more relevant as compared with more spectacular and rare
threats. We also found that the perception of relevance
varied among the different Ministries. Since this scenario
package was in particular developed to trigger
civil-military co-operation and to invite to cross-sector

co-ordination, we found, surprisingly enough, that the Ministry of Defence did not see the relevance of more than just every fourth scenario, while the Ministry of Justice saw the relevance of just about half of the scenarios. Furthermore, dilemmas were encountered regarding scenario quality versus the ethical challenges and risks of displaying and thereby compromising national vulnerabilities. We also found that modelled scenarios can contribute to raising risk awareness and aid in extending the mental perception of threats among the different actors. The aim has therefore been to enhance a broader understanding of the threats that should also form the baseline in any risk analysis. The modelled scenarios can also be used for table-top exercises and workshops with the aim of analysing emergency preparedness and collaboration needs across sectors.

Interdependency-based approach of complex events in critical infrastructure under crisis: A first step toward a global framework

Babiga Birregah & Anne Muller

CREIDD, UMR STMR, University of Technology of Troyes, France

Eric Châtelet

LM2S, UMR STMR, University of Technology of Troyes, France

ABSTRACT

One of the major challenges in the management of critical infrastructures under major crisis is that complexity is intimately coupled with emergence of intrinsic properties. Any disturbance, even insignificant, can lead to widespread and compound crisis when some conditions are met. In most cases, accidents are modelled as a chain of discrete events which occur in a particular temporal order. The principle of domino effect, introduced

by Heinrich in the 1940's (Ferry 1988), has been used successfully in relatively simple systems for losses caused by failures of physical components or human errors. One other aspect for an efficient application of domino effect assessment is that the chosen events must be easy to handle and model. In addition, these models are sometimes limited to some complex systems (Hollnagel, Woods & Leveson 2006). The reasons can be the subjectivity or the incompleteness in the selection of the events and the conditions. Systemic approach of accident in critical infrastructures reveals that it is neces sary to take into account not only the succession of events, trigged by specific conditions, but also their "combinations". These events combinations involve the interdependencies between the subsys tems of the system. In this paper we define a critical infrastructure as a complex interconnected system of sub-systems (CI-SoS) connected by depend encies such as geographical, physical, cyber and logical—these last dependencies are usually called "functional" in risk assessment (Du-denhoeffer, Permann & Manic 2006, Rinaldi, Peeren-boom & Kelly 2001, Briš, Soares & Martorell 2009). We propose that the critical events, observed at the

system level, must be regarded as complex events

Learning decision making: Some ideas on how novices better can learn from skilled response personnel

M. Sommer

University of Stavanger, Stavanger, Norway

ABSTRACT

Decision making is a critical task of crisis and emergency management, and it is widely acknowledged that the response personnel's decision making during a response is important for the outcome. Learning to make adequate decisions in operational, high-risk settings is essential in developing competence and professional capability. Naturalistic Decision Making has contributed to new and better understanding of decision making in operational environments. This perspective focuses on experienced personnel operating in real life settings, trying to understand how people make decisions under time-pressured, stressing, risky, and dynamic situations.

Even if commanders and leaders normally undergo formal training and education, "on-the job" training appears to be invaluable and decisive in development of expertise in decision making (Flin & Arbuthnot, 2002). According to experi

enced practitioners (Lloyd & Somerville, 2006), “real learning” occurs when novices engage in actual practice, giving the novice access to information through physical practice, actual experiences and provision of information offered by experienced personnel.

To improve learning processes and performance, areas for learning, how information is made available and accessed, and individuals’ embodiment, must all be part of the analysis (Sommer & Njå, 2011). By using a combined approach to learning (combining socio-cultural elements and individual aspects) novices can better get access to and acquire skilled person’s “wisdom”.

There are two major challenges related to learning from skilled response personnel. The first challenge is that skills in situation assessment, and decision making in general, mainly rely on intuition and tacit knowledge. The second challenge is to present information (feedback, instructions, explanations, etc.) to novices in such a way that

D. Lachtar & E. Garbolino

Crisis and Risk Research Centre, Mines ParisTech, Sophia

Antipolis, France

ABSTRACT

Crisis management has become an essential activity for all public and private organizations. It is most often based on a specific tool called “cri sis cell” which aims to implement precautions of anticipation, vigilance and intervention to meet the targets.

In 2004, the French state established a legisla tion to modernize the civil defence to organize and manage crises (Bill to modernize the civil security, Senate, N°277). This law allows a municipality to establish a crisis cell to protect people and safe guard the environment.

However, these plans do not guarantee optimal performance of crisis units. Crisis cells may become particularly vulnerable, and unable to fulfill their missions according to the event.

The estimation of the decisions consequences in a risky situation will be delicate because of the complexity of urban land in question (physi cal structure, networks, etc.) and environment on which these decisions must be taken.

This fact underlines the importance of the implementation of a comprehensive approach for

decision making, particularly on indicators ensur

ing an effective management of emergencies in

terms of space and time.

The objective of this paper is to present a meth

odology for the analysis of the vulnerability of the

crisis cell and assess the performance of crisis man

agement at the municipal level.

The performance is defined as a weakness, ten

derness, defect or flaw in a defense system that

might endanger the integrity of this system and

what it protects, under the action of internal or

Quantitative approach of organizational resilience for a Dutch

emergency response safety region

J.M.P. van Trijp

Libertas in Vivo v.o.f., Utrecht, The Netherlands

M. Ulieru

University of New Brunswick, Fredericton, NB, Canada

P.H.A.J.M. van Gelder

Delft University of Technology, Delft, The Netherlands

ABSTRACT

Resilience is an important concept to determine

how well a Dutch Emergency Response Safety

Region behaves under stress. The main objective of

this study is to determine the intrinsic value “Resil

ience”. It is concluded that according to literature

the concept of “Resilience” can be best described by the generic approach “Operational Resilience” and is defined as: -The ability of an organization to prevent disruptions in the operational process from occurring; -When struck by a disruption, being able to quickly respond to and recover from a disruption in operational processes. The follow ing four items from literature are derived: Situa tion Awareness (awa); Management of Keystone Vulnerabilities (kv); Adaptive Capacity (ac) and Quality (q).

A large scale survey among safety stakeholders in The Netherlands was conducted where those items were explored. The function of Resilience on the defined items can be described as:

$$f(R_{ero}) = R_{ero}(R_{awa} + R_{kv} + R_{ac} + R_{q} + \varepsilon) \quad (1)$$

where R_{ero} = Resilience of Dutch Emergency Response Safety Region; R_{awa} = Resilience is a function of Awareness; R_{kv} = Resilience is a func tion of Keystone Vulnerabilities; R_{ac} = Resilience is a function of Adaptive Capacity; R_{q} = Resilience is a function of Quality; and ε = unspecified data and items which are also a function of Resilience. $f(R_{ero})$ may also be defined as Dynamic Operational Resil ience as it dynamically describes the actual state of

resilience of the organization.

Stolker (pp. 46, 2008) uses a Value Tree based on

the Multi-Attribute Utility Theory (MAUT) devel

oped by Goodwin & Wright (2004) to measure the

resilience index which may be considered similar

to the postulated Dynamic Operational Resilience

Security incidents and subsequent adaptations of disaster response

in complex humanitarian emergencies

B.I. Kruke

University of Stavanger, Stavanger, Norway

ABSTRACT

Humanitarian workers in complex emergency areas

face an increasing number of security challenges

in their daily operations. Mark Duffield (1994)

defines a complex emergency as “a major humani

tarian crisis of a multi casual nature that requires a

system wide response”. Russell R. Dynes calls this a

conflict disaster (2004). Thus, the lack of security in

complex emergencies may put humanitarian work

ers at risk, and thereby influence humanitarian

operations. Responses to security challenges vary

to a great extent from emergency to emergency,

and from agency to agency. The same is the case

with how agencies work to understand the security

situation in the emergency area. Where military forces invest a substantial part of their operations in assessing the current situation in the emergency area, humanitarian agencies do not have similar capacities.

This paper highlights four topics on security and humanitarian operations in complex emergency areas. Firstly, what is the trend on attacks on humanitarian workers? We learn from newspaper articles and reports from the field of security related incidents directed towards humanitarian workers. However, we need a more thorough understanding of the size of the problem and also of who are targeted. Secondly, how is security assessments and operational security decision-making conducted across the aid sector? Thirdly, are local organisations and people involved in security assessments? The locals normally have a good understanding of the situation in their neighbourhood. They may at the same time be in a very exposed position. Fourth, how do humanitarian agencies adapt their responses to the security situation in complex emergency areas?

The paper draws on some of the latest developments on security incidents and subsequent

humanitarian adaptations in disaster response.

The article also draws on experiences gained by the

author especially during fieldwork in South Darfur

in 2005, but also in Khartoum in 2007. The paper concludes that an increasing number of security incidents have a massive impact on humanitarian operations. The responsibilities to protect humanitarian workers, the humanitarian agencies security systems, and the tools on how to assess the security situation in conflict areas are in place. All the same, we have seen a trend of increased attacks on aid workers, and in particular on local staff and partners. Thus, humanitarian agencies must balance the humanitarian impact of their operations in conflict areas with the duty to take care of staff and partners. Stricter security regulations and remote management are humanitarian agencies' responses to incidents directed towards humanitarian workers. These approaches may be criticised for several reasons: 1) Increased involvement of local staff and partners pose an ethical dilemma because they are put at risk when international staffs are withdrawn; 2) A dynamic environment in conflict areas increases the need for field-level presence to assess the situation and to maintain an updated threat profile. The higher the organisational risk the higher the levels involved in the decision-making process. However, decision-makers at higher hierarchical levels need updated information from the field to conduct reliable decision-making. Thus, remote management and stricter security regulations may worsen the potential for risk assessments as foundations for reliable decision-making; 3) Relations with local actors and communities must be cultivated to obtain the consent and security guarantees of the various parties of the conflict. Thus it is a need to continue and to speed up a process of professionalization of humanitarian agencies on how to continuously assess and handle security threats at field level in complex emergency areas. Remote management and stricter security regulations may worsen the potential for risk assessments as foundations for reliable decision-making to adapt to the dynamic situation and needs at field level. This page intentionally left blank Decision making under risk This page intentionally left blank

A guidance for implementing decision-aiding in risk management

F. Beaudouin

EDF R&D, Chatou, France

M. Merad

INERIS, Verneuil-en-Halatte, France

ABSTRACT

The justification of decisions in risk management is of paramount importance. How to rank risky actions or making tradeoffs between conflicting objectives are typical questions? Addressing such questions entails stringent basis in order to gain confidence and acceptance from decision-makers or stakeholders. However, decision-aiding is often confused with and reduced to a problem of assess ment. The pivotal principle of “bounded ration ality” due to H. Simon helps to understand that decision-aiding cannot be reduced to a problem of optimization: a decision process encompasses indeed additional tasks that are often overlooked. The purpose of this paper is to establish a com plete canonical model that provides guidelines to the decision-analyst. It falls into five steps ranging from ‘stating and framing the problem’ to ‘working out a recommendation’. The kernel of the canoni cal model relies on two main tasks: ‘choosing the paradigm and building the model’ and ‘eliciting

subjective information', though often disregarded.

As far as risk management is concerned, the uncertainty that impacts consequences of actions raises the following difficulty: how to take into account the nature of assessments (i.e. in par ticular the property of scales) and process it in a consistent manner? It is up to the analyst to grasp properly the context and implement appropriate models to represent and elicit subjective informa tion (judgmental information, tradeoffs, attitude towards risks). This paper shows therefore that resorting to techniques from decision-aiding and economics of risk is here valuable.

Elements of guidance are based on the authors' experience as practitioners. They are exemplified through two full-scale cases experienced at EDF and INERIS. The first case consists in choosing investments of prevention facing uncertainty of outcomes and multiple conflicting objectives, for hydropower plants. According to Roy' taxonomy, it amounts to a ranking problem. This case inspired by the American School of Decision-Aiding is based on the multiattribute utility paradigm. It is

Dealing with uncertainties in long term investment planning of electricity distribution systems with distributed generation

M.D. Catrinu, M. Istad & D.E. Nordgård

SINTEF Energy Research, Trondheim, Norway

ABSTRACT

This paper discusses the uncertainties in electricity distribution system investment planning for integrating small-scale generation units (distributed generation- DG) in low and medium voltage electricity networks.

Traditionally, distributions systems where intended for unidirectional power flow to connect end-users and the main uncertainty in planning was related to electricity demand estimation (in terms of location, timing of new connections and load).

This situation has changed dramatically the last 15 years or so when the amount of renewable distributed generation increased tremendously due to countries commitments to cut greenhouse emissions by using all available renewable resources, including small scale energy generation potential.

This trend is expected to continue as the technologies for small scale renewable power production are advancing and becoming more affordable.

In Norway, the main part of DG are small scale hydro (from kW to 10 MW)—which are being

built by private actors owning the rights to a small river or waterfall suitable for installation of a DG unit. The DG-units will often be located in remote places with a relatively weak electricity grid, with low local load and long distances to the main grid. Distribution companies have through their network license an obligation to connect all distributed gen eration units to the network, assuming that certain requirements are fulfilled. Network reinforcements are often necessary to integrate the DG units with out compromising network power quality.

The presence of distributed generation changes the way distribution systems should be planned and built. With such a rapid increase in the number of distribution generation units being installed in some networks, planners need proactive and robust

Forming risk clusters in projects to improve coordination between risk owners

F. Marle & L.A. Vidal

Ecole Centrale Paris, France

ABSTRACT

Projects are facing an ever-growing complexity, with more and more interdependencies between its elements, and thus its risks. Since project risks have

increased in number and criticality, lists thus need to be broken down into smaller, more manageable clusters. Classical clustering techniques are gener ally based on a single parameter, like risk nature, criticality or ownership. Risk interactions are therefore not properly considered when building up clusters. That is why our objective is to group risks so that the interaction rate is maximal inside clusters and minimal outside. This will facilitate the communication and coordination between the actors who are committed in the management of the project and its risks.

In this paper, we propose to capture the poten tial interactions between project risks by a mix of expertise and experience. Then, we propose an algorithm based on the combined use of heuristics and optimization software in order to propose a configuration that maximizes the objective while respecting the constraints. Finally, we propose an application to a real project.

The first constraint of the optimization problem is the size of the cluster, that is to say the maximum number of risks inside a cluster. But, depending on the assignment of actors to risks, we may have for the same number of risks n between one and n dif

ferent risk owners, which does not have the same sense and the same implementation difficulty. This paper thus focuses on the addition of a constraint on the number of different owners inside each clus ter. It shows how the addition of this constraint enables to propose meaningful and operationally realistic clusters, regarding not only the interac tion rate between risks but also the relationships between risk owners. Indeed, it has to be noted that the clustering decision involves human group management, since the people behind the risks

On the use of value of information measure in decision making—A drilling jar case

J.T. Selvik

University of Stavanger and IRIS (International Research Institute of Stavanger), Norway

H.P. Lohne

IRIS (International Research Institute of Stavanger), Norway

T. Aven

University of Stavanger, Norway

ABSTRACT

A decision problem is considered in which it is questioned whether to collect some further infor mation prior to making the decision. The infor mation relates to aspects of cost, benefits and uncertainties. A common tool used for meeting this

challenge is the Value Of Information (VOI) meas

ure. This tool compares the costs of the acquisition

to the added expected utility (or expected monetary

value) produced by a specific improvement of the

decision basis. The purpose of the present paper is

to discuss the use of the VOI measure in a decision

making context. To what extent does this measure

provide an adequate decision making basis?

A case from the oil and gas industry, a drill

ing jar case is used to illustrate the discussion. The drilling jar case relates to possible reliability testing before making a decision on which jar to select for a tender. A standard VOI analysis is performed using a relatively simple model based on expected monetary values to assess the optimal jar alternative for this tender. The limitations of using the results for decision support are discussed, and an extended VOI decision process is suggested. The process highlights that uncertainty assessments should be conducted that see beyond the probabilistic analysis. The VOI results alone are not sufficiently informative to guide the decision maker on which jar to choose. However, placed in the wider process, also involving managerial review and judgements, the VOI measure may provide useful support to the decision making.

Performance-based fire safety—risk associated with different designs

H. Bjelland & O. Njå

University of Stavanger, Stavanger, Norway

ABSTRACT

Fire safety in buildings is based on long traditions

with prescriptive regulations and prescribed solu

tions. A prescribed solution is to be understood as

a building design concept that fulfills the minimum requirements in the building regulations. Such solutions are generally based on previous experience with fires and building traditions. After major fires, measures were introduced into the regulations to prevent the experienced consequences in future fires, i.e. a reactive regulation approach. However, during the last decades a performance-based regulation approach has been introduced in many countries, including Norway. This approach makes it possible to justify alternative designs, if it can be verified that the safety level is in accordance with the functional requirements in the regulation (Meacham 1996). Prescribed, or pre-accepted, solutions still exists as an alternative to the performance-based approach. Thus, pre accepted solutions often constitute a definition of what is safe enough. The design practice of today is heavily influenced by comparisons with pre accepted solutions in efforts to qualify designs. If the safety level of the alternative design is equivalent or higher than the pre-accepted solution, the design is considered to comply with the regulation (IRCC 2010).

Looking at the different editions of the Norwe

gian regulations from early 20th century, we find that the means of egress has been the major remedy when providing fire safety in multi-storey residen tial buildings. While the residential building and apartments have remained quite the same, there have been a number of different escape staircase concepts (Bjelland 2009). A fundamental question in this paper is whether this focus on staircases could be justified, if the goal is to reduce risk to the occupant’s lives?

In the paper we examine fire safety designs based

Sequential optimization of oil production under uncertainty

Arne B. Huseby & Nikita Moratchevski
University of Oslo, Norway

ABSTRACT

Optimization is an important element in the management of multiple-field oil and gas assets, since many investment decisions are irreversible and finance is committed for the long term. Recent studies of production optimization include (Horne, 2002) and (Neiro & Pinto, 2004).

(Huseby & Haavardsson, 2009) considered the problem of production optimization in an oil or gas field consisting of many reservoirs sharing the same processing facility. In order to satisfy

the processing limitations of the facility, the pro
duction needs to be choked. Thus, at any given
point of time the production from each of the
reservoirs are scaled down so that the total pro
duction does not exceed the processing capacity.
(Huseby & Haavardsson, 2009) developed a gen
eral framework for optimizing production strate
gies. In (Huseby & Haavardsson, 2010) this work
was extended to cases where the production is
uncertain.

In the present paper we consider a new variant
of this problem where the oil production from a
given single reservoir is described relative to a
sequence of time periods. In each time period the
production is limited by two factors: the potential
production volume and the amount of oil that can
be processed at the processing facility. At the start
of each period one needs to book a certain process
ing quota. This quota has a cost which is propor
tional to the size of the quota. At the same time the
production generates an income proportional to
the processed volume. If the quota is greater than
the potential production volume, one ends up with
paying too much for the quota. On the other hand,
if the quota is less than the potential production

Shared collaboration surfaces used to support adequate team decision processes in an integrated operations setting

M. Kaarstad & G. Rindahl

Institute for Energy Technology, Halden, Norway

ABSTRACT

The petroleum industry is undergoing a transition made possible by new and powerful information technology. Traditional work processes and organizational structures are challenged by more efficient and integrated approaches to offshore operations. Several companies on the Norwegian continental shelf have implemented integrated operations (IO) as a strategic tool to achieve safe, reliable and efficient operations (Ringstad & Andersen, 2007). In integrated operations, traditional work processes and organizational structures are challenged by more efficient and integrated approaches to offshore operations. The new approaches make it possible to reduce the impact of traditional obstacles, e.g., geographical, organizational or professional, to efficient decision-making (Ringstad & Andersen, 2007).

Integrated operations are both a technological and an organizational issue, and imply both the use of new technology and new work processes.

The IO technology consists of high-quality video conferencing, shared workspaces and data sharing facilities and involve people in discussions both onshore and offshore. The shared workspaces include so-called collaboration rooms (operation rooms) for rapid responses and decision-making. In an operational context, a number of deci sions are required, the decisions are interdepend ent, the environment changes, both autonomously and as a consequence of the actions taken by the decision maker; and the decisions are made in real time. Because the successful performance of many important tasks requires skillful decision making, the identification of forms of decision support for dynamic decision-making has become a research priority. However, this identification process has proven to be very challenging (Lerch & Harter, 2001).

Personnel working in an IO setting will often benefit from decision support in different situ

Visualization and verification of dependable work processes for stakeholder-driven organizations

Atoosa P.-J. Thunem & Harald P.- J. Thunem
Institute for Energy Technology, Halden, Norway

ABSTRACT

Although some industries still seem to distinguish between the terms “workflow” and “business proc ess” when speaking about their value chain, it is almost impossible to justify any fundamental differ ence between a work process and a business process. When thinking about business processes in today’s organizations, they have in fact no meaning if they each do not encompass work states and transitions as well as their prerequisites, all represented by vari ous technological, human and organizational prop erties of a work process. Individually and jointly, these work processes add value to the products and services “passing through” the processes and offered to all stakeholders (including the employ ees and customers). In reality, each work process is associated with a certain value-adding business sub-goal, which is usually the responsibility of a functional (operational) unit or department.
How the values are defined and thus measured is of course different from one enterprise to another, depending on, among others, the types of stake holders, certain legislations and regulations the enterprise needs to relate to, and cultural factors of the enterprise itself. Therefore, the values also play a significant role in how the sub-goals and

therefore work processes achieving each of them

are defined, managed and categorized. That is why

some organizations consider all their sub-goals as

equally value-adding (towards the overall goal and

mission of the organization), and therefore place

the associated work processes as a part of the value

chain, while other organizations operate with two

groups of sub-goals, where the primary group is

understood to form the organization’s value chain.

Consequently, only specific, “primary” work proc

esses are placed there. The others are considered as

supporting, “secondary” work processes across the

mutually parallel primary work processes. In such

organizations, the “secondary” work processes add

value to the products and services by influencing

the primary work processes.

A major problem related to design and change of

work processes in implementation and management

A comparison of scenario binning methods for dynamic probabilistic

risk assessment

K. Metzroth, D. Mandelli, A. Yilmaz, R. Denning & T. Aldemir

The Ohio State University, Columbus, OH, US

ABSTRACT

Dynamic Event Tree (DET) analysis is an effective

approach for evaluating plant response during the course of a transient in the presence of modeling or stochastic uncertainties. In addition, it can account for the time or process history dependencies of these uncertainties in a physically consistent way by tracking all generated scenarios using the same simulation tool. DET analysis produces very large output datasets, and one of the biggest challenges in DET analysis is the management and interpreta tion of the very large amount of data that is gener ated. A possible approach to analyze DET output data is to place scenarios into groups based on similar characteristics to enable the analyst to bet ter conceptualize the meaning of the results and to reduce the effort required in subsequent stages of the analysis (Mandelli, 2010). However, the question remains as to what scenario characteristics should be used to define “similarity”. In classical Level 1 PRA (as outlined in NUREG-1150 (U.S.N.R.C., 1990)) scenarios were grouped mostly accord ing to the states of various active plant systems. Applying such a method directly to DET analysis may not be appropriate since the scenario group ings considered in NUREG-1150 for Level 1 PRA are time-independent and it is possible that the

timing of system actuation, failure, or recovery could have a significant impact on the scenario outcome. Hence, it is possible that scenarios with similar active component states have quite different consequences. In addition, DET analysis produces a wealth of data which can be utilized to group scenarios in different ways (e.g. based on actual plant physical variables rather than on inferring the plant physical state based on active component states), depending of the objectives of the analysis. The Mean-Shift-Methodology (MSM) (Mandelli, 2010) is proposed as a means to group DET scenarios based on their physical character

A dynamic Level 2 PRA using ADAPT-MELCOR

D.M. Osborn, D. Mandelli, K. Metzroth, T. Aldemir, R. Denning & U. Catalyurek

Nuclear Engineering Program, The Ohio State University, Columbus, OH, US

ABSTRACT

The current approach to Level 2 Probabilistic risk assessment (PRA) using the conventional event-tree/fault-tree methodology requires pre specification of event order occurrence which may vary significantly in the presence of uncertainties. Manual preparation of input data to evaluate the possible scenarios arising from these

uncertainties may also lead to errors from faulty/ incomplete input preparation and their execution using serial runs may lead to computational chal lenges. A methodology has been developed for Level 2 analysis using dynamic event trees (DETs) that removes these limitations with systematic and mechanized methodology as implemented using the Analysis of Dynamic Accident Progression Trees (ADAPT) software (Catalyurek et al., 2010; Hakobyan et al., 2008).

This paper discusses the work which has been conducted for a Level 2 PRA Station Black out Scenario using a dynamic event tree analysis for a series of MELCOR input decks contain ing a 3-loop PWR with a steam supply system and a sub-atmospheric dry containment. This work is an extension of past ADAPT-MELCOR dynamic PRA experiments (Hakobyan et al., 2008; Hakobyan et al., 2006a, b) in which additional parameters are considered. Creep rupture distribu tions for Carbon Steel (CS), Stainless Steel (SS), and Inconel (IS) are considered not only for the

Photogrammetric Computer Vision Laboratory, The Ohio State University, OH, US

T. Aldemir

Department of Nuclear Engineering, The Ohio State University, OH, US

ABSTRACT

While the traditional Event-Tree/Fault-Tree (ET/FT) approach is still the most popular approach for Probabilistic Safety Assessment (PSA), difficulties arise in the PSA modeling of systems with significant hardware/process/software/firmware/human interactions. Also, it is not clear how passive system behavior can be modeled with the ET/FT approach. Such difficulties may be overcome with the use of Dynamic Event Trees (DETs). A challenge with DETs for realistic systems is computational requirements. Thousand of scenarios may need to be simulated following a single initiating event which leads to long runtimes, high computational complexity of analysis and interpretation of the produced scenarios. However, not all of the scenarios may carry the same significance. In fact, experience shows that a high percentage of the scenarios exhibits normal transient behavior (i.e., does not lead to a situation that has to be avoided) and follow similar evolution pathways. These scenarios

can be assigned lower priority, delayed or even discontinued during simulations, allowing more efficient utilization of computing resources. In this paper, we propose a probabilistic approach for classification of each scenario in a DET as non failure or failure using Hidden Markov Models (HMMs). To address the problems stated above, the classification must be performed online, using only the part of the scenario that is available so far, while its execution still continues.

HMMs have been widely used in a large variety of applications, including manipulations of large sequences of data obtained over a period of time (MacDonald & Zucchini 2009). The main com ponents of a HMM are the unknown or hidden states and the observations generated depending on these states. The transitions from one state to another are controlled by transition probabilities,

Application of the dynamic hazop to an air separation distillation column

J.S.G.C. Matos

White Martins Gases Industriais Ltda. (Praxair Inc.), Rio de Janeiro, RJ, Brazil

P.F. Frutuoso e Melo

COPPE/UFRJ-Programa de Engenharia Nuclear, Rio de Janeiro, RJ, Brazil

M. Nele

Escola de Química/UFRJ, Rio de Janeiro, RJ, Brazil

ABSTRACT

The development of the chemical industry has required larger industries, capable of producing more products in a shorter period of time. To accomplish this goal, chemical process industries became more complex, bringing more hazards to plant operation (e.g.: higher temperatures and pressures). This lead to higher requirements from regulatory agencies and more detailed hazard anal ysis techniques development.

This work covers the use of dynamic simulation with process hazard analysis (dynamic HazOp) which provides more accurate and trustful informa tion than traditional HazOp, which is a qualitative analysis. This methodology used allows the evalu ation of a deviation occurrence, deviation conse quences magnitude, time needed for the worst case scenarios to be reached, and actions that should be taken in order to avoid or mitigate the occurrence of the deviation.

For our study case, the lower column of an air separation plant was used. The deviations applied were pressure increase of one inlet stream, external

temperature increase (simulating a fire), addition of hydrocarbons to the inlet stream (simulating severe atmospheric pollution) and the increase of the inlet streams temperature. Dynamic profiles showing the variations from the normal operating values of the process variables were calculated to check the impacts of the deviations applied to the system.

The simulations performed are supposed to show not only process safety impacts but also the possibility of performing dynamic simulations associated with the traditional HazOp in order to confirm the results in the analysis. Therefore, the consequences with operation impact were also important for this study.

The results showed the need of checking whether safety relief devices of the system analyzed were capable of relieving the maximum pressure indi

Capability of the MCDET method in the field of dynamic PSA

M. Kloos

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH, Germany

1 INTRODUCTION

Motivations for the development of the MCDET method were the deficiencies of the classical PSA approach in modeling complex accident scenarios

and the hardly quantifiable uncertainty on its results due to the uncertainty on the concept or completeness of the applied simplified models. The question is, how realistic are probabilistic safety/risk assessments derived from the simplified—mostly static—PSA models?

The accident scenarios to be considered in a PSA are characterized by complex interactions over time between the technical system, the physical-chemical process and operator actions. Due to stochastic influencesa variety of potential event sequences has to be considered, and the assessment of the consequences of an accident scenario can only be probabilistic. It is obvious, that the spectrum of event sequences may be tremendous, if there are aleatory uncertainties in the physical-chemical process (e.g., pressure release rates, coolant or feed-water injections rates, etc.) or in the timing of system function failures and of human actions. Only if a PSA is able to account for all the sequences which may evolve and to rank the sequences according to their likelihood, it can provide a well-founded probabilistic assessment.

The MCDET method developed at the GRS allows for an integral probabilistic modeling of acci

dent scenarios along the time axis. It provides prob

abilistic assessments for accident sequences which

adequately account for the spectrum of sequences

which may actually evolve. The combination of

Monte Carlo (MC) simulation and the Discrete

Dynamic Event Tree (DDET) approach as real

ized in MCDET is capable of accounting for any

aleatory uncertainty at any time without need of

significant simplifications.

The implemented MCDET module system

can in principal be coupled with any determin

istic dynamic code simulating the behavior of

a nuclear power plant. Beside aleatory uncer

tainties, MCDET can also consider epistemic uncertainties which determine how precise probabilistic assessments can only be provided due to the knowledge uncertainties involved in the calculation. Methods were developed to reduce the computational effort of epistemic uncertainty evaluations in the framework of MCDET analyses. The MCDET module system was supplemented by an extra crew module which enables calculating the dynamics of operator actions depending and acting on the plant dynamics as modeled in a deterministic code and on stochastic influences as considered in the MCDET modules. The crew module allows for running situation-dependent sequences of human actions as they are expected for a dominant mental state and cognitive behavior. The combination of the MCDET and crew modules with an appropriate deterministic code allows for evaluating complex accident scenarios where human actions, technical installations, the physical-chemical process and stochastic influences are the main interacting parts in the course of time. A scheduler program arranges the corresponding calculations (Fig. 1). The capacity of the MCDET and crew modules has been demonstrated by several applications. Two large scale applications are described in the paper. An overview on the MCDET method and the

implemented modules is given as well. Figure 1. A scheduler program arranges the calculations of the MCDET modules, the crew module and a dynamic code.

Development of a simulator independent cognitive human reliability model for nuclear accident conditions

R. Sundaramurthi & C. Smidts

The Ohio State University, Columbus, OH, US

ABSTRACT

This paper describes a simulator independent human reliability model that can be applied to the probabilistic assessment of any nuclear power plant accident. Unlike mechanical systems where reliability has been quantified and the systems designed to high reliability standards, it is difficult to measure the degree of reliability of an operator. It has been documented that Human Error Probability (HEP) can be as high as 0.5 for certain tasks (Swain, 1983) and that uncertainty margins are significant. As such, human behavior is one of the primary contributors to uncertainty in risk assessment and requires high fidelity modeling. High fidelity modeling is obtained by carefully replicating the operating conditions as they unfold, as well as by modeling the various internal decision making and situation assessment processes that take place during an accident. This can only be achieved

by the combination of a dynamic reliability mod

eling environment, powerful and high fidelity proc

ess simulation and cognitive operator models. The

model discussed in this paper is a derivative of

IDA (Smidts, Shen & Mosleh 1996), which models

the operator behavior by considering its cognitive

aspect through the three modules of information,

decision making and action. Four models/modules

are designed which along with the interface facili

tating the interactions between them constitute the

HRA model (IDA-SI) (Fig. 1). The components

I n

f o

r m

a t

i o

n PS/DM KB PSF WM Mental Model Memory Model Actions

Figure 1. IDA-SI Overview of Modules and their

interactions.

Dynamic reliability and uncertainty analysis of severe accident

with randomly delayed events

R. Alzbutas

Lietuvos energetikos institutas, Lithuania

Kauno technologijos universitetas, Lithuania

P.E. Labeau

Université Libre de Bruxelles, Belgium

ABSTRACT

The Stimulus-Driven Theory of Probabilistic Dynamics (SDTPD) and its simplified version the Theory of Stimulated Dynamics (TSD) have been introduced for the analytical modeling and the simulation of hybrid (continuous-discrete) systems as well as for dynamic reliability considerations. The main reason for TSD was to keep alive the concept of countable sequences that is at the heart of the classical safety assessment approach, keeping at the same time the level of SDTPD complexity tractable. The described theory deals with the concepts of stimulus and delay in event sequence delineation, and their implementation.

In addition, the focus is set on the simulation and analysis of systems with delayed events. Because stimuli activation and random delays condition the event occurrences, the history of stimuli activations during the accident transients does matter in calculating the frequencies of events. Thus, an extension of the Markovian process accounting for these features is considered.

An approach of non-Markovian simulation

and uncertainty analysis is discussed in order to simulate complex dynamic systems and to adapt SDTPD for practical applications, mostly in the context of dynamic reliability analysis. This devel oped approach and related methods for uncer tainty analysis have been used as a basis for test case simulation in the perspective of its applica tions for severe accident scenario analysis. Various formal definitions and a methodology of how to assess uncertain parameters' influence on the estimation of results are considered before the test case. For the analysis of the dynamic results' sensitivity to the uncertain model parameters, the uncertainty analysis is integrated within TSD. It is also introduced as a possible way for analysis of TSD-based simulation results and demonstration

Labeau, P.E. et al. Dynamic Reliability: Towards an Integrated Platform for Probabilistic Risk Assess ment, Reliability Engineering and System Safety 68, pp. 219–254 (2000).

Labeau, P.E. & Izquierdo, J.M. Modeling PSA Prob lems-I: The Stimulus-Driven Theory of Probabilistic Dynamics, Nuclear Science and Engineering 150, pp. 1–25 (2005). Raimond, E. & Durin, T. Comparison between classical and dynamic reliability approaches. Specification and results of a benchmark exercise, European Review Meeting on Severe Accident Research

(ERMSAR), Forschungszen-trum Karlsruhe GmbH (2007).

Lazy forward-chaining methods for probabilistic model-checking

Florent Teichteil-Königsbuch, Guillaume Infantes & Christel Seguin

ONERA—The French Aerospace Lab—Toulouse, France

Model-checking of probabilistic discrete-event systems is a thriving research area with still impor tant theoretical issues and a growing interest from industries. Exact methods used in state-of-the-art model-checkers like PRISM or MRMC do not scale very well and are still not relevant for large industrial systems. On the other hand, simulation based methods like stochastic comparison or the APMC model-checker scale better, but only pro vide statistical and approximate results, that are not well-suited to critical systems where quantitative properties must be proved without approximation.

This paper targets a new algorithmic framework inspired by recent advances in probabilistic auto mated decision-making, that allows to validate without numeric approximation quantitative prop erties of large discrete-time systems defined in for mal languages such as PRISM and AltaRica.

Our algorithm constructs an incremental graph of reachable states from a known initial state. Since

PCTL properties boil down to validate until for

mulas f u f p t T 1 2α (f 1 is true until f 2 is true
within T

time steps, with probability higher than α), we stop

the construction of a path in the graph when either

f 1 becomes false, or t becomes equal to zero, or f 2

becomes true. The transitions of the graph are gen

erated on-the-fly when necessary from the high

level language description. An important feature

of our algorithm is the lazy discovery of reachable

strongly connected components (SCCs) of the graph, i.e. the sets of states that are bilaterally connected, using the framework of Tarjan's depth-first search algorithm for any oriented graph. Starting from a given initial state, this algorithm explores the graph of reachable states by expanding paths until absorbing states or loops are reached, then it goes up these paths to identify on-the-fly each SCC once. The main advantage of identifying SCCs is that the probability of the formula f t T 1 2 f u can be computed locally inside each SCC. Moreover, as SCCs are discovered one after the other in a backward manner when going up paths, the latter formulas are computed only once and guaranteed to be exact. The local computation of until formulas can be performed with state-of-the-art computation schemes used in PRISM or MRMC (in these model-checkers, validation of quantitative properties relies on sparse data structures defined over all states of the model, but not over local states). In this paper, we present our algorithm for exactly validating PTCTL formula using on-the-fly SCCs discovery and local computations. We highlight the key ideas of this algorithm on examples from embedded aeronautical avionics systems, modeled in PRISM and AltaRica. We also show preliminary results compared with other stateof-the-art probabilistic model-checkers such as PRISM and MRMC.

Reliability assessment for complex systems operating in dynamic

environment

G. Babykina, N. Brinzei & J.-F. Aubry

CRAN, UMR 7039, Nancy-Université, CNRS.
Vandoeuvre-les-Nancy, France

G.A. Pérez Castañeda

Instituto Tecnológico de Tehuacán. Tehuacán, Puebla, Mexico

ABSTRACT

The paper aims to study a complex repairable system, operating in a dynamic environment. The reliability of the system is assessed by means of statistical modeling. We consider a system with several redundant components. The system oper ates in different modes defined on one hand by discrete states of its components (active/passive, failure/normal operation) and on the other hand by the operational environment conditions. These conditions are defined by continuous physical phe nomena. The system's failure is conditioned by a certain combination of its components failures. The dynamic operational environment, the differ ent discrete modes of system's operation and the deterministic and/or stochastic transitions between these modes are simultaneously accounted for by means of the Stochastic Hybrid Automaton (SHA). The SHA model contains the possible states of the system and the events which govern the transitions between these states. Some transitions occur when

the components fail according to a random fail

ure rate (stochastic transitions). Other transitions

can be governed by the deterministic behavior of

the physical phenomenon defining the operational

environment of the system. The objective in this

context is to estimate the global system's failure

rate. Monte Carlo simulations are carried out to

generate a long trajectory followed by the system.

The system's failure behavior is then modeled using

Using dynamic Bayesian networks to solve a dynamic reliability problem

Perrine Broy

Université de technologie de Troyes & CNRS, Troyes, France

EDF R&D, Département Management des Risques Industriels, Clamart, France

Hassane Chraibi & Roland Donat

EDF R&D, Département Management des Risques Industriels, Clamart, France

ABSTRACT

In probability risk assessment, evaluation of

system reliability tries to be more and more precise.

To that end, physical phenomena affecting the

systems should be taken into account. Such sys

tems are called hybrid systems and are often ref

erenced in the literature as a part of the dynamic

reliability framework.

The evolution of hybrid systems is a combina
tion between discrete stochastic events on the one
hand and continuous or transitional deterministic
phenomena on the other hand.
Mathematically, hybrid systems are generally
represented by Piecewise Deterministic Markov
Processes (PDMP). A PDMP (Davis 1984) is a
pair consisting of a random vector in a finite state
space and a deterministic vector in a continuous
state space. The random vector describes the con
figuration of the system and the deterministic vec
tor characterizes some environmental variables.
The evolution of these variables is governed by dif
ferential equations that depend on the configura
tion in which the system stands.
There are some methods which are supplied with
tools dedicated to describe and quantify PDMP.
Each method has its advantages and disadvan
tages, depending on the criteria such as readability,
flexibility or time of calculation.
In an industrial context, it is essential to get a
representation of the system both readable and
trusty. Furthermore, an elaborated mathematical
background and existing software tools should
lead to limit simplifying assumptions and decrease

the computation time. Thus a challenge is to judi

A comparison of distribution estimators used to determine

a degradation decision threshold for very low first order error

O. Hmad & A. Mathevet

Safran Engineering Services, Etablissement de Villaroche, France

P. Beauseroy & E. Grall-Maës

Institut Charles Delaunay UMR STMR (6279), Université de Technologie de Troyes, France

J.R. Masse

Safran Snecma, Etablissement de Villaroche, France

ABSTRACT

Before introducing a monitoring algorithm in an

operational system, it is important to assess very

carefully its performances. The performance esti

mation of the algorithm requires the tuning of a

decision threshold based on its abnormality deci

sion criterion for very low first order error. In this

paper a detection process for deciding between

correct and incorrect behavior of the start system

is considered. The first order error (Pfa) of the

detector required by the companies is about 10E-9,

which is very low. Thus the decision threshold has

to be properly determined in order to satisfy this

requirement. The value of this threshold depends

only on the distribution of the abnormality deci

sion criterion Y under the hypothesis of no degra
dation. The distribution law of Y is not known and
the searched threshold has to be determined using
some limited data set.

The approach we use consists in determining the
threshold using an estimation of the abnormality
decision criterion distribution. Three methods to
estimate this distribution are compared. Firstly,
a Gamma distribution model has been considered
because the distribution of Y should be approxi
mately a Gamma distribution. Secondly non
parametric probability density estimator has been
considered. A Parzen window estimator has been
used. Thirdly we considered the Johnson trans
formation which is used to convert non normal
random variable to obtain a new one which distri
bution is normal.

This communication presents a comparison of
these three methods according to threshold estima
tion for very low first order error and concludes
about the robustness of Johnson transformation
for this problem. Two cases were studied: one
when the abnormality decision criterion follows

Johnson, N.L. (1949). “Systems of frequency curves
generated by methods of translation”. Biometrika 36,

149-176.

Parzen, E. (1962). “On estimation of a probability den

sity function and mode”. Annals of Mathematical

Statistics 33, 1065-1076.

Shapiro, S.S. & Wilk, M.B. (1965). “An analysis of vari

ance test for normality”. Technometrics 14, 355-370.
Silverman, B.W. (1986). “Density Estimation for Statistics and Data Analysis”. Chapman and Hall: London. Slifkerm J.F. & Shapiro, S.S. (1980). “The Johnson System: Selection and Parameter Estimation”. Technometrics 22(2), 239-246.

A first step toward a model driven diagnosis algorithm design

methodology

J.-M. Flaus, O. Adrot & Q.D. Ngo

Laboratory G-Scop, Grenoble, France

ABSTRACT

Large-scale complex process plants are safety

critical systems where the real-time diagnosis is

of great importance. In a model based systems

engineering approach, the structured development

process from the concept to the production to the

operation phase is organized around a coherent

model of the system. This model contains in par

ticular mathematical relations about the behaviour

of the system that could have been used for simula

tion in the design phase.

The objective of this work is to use this infor

mation to design automatically an online diagnosis algorithm.

In order to detect abnormal behaviour, model based algorithm compares the observed behaviour to the expected behaviour. To do this, Analyti cal Redundancy Relation (ARR), must be build.

An Analytical Redundancy Relation (ARR) is a constraint deduced from the system model which contains only observed variables, and which can therefore be evaluated from any observations set to check if observed and expected behaviours are consistent.

The approach allows:

- To extract the valid relations about behaviour for a working mode of the system.
- To build, using symbolic analysis graph path search, analytical redundancy relation for the various system configurations.
- To evaluate this ARR in using set valued compu tations (interval arithmetic) to take into account model and measurements uncertainties.

The model of the system is given as a set of model blocks, which define variables, relation between these variables, input/ouput visibility of these variables and connections between variables

of different blocks. Such a model definition is used with some syntax variations in numerous simula tion tools such as Modelica, Matlab, SysML or

A generic adaptive prognostic function for heterogeneous multi-component systems: Application to helicopters

P. Ribot & E. Bensana

Onera—The French Aerospace Lab, Toulouse, France

ABSTRACT

Maintenance efficiency of industrial systems is an important economical and business issue. It is a way to improve reliability and safety while reduc ing the final cost of systems. The Helimaintenance project aims at optimizing the maintenance of civil helicopters. The objective is to develop an integrated logistics system in order to support the scheduling of maintenance actions and reduce the unavailability of helicopters. Maintenance actions must be decided on an efficient and com plete analysis of the health of the system when it is operating. An embedded supervision system is in charge of monitoring the helicopter and detecting problems and misbehaviors which require mainte nance actions. The supervision system integrates a diagnostic function to accurately determine which components may cause a system failure and have

to be replaced by a maintenance action. In order to optimize the maintenance cost, it is also necessary to perform preventive maintenance by deciding to perform actions on the system before the problems actually occur. To reach this objective, a prognostic reasoning must be performed over the system to establish whether a preventive action is pertinent at a given time. A data processing system integrating a prognostic function receives information from the supervision system (embedded sensors, pilot observations, diagnostic result) and suggests component replacements before they fail. For this purpose, the prognostic function has to compute a fault probability for each component and evaluate their Remaining Useful Life (RUL for short). Classical reliability methods can be used to compute the RUL of components but they do not take into account the real stress of the supervised system when it is operating. A stress can result from a fault within the system or an abnormal solicitation (like mechanical vibrations, thermal impacts, pressure, etc.) that may affect the system RUL. An adaptive prognostic function is then required to take into account the current condition of the system that is evaluated by the diagnostic function and by monitoring environmental conditions. Aeronautical systems, like helicopters, are complex systems built from an

assemblage of heterogeneous components (mechanical, hydraulic, electric or software, etc.). In this paper, a formal generic modeling framework is presented for a heterogeneous multi-component system. Available knowledge about each component is represented in an abstracted but homogeneous way with a set of parameters, a set of ranges for parameters and a set of relations describing the component behaviors. The component description is refined by introducing a structural model and a functional model. Some operational modes are then defined for components according to the functional state of the system. In order to evaluate the RUL of components, the prognostic function has to predict the occurrence of each possible fault that may occur on the system components. The proposed prognostic methodology uses reliability analyses and physicsbased models in order to compute fault probabilities of components. Due to its flexibility, the parametrized Weibull model is used to represent a fault probability density function. The Weibull characteristics depends on component solicitations that are modeled as component parameters. The parameter values are either monitored by sensors or estimated from current diagnosis and allow to model the component degradation. The first component that is predicted to fail may cause some abnormal solicitations on components it interacts with. The prognostic function has to take the fault propagation in the system into account by predicting abnormal solicitations caused by future faults that may accelerate the component degradation. These fault probabilities of components have to be updated according to new parameters values resulting from sensors or estimated from on-line diagnosis. For illustration, the proposed prognostic function is finally applied to an example of a helicopter transmission system.

Advanced text mining algorithms for aerospace anomaly identification

Z. Bluvband & S. Porotsky

A.L.D, Tel-Aviv, Israel

ABSTRACT

The paper describes an advanced text categoriza

tion procedure developed and successfully used

in aerospace industry, especially for safety assess

ment, analysis and improvement. Typically, failure reports are human-written records, usually just free text written by professional people. Therefore understanding and treatment of this statistical documentation is vital for Safety and Reliability measurement and improvement. The purpose of presented paper is the computerized analysis and interpretation of human reported free-text aviation safety records, in order to automatically “read”, discover and treat anomalies occurred in the field. The methodology and algorithms were verified on actual, significant and appropriate Safety and Reli ability data bases including the ASRS (Aviation Safety Reporting System) data base (http://asrs. arc.nasa.gov/index.html) containing millions of unprocessed safety events reports. One of the most important applications and goals of the research is to assign new in-coming reports to one or more from the several of predefined categories on the basis of their textual content.

Examples of anomalies, extracted from ASRS (Aviation Safety Reporting System) data base (http://asrs.arc.nasa.gov/index.html), are “817: Ground Incursion—Landing without Clear ance” (occurs in 2% of the reports), “856: In

flight Encounter—Turbulence” (occurs in 3% of the reports), “860: In-flight Encounter—VFR in IMC” (occurs in 1% of the reports), etc.

Optimal categorization functions can be constructed from labeled training examples (i.e., after human expertise) by means of super vised learning algorithm and cross-validation.

Numerous methods for text categorization have been developed lately: Neural Networks, Naive Bayes, AdaBoost, Linear Discriminant Analysis, Logistic Regression, Support Vector Machines (SVM), etc. SVM has become a popular learn ing algorithm, used in particular for large, high dimensional classification problems; it has been shown to give most accurate classification results in a variety of applications. However the Direct application of these methods to Aerospace Anomaly Discovery is restricted for the following reasons: a. fully automatic procedure can support only middle values of output parameters Recall and Precision, 50–75%; b. safety report statistical parameters are absent, i.e., the frequency of words in a report has been changing on a “year to year” basis. The method suggested in the paper is based on SVM binary classification approach intended to perform a multi-label categorization, but practically performing several times the binary one of type OneVersus-Rest (according to the amount of anomalies). In the standard SVM method, the optimal separating function is reduced to a linear combination of kernels on the training data with training feature vectors X and corresponding labels y. If $y(X) \geq 0$, the non-marked document X is recognized as “Positive” for current category

(anomaly), otherwise as “Negative”. To support high values of output criteria (e.g., both Recall and Precision have to be simultaneously more than 90 … 95%) and non-stability of the report statistics, we propose the mixed, partially automated approach for the selection of most of anomalies automatically, by means of text categorization algorithm, with occasional usage of human expertise. The following additional metaparameters are introduced: • G low —Low boundary for separating function; • G high —High boundary for separating function. The proposed Text Categorization algorithm is performed as following: If y(X) ≥ G high , the non-marked document X is recognized as “current category” and expert should not verify this solution; If y(X) ≤ G low , the non-marked document X isn’t recognized as “current category” and expert should not verify this solution; If Glow < y(X) < G high , the expert should manually verify this document for current category. Some numerical results, based on ASRS On-Line Data Base, are considered. In order to support values of Recall = 0.9 and Precision = 0.95 for anomaly “860: In-flight Encounter—VFR in IMC” it is necessary to perform an expert verification of 910 reports from the total amount of 10,000. Thus we are able to achieve significant acceleration of expert work (reduction of report amount, verified by expert after automatic text categorization)—11 times less reports to review.

ANN based Bayesian hierarchical model for crack detection

and localization over helicopter fuselage panels

C. Sbarufatti, A. Manes & M. Giglio

Politecnico di Milano, Milano, Italy

ABSTRACT

If from one hand the aerospace industry is trying

to extend the duration of life-limited components,

from the other hand a deep control is necessary

over the structures to guarantee both the machine

availability and reliability. In effect, thanks to the

advance in the evaluation of the actual structural

health by means of a Structural Health Monitor

ing (SHM) system, it could be possible to set a Condition Based Maintenance (CBM). Inside this frame, the key factor is the disposal of detection and monitoring systems as reliable as possible in order to conjugate safety with economics objec tive. The first step for developing such advanced technology would be the disposal of a robust dam age detection system, able to recognise, locate and quantify the damage in a certain component.

The work described hereafter is a simulation of crack detection and localization problem over a typical aerospace structure, consisting of a riv eted aluminium skin, stiffened with some reinforc ing elements, as the one experimentally tested by Giglio (2008) for damage tolerant material charac terization purposes. The combined use of Bayesian Hierarchical Models (BHM) and Artificial Neural Networks (ANN) is proposed. As a matter of fact, the enormous resemblance between hierarchical models and distributed detection problems makes the former applicable to problems where param eters and/or observations interact (in the form of conditional probability) through a certain hierar chical structure. In addition, Finite Element (FE) numerical Models for damage inside the struc

ture (Figure 1) could be used to train algorithms, as reported in detail by Katsikeros (2009). Basic system knowledge would result, upon which to introduce the variability by means of real sensor network data, coming from similar structures stud ied by Sbarufatti (2010), in order to consider the problem from a statistical point of view. The ANN could then be used as a level of the BHM presented by Chen (2002), thus reformulating the decision problem using hierarchical models and perform

Contribution to specific determination of system state and condition

D. Valis

University of Defence, Brno, Czech Republic

L. Zak

Brno University of Technology, Brno, Czech Republic

ABSTRACT

Nowadays system requirements are set up and evaluated in various manners. When determining an item technical state, there are many options available. However, in order to specify the state and the condition of a system, we choose one off line approach. The paper deals with mathemati cal processing, monitoring and analysing oil field data. Such data comes from the laser spectrogra

phy within tribodiagnostic oil tests. When analys ing oil data, we apply mathematical methods based on the analyses and calculations of time series. It is expected to get the results which will help to improve maintenance policy, life cycle costing and operations. Due to the fact that the data sample has been classified as fuzzy and uncertain, the FIS (Fuzzy Inference System) is used.

The growing dependability and operation safety requirements of modern equipment along with the increasing complexity and the continuous reduc tion of the expenses of operation and maintenance might be satisfied among others by the consistent use of modern diagnostic systems. Present systems can be equipped with signal processors related to board computers and intelligent sensors which are the source of the primary information on a tech nical state in real time. The main task of object technical state diagnostics is to find out incurred failures, and also prevent from failure occurrence while detecting and localizing changes in an object structure.

The paper is going to deal mainly with the anal ysis of tribotechnical system outcomes (TTS— friction in it, wear and lubrication). Regarding the

tribotechnical system, the basic information on

tribological process, operating and loss variables is

provided. Tribology is the science and the technol

ogies of interacting surfaces in a relative motion.

The function of a tribotechnical system is to use

the system structure for converting input vari

ables (e.g., input torque, input speed, input type of

motion, and sequence of motions) into technically utilizable output variables (e.g., output torque, output speed, output motion) (GfT, Moers 2002, Czichos & Habig 2003). The primary type of interaction depends greatly on a friction state. Consequently, when a lubricant is present, the atomic/molecular interaction might not occur, while the mechanical interaction can. Friction and wear in a given TTS ultimately depend on the interactions between elements. The friction state, the effective mechanisms of friction and wear, and the contact state can be used to describe the interactions. The tribological loads occurring in the real contact areas produce tribological processes. These tribological loads include the dynamic physical and chemical mechanisms of friction, wear and boundary-layer processes. Due to the TTS there are a lot of oil diagnostic data available. The data were also obtained thanks to the maintenance monitoring program in the Czech Armed Forces. These data are considered to be the final outcome of tribodiagnostic, but they are not when it comes to assess system health and condition. These data can tell us a lot about lubricants/life fluids quality itself and a system condition. In terms of reliability, maintainability and safety we consider such data to be very valuable. There are methods analysing oil/life fluids samples. Some of these methods have been used in this paper in order to determine the physical quality of a sample and to get the picture of it, e.g. age, condition, etc. Since the system operation, the taking of oil samples and the outcomes themselves are very fuzzy, we adapted some approaches from the fuzzy logic theory. This function was later supported by the approaches of fuzzy logic.
REFERENCE Czichos, H. & Habig, K.-H. 2003. Tribologie-Handbuch; Reibung und Verschleiß, 2nd edition. Weisbaden: Vieweg. In German.

Decision support with a markovian approach for maintenance

context activities

P. Vrignat, M. Avila, F. Duculty & B. Robles

University of Orléans, PRISME Laboratory, MCDS Team, IUT de l'Indre, Châteauroux, France

F. Kratz

ENSI, PRISME Laboratory, MCDS Team, Bourges, France

ABSTRACT

Industrial processes need to be maintained to prevent breakdown. Some years ago, maintenance activities were only deployed to repair process after the problem occurs.

As in these studies, we show that a degradation level of a process can be proposed to the expert, from series of "field" events. In this study, we try to learn, without "a priori", this default signature.

The originality of our work, is to use maintenance activities as an indicator (Figure 1). Works, pre sented in this paper, take part of condition moni toring systems. Using observations provided on the process, we try to generate an availability indi cator which can be used by maintenance manager to plan actions dynamically (Figure 1). Accord ing to system availability, preventive maintenance could be scheduled to prevent uncontrolled stops of system.

The replacement of components for which

failure is thought to be imminent, can be per

formed when the component is strongly damaged

according to different use criteria, or when it has

reached a critical condition. The success of this

approach depends on the ability to predict remain

ing life of the component and when to perform the

replacement.

Hidden Markov Models (HMM) have been

Figure 1. Works goals.

Diagnostic of discrete event systems using timed automata

in MATLAB SIMULINK

Z. Simeu-Abazi

G-SCOP laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

E. Gascard

TIMA laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

F. Chalagiraud

Polytech'Grenoble, Université Joseph Fourier, Grenoble, France

ABSTRACT

In the field of dependability, diagnostic plays a

most important role in the improvement of the

operational availability of equipments. In the

industrial field, a significant part is devoted to

the maintenance, the tests and the diagnostics of

systems (Blanke et al., 2003). Generally, diagnos

tic involves two interrelated phases: the detection and the localization of failures. The approach proposed in this paper is based on operating time and is applicable to any system whose dynamical evolution depends not only on the order of discrete events but also on their durations as in industrial processes.

Diagnosis of faults is achieved through the implementation of a model observer based on timed automata. This observer called diagnoser makes it possible to detect and locate possible process failures in real time. A failure is detected when an event is not reaching the desired date, or if it lasts too long compared to its ongoing operations. Temporal knowledge of the process to be monitored is therefore essential (Lunze et al., 2001, Simeu-Abazi et al., 2010).

The proposed diagnoser is a monitoring tool that can detect, isolate and locate a fault in a system. The used methodology is based on the timed automata.

The presence of an error corresponds to the execution of a state defined as the defective controller. For the detection phase, parameter detectability is the ability to detect a fault in the system. For

the localization phase, the isolation is a property

that corresponds to the ability to isolate (locate)

Differential evolution for optimal grouping of condition monitoring

signals of nuclear components

P. Baraldi, E. Zio, F. Di Maio & L. Pappaglione

A. Politecnico di Milano, Milano, Italy

R. Chevalier & R. Seraoui

Electricité de France—R&D, France

ABSTRACT

It is well known that grouping measured signals

and then building a specialized model for each

group allows to remarkably increase the condi

tion monitoring performance (Roverso, D. et al.,

2007). In this paper we propose an approach for

optimally grouping a large number of signals

measured, for utilization in models for reconstruct

ing the equipment behavior in normal conditions.

The algorithm considered in this work is based on

the Auto-Associative Kernel Regression method

(AAKR), an empirical modeling technique that

uses historical observations of the signals taken

during normal plant operation (Hines, J.W. &

Garvey D.R. 2006). We use a Differential Evolu

tion (DE) algorithm for the optimal identification

of the groups (Storn, R. & Price, K. 1997); the deci
sion variables of the optimization problem relate
to the composition of the groups (i.e. which signals
they contain) and the objective function (fitness)
driving the search for the optimal grouping is con
structed in terms of quantitative indicators of the
performances of the condition monitoring mod
els themselves: in this sense, the DE search engine
functions as a wrapper around the condition
monitoring models (Fig. 1). A real case study is
considered, concerning the condition monitoring
of the Reactor Coolant Pump (RCP) of a nuclear
Pressurized Water Reactor (PWR). The results of
the grouping are evaluated with respect to the accu
racy, i.e. the ability of the overall model to correctly
and accurately reconstruct the signal values when
the plant is in normal operation and robustness, i.e.
the overall model ability to reconstruct the signal
values in case of abnormal operation and conse
quent anomalous behavior of some monitored
signals of the estimates of the monitored signals by
the condition monitoring model developed on the
optimal groups, and compared with those achieved
with groups obtained using Genetic Algorithm

Ensemble of unsupervised fuzzy C-Means classifiers for clustering

health status of oil sand pumps

F. Di Maio

Energy Department, Polytechnic of Milan, Milan, Italy

E. Zio

Energy Department, Polytechnic of Milan, Milan, Italy

Ecole Centrale de Paris and Supelec, Grande Voie des Vignes, Chatenay-Malabry Cedex, France

M. Pecht, P. Tse & K. Tsui

Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong,

Kowloon Tong, Hong Kong

ABSTRACT

Detection of anomalies and faults in slurry pumps is an important task with implications for their safe, economical, and efficient operation. Wear, caused by abrasive and erosive solid particles, is one of the main causes of failure. Condition monitoring and on-line assessment of the wear status of wetted components in slurry pumps are expected to improve maintenance management and generate significant cost savings for pump operators.

In this context, the objective of the present work is to present a framework for the assessment and measurement of the wear status of slurry pumps when available data is extremely limited.

Figure 1 shows the flowchart of the method:

the first step entails the collection into a dataset

of raw data, e.g., vibration data; feature extraction

consists in the evaluation of the most common

summary statistics, e.g. mean, standard deviation,

in order to summarize the characteristics of the

available data; the aim of feature selection is then to obtain the features which are essential for class separation which is the goal of the last step, i.e., classification. Experimental data were collected from a number of slurry pumps that are used to deliver a mixture of bitumen, sand, and small pieces of rock from one site to another. For each pump, vibration is monitored as a symptom of system health. Vibration signals have been collected at the inlet and outlet of slurry pumps operating in an oil sand mine. The main idea is to combine the predictions of multiple unsupervised classifiers, based on fuzzy C-means clustering (FCM), to reduce the variance of the results so that they are less dependent on the specifics of a single classifier. This also reduces the variance of the bias, because a combination of multiple classifiers may learn a more expressive concept class than a single classifier. The method relies on an unsupervised clustering ensemble methods, based on FCM for classifying the available data. In particular, the adopted unsupervised FCM approach exploits the advantages of the automated generation of fuzzy rules, low computational burden, and the high-level, humanlike thinking and reasoning of fuzzy systems, which offer an appealingly powerful framework for tackling practical classification problems. Fault detection based on FCM allows building clusters with uncertain boundaries accommodating for different pump locations and different pump types and sizes. Moreover, the cluster centers identified by the FCM can turn out useful during on-line fault detection for classifying a new developing degradation pattern into healthy/ failed clusters according to the distances of the feature values from the centers. The application of Figure 1. Pattern recognition flowchart.

the framework (data collection, feature extraction,

feature selection and classification) can be useful

for industries to monitor the health of a machine

prone to degradation and sporadic catastrophic

breakdowns and dynamically plan equipment

maintenance. However, further verification with

additional real data is required for the frame

work to be of practical use in real industrial

Evaluation of relevance of stochastic parameters on Hidden Markov

Models

B. Roblès, M. Avila, F. Duculty & P. Vrignat

PRISME Laboratory, MCDS team University of Orleans, France

F. Kratz

PRISME Laboratory, MCDS team ENSI, Bourges, France

ABSTRACT

Prediction of physical particular phenomenon

is based on knowledge of the phenomenon. This

knowledge helps us to conceptualize this phenom

enon around different models. Hidden Markov

Models (HMM) can be used for modeling com

plex processes. This kind of models is used as tool

for fault diagnosis systems. Nowadays, industrial

robots living in stochastic environment need faults

detection to prevent any breakdown. In this paper,

we wish to evaluate relevance of Hidden Markov

Models parameters, without a priori knowledges.

After a brief introduction of Hidden Markov

Model, we present the most used selection criteria of models in current literature and some methods to evaluate relevance of stochastic events resulting from Hidden Markov Models. We support our study by an example of simulated industrial process by using synthetic model. Therefore, we evaluate output parameters of the various tested models on this process, for finally come up with the most relevant model.

Data used for evaluation: We use synthetic model to produce about 1000 data events. These simulated symbols, according to real industrial process, are obtained by using uniform and normal distribution. Correlatively, we produce states for others models by using same process. Then, these states are used to compare models whose states are obtained by differents learning and decoding algorithms:

- Baum-Welch learning, decoding by Forward,
- Segmental K-means learning, decoding by Viterbi.

Criteria used for evaluation: We try to evaluate the best Hidden Markov Model, by using

Exploitation of built in test for diagnosis by using Dynamic Fault Trees:

Implementation in Matlab Simulink

Eric Gascard

TIMA laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

Zineb Simeu-Abazi

G-SCOP laboratory (CNRS—Grenoble INP—UJF), Grenoble, France

Joseph Younes

Polytech'Grenoble, Université Joseph Fourier, Grenoble, France

ABSTRACT

Fault tree (FT) (Vesely, Goldberg, Roberts & Haasl 1981) is a tool commonly used to assess the causes of industrial system failures. It is particularly used in order to guarantee safety levels of complex sys tems, and to avoid excessive financial losses. As an example, in the aeronautical field, the diagnostic of all the electronic devices of an aircraft is based on the alarm messages recorded during a flight. In order to establish a diagnostic FT can be used to correlate these alarms between each the others according to specific rules. However, some of these warnings can be false alarms and the localization of the system failures can be ambiguous. Further more, FT are limited because they are built with traditional logic gates (OR, AND) which do not consider the dynamic aspects such as the time and the dependencies in an automated system.

Consequently, a new type of logic gates has been created to extend the FT into a new version called Dynamic Fault Tree (DFT) (Dugan et al., 1990, Dugan et al., 1992) which uses both the traditional and the dynamic logic gates in order to consider all the functioning aspects of discrete event systems. It will make it possible to improve the efficiency of the diagnostic resulting in lower maintenance costs and better safety levels of automata.

This paper presents the purpose of Dynamic Fault Tree in order to diagnose discrete event sys tems. The aim is to filter built in test false alarms (Rosenthal & Wadell 1990, Westervelt 2004) in automated systems that feature dependencies. This work consist in programming the logic gates using the StateFlow library of Matlab Simulink and add them to a Matlab toolbox created especially

Fault detection through physical modelling in an axial flow compressor of a combined-cycle power plant

J.A. García-Matos, M.A. Sanz-Bobi & A. Muñoz

Institute for Research in Technology (IIT)—ICAI School of Engineering—Comillas Pontifical University, Madrid, Spain

A. Sola

Iberdrola Generación S.A

ABSTRACT

Technological development in recent decades has resulted in a steady growth in power demand, which has required an increase of electrical power genera tion resources. All these new generating resources require significant investments and maintenance, which involve high costs for companies and lead to higher energy costs. In this context, it is very important to implement an appropriate system able to monitor the health of the assets and, in par ticular, to detect and diagnose faults in advance.

An important part of these new genera tion resources are combined-cycle power plants. In these facilities, the axial flow compressor within gas turbines is a critical component. Its malfunc tion could cause important repair costs, important non-production losses and even power plant shut downs (Carazas & de Souza 2010). For this reason, early fault detection and diagnosis in these equip ments are extremely valuable in order to prevent undesired unavailabilities and to ensure the reli ability of the service.

One of the best options to perform evaluation of the health condition of an asset is its continuous monitoring based on multiple sensors acquiring

data from the most critical variables of the system (Garcia et al., 2006). Traditional fault detection and diagnosis methods use these data to perform their tasks. It ought to be taken into account that in many cases not all relevant variables can be con tinuously monitored. This might be due to costs constraints or to the technical difficulty for meas uring certain physical variables. However, some of these non measurable variables can precisely describe the system behaviour because they have a clear physical meaning. Some changes in their typical values that could alert about any anomaly or change in the current condition of an industrial component.

This paper proposes a new method for fault detection and diagnosis using real-time informa

Fault propagation in systems operating phased missions

R. Remenyte-Prescott & J.D. Andrews
University of Nottingham, UK

ABSTRACT

Locating causes of faults and reducing system maintenance downtime can have substantial ben efit to complex engineering systems. Fault diag nostic systems use sensor information in order to determine the causality of loss of functionality in

terms of component failures. In practice a limited number of sensors can be installed, therefore, a strategy is needed on how to select the sensors. For example, the sensors can be chosen according to the value of the information that they produce to the fault diagnostic process. The value of each sen sor can be described by the effect on the variable which it measures, when component failures occur and the disturbances are propagated through the system. In order to identify the symptoms of com ponent failures a fault propagation technique is needed, which can monitor the deviations in the system process variables, produced when single or multiple component failure events occur.

A fault propagation process can aid in the design of the fault diagnostic system, but it also has a use in its own right. Such modeling approach can be used to confirm or reject the occurrence of reported faults. This situation can occur dur ing the system start-up phase when false faults are reported due to high levels of vibration or due to independently designed interfaces of subsystems. This can result in unnecessary system shutdowns. Using the fault propagation modeling to establish whether the reported faults exist can help to avoid

such situations.

Traditional techniques to model fault propa

gation, such as digraphs (Lapp & Powers 1977),

decision tables (Kumamoto & Henley 1979) and

mini-fault trees (Kelly & Lees 1986), are limited in

their capability to model dynamic system behav

ior. Therefore, this paper considers Petri nets due

to their suitability to model system complexities,

such as multiple failure modes, multiple compo

nent failures, phased mission systems and dynamic

effects of component failures. The novelty of the

Guaranteeing high availability of wind turbines

G. Haddad, P.A. Sandborn, T. Jazouli & M.G. Pecht

CALCE, University of Maryland, College park, MD, US

B. Foucher & V. Rouet

EADS Innovation Works, Suresnes, France

ABSTRACT

Alternative energy sources have increasingly

gained the interest of governments, research insti

tutes, academia, and industry in order to advance

the penetration of sustainable energy to reduce the

dependency on and environmental hazards posed

by traditional energy sources such as coal and oil.

Wind energy stands at the forefront of these energy

sources; the United States Department of Energy

(DoE) and the National Renewable Energy Lab

(NREL) for instance, under the ‘20% Wind Energy

by 2030’ plan, announced that the US could feasi

bly increase the wind energy’s contribution to 20%

of the total electricity consumption in the United

States by 2030 (U.S. DoE, 2008).

Wind energy sources face numerous challenges

that obstruct them from competing with tradi

tional sources, and capturing a significant market

share. Wind energy has not been proven out over

a sufficient amount of time to assess their long

term viability. Furthermore, the reliability of wind

turbines turned out to be different from what was

originally predicted.

This paper presents the major challenges with

guaranteeing high availability of wind turbines;

reliability and maintainability, and availability- a

function of both. The paper then discusses Prog

nostic and Health Management (PHM) meth

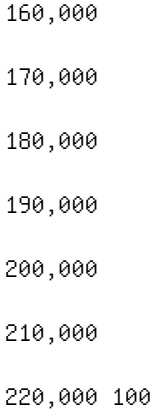
ods as potential solutions for guaranteeing high availability of wind turbines. PHM consists of methods and technologies to assess the reliability of systems in the actual life cycle and mitigate system risks. PHM is an enabler of ConditionalBased Maintenance (CBM), which can potentially reduce the operation and maintenance cost of wind farms. The paper then discusses the efforts of prognostic and health management or condition monitoring that have been performed on wind turbines. They are mainly focused on the gearbox, generators, blades, oil, electronics, and overall performance. We then propose a solution for the health monitoring of the blades and

gearboxes of turbines; TRIADE, and we give the specifications of the sensor system that are relevant to the application. Finally we perform a return on investment analysis to justify the implementation of PHM on wind turbines. We consider TRIADE with data for offshore wind farms from the literature. Results include optimal prognostic distance, life cycle costs with and without PHM, and a distribution of the return on investment. This work sheds the light on the importance of PHM to the wind energy industry and demonstrates the economic viability of implementing PHM using an already developed sensor system.

REFERENCE U.S. Department of Energy-Energy Efficiency and Renewable Energy, 2008, 20% Wind Energy by 2030, Increasing Wind Energy's Contribution to U.S. Electricity Supply.

Figure 1. Variation of mean life cycle cost with a fixed

maintenance interval (1000-socket population).



s t

p

e r

S

o

c k

e t

(

E

u

r o

s) Optimum prognostic distance = 470 hours

Method of fault detection and isolation in nonlinear electrical circuits

A. Zhirabok & D. Tkachev

Far Eastern Federal University, Vladivostok, Russia

ABSTRACT

Electrical circuits are a convenient tool for

modeling different technical objects such as trans

formers, synchronous and asynchronous electrical

machines, drives, and so on. For this reason, electri

cal circuits are the subject of investigation for fault

diagnosis. In the past decades several approaches

to the diagnosis of circuits have been developed

(Liu 1991). The majority of papers considering

the problem of fault diagnosis in electrical circuits use methods of identification (Kinsht et al., 1983, Benlder & Salama 1985, Simani et al., 2002). These methods allow providing an exhaustive analysis (in particular, determining values of parameters) but demand comprehensive information about the circuit operation and are of high computational complexity. At the same time, in practice, one need only to know that parameters of some elements have been changed.

In this paper, the method of fault detection and isolation in electrical circuits described by linear and nonlinear equations is suggested. It does not use methods of identification and allows finding out an element whose parameter has been changed, i.e., has been deviated from its nominal value. The suggested method is based on methods used for diagnosis in dynamic systems (Zhirabok & Usoltsev 2002). This method uses simple matrix methods and can be applied for diagnosis in nonlinear elec trical circuits containing non-differentiable nonlin earities such as saturation and hysteresis.

To solve the problem under consideration, so-called logic-dynamic approach developed in (Zhirabok & Usoltsev 2002) is suggested. This

approach includes the following three steps.

Step 1. Replacing the initial nonlinear model

describing the circuit by certain linear model.

Step 2. Solving the fault detection and isolation

problem for this linear model with certain addi

tional restrictions by known methods. The step

results in a set of linear diagnostic observers.

Step 3. Transforming the obtained linear observ

ers into the nonlinear ones by adding nonlinear

terms. The step results in a set of nonlinear

Modeling and fleet effect for the diagnosis of a system behavior

F. Ankoud, G. Mourot & J. Ragot

Centre de Recherche en Automatique de Nancy, CNRS, UMR 7039, Nancy-Université, Nancy, France

R. Chevalier & N. Paul

EDF R&D, Département STEP, Chatou, France

ABSTRACT

In many industrial sectors, a group of identical

machines can be exploited by the same process

(nuclear power plants, wind farms, etc.). These

machines may, however, work under different con

ditions. Such a set of machines is called a “fleet of

machines”. In this paper, the problem of modeling

the normal behavior of those machines, in the aim

of their diagnosis, is considered. Under linearity

hypothesis, models describing the normal behavior of identical machines of a fleet may share some common parts (with the same explanatory variables and coefficients) depending on the environmental conditions under which the machines are operating. Identifying these models under the consideration that they may share some common parts is an unsolved problem in the literature. In [2], a method is presented in order to identify, based on the data collected on several identical machines, both the structure and the coefficients of the linear models using a generalization of the LASSO method [4]. However, this approach supposes that all the models have the same structure and approximately the same coefficients. In [3], a method for estimating the coefficients of the models sharing some a priori known common part is proposed.

A method for identifying the models of different machines of the same fleet taking into account an identified common part shared by all the models was presented in a previous work [1].

All existing work on the identification of multiple linear models does not take into account that, in

Centre de Recherche en Automatique de Nancy, CNRS UMR 7039,
Nancy-Université, Nancy, France

Pierre Beauseroy, André Smolarz & Edith Grall-Maës

Institut Charles Delaunay, STMR CNRS UMR 6279, Université
de Technologie de Troyes, Troyes, France

ABSTRACT

Classical machine learning technologies have

achieved much success in the learning of a sin

gle task at a time. However, in many practical

applications we may need to learn a number of

related tasks or to rebuild the model from new

data, for example, in the problem of fault detec

tion and diagnosis of a system that contains a

set of equipments a priori identical but working

under different conditions. Indeed, it is common

to encounter in industrial problems a number of

a priori identical plants, such as in the building or

maintenance of a fleet of nuclear power plants

or of a fleet of their components. In such cases,

the learning of the behavior of each equipment

can be considered as a single task, and it would

be nice to transfer or leverage the useful informa

tion between related tasks. Therefore, Multi-Task

Learning (MTL) has become an active research

topic in recent years.

While most machine learning methods focus

on the learning of tasks independently, multi-task learning aims to improve the generalization performance by training multiple related tasks simultaneously. The main idea is to share what is learned from different tasks (e.g., a common representation space or some model parameters that are close to each other), while tasks are trained in parallel [1]. Previous works have shown empirically as well as theoretically that the multi-task learning framework can lead to more intelligent learning models with a better performance.

In this paper, we present a new approach to multitask learning based on one-class Support Vector Machines (one-class SVM). The one-class SVM proposed by Schlkopf et al. [2] is a typical method for the problem of novelty or outlier detection, also known as the one-class classification problem due to the fact that we do not have sufficient knowledge about the outlier class. For example, in the application of fault detection and diagnosis, it is very difficult to collect samples corresponding to all the abnormal behaviors of the system. In the

Central Institute for Labour Protection—National Research Institute, Warsaw, Poland

O. Hryniewicz

Systems Research Institute Polish Academy of Sciences, Warsaw, Poland

ABSTRACT

The analyses of accidents happened in the course of machine operation presented in Dźwiarek (2004) showed that 36% of them were caused by improper functioning of the machine control systems. Additionally, in the group of accidents caused by improper functioning of machine con trol systems serious accidents happened much more frequently (41%) as compared to the group of accidents with no relation to the control sys tem (7%). Those results proved that designers of the safety related control systems should improve their resistance to fault, which most frequently means the application reliable elements and redundant architecture of the systems. In pre venting the accidents due to improper operation of the control system periodical inspection of their functioning is of crucial importance. There fore, the control system designer should specify how often the system should undergo the periodi cal inspection. The paper presents some recom

mendations for the determination of periodical inspection frequency of safety related control systems in machinery. The recommendations are based on very simple and easy to use mathemati cal models which have been developed by adap tation and simplification of models used for the determination of maintenance policies of com plex systems.

Let us consider the simplest case when the inspection allows immediate verification if a sys tem is ready to perform its safety function or not. The assumption that the “probability of a dan gerous failure per hour” remains constant over the whole life cycle of the machine accepted in standards ISO 13849-1 and IEC 62061 means that also the availability of the system should remain unchanged in every year of its exploitation. Tak ing into consideration the values of PFH D for par ticular PL or SIL, we can determine the required availability of the system per year A r (see Table 1).

If we set the required value of the availability A r we can find the inspection interval T by solving equation A(T) = A r . Hence, the required inspection interval should be calculated from the following e quation T 0 3 6 0 2 2 = ( ) 3 ( ) A r 1- ≈ ( ) A r 1- ,25 2 . λ λ (1) When the safety related control system has parallel structure w ith two channels described by the

exponentially distributed random variables characterised by failure rates λ 1 and λ 2 , respectively, we can use a procedure proposed in the international standard ISO 13849-1 , Annex D that allows to a pproximate this system with an equivalent one havin g two identical channels characterized by the f ailure rate calculated. Practical implementation of the proposed recommendation is illustrated on some actual case stud ies. The frequency of inspection has been determ ined for: system monitoring the access door to the dangerous zone of a machine with low risk level, s ystem monitoring the access door to a robot group with a high risk level and redundant control system of a light curtain that monitors the access to the dangerous zone of an assembly automatic mach ine. REFEREN CE Dźwiarek, M. (2004). An analysis of Accident Caused by Improper Functioning of Machine Control Systems. International Journal of Occupational Safety and Ergonomics, Vol. 10, No. 2, 129–136. Table 1. Required availability of the system per year for particular SIL and PL. Performance level (PL) A r Safety integrity (SIL) level a 0,957 No correspondence b 0,987 1 c 0,997 1 d 0,99956 2 e 0,999956 3

Predictive maintenance policy for oil well equipment in case of scaling

through support vector machines

M.C. Moura, I.D. Lins, R.J. Ferreira & E.L. Droguett

Center for Risk Analysis and Environmental Modeling, Department of Production Engineering,

Federal University of Pernambuco, Recife, Brazil

C.M.C. Jacinto

Petrobras-CENPES, Rio de Janeiro, Brazil

ABSTRACT

In the context of oil industry, scale deposition

(fouling caused by salt accumulation) may prevent

equipment of properly actuating. This may repre

sent the interruption of oil production as well as

economical losses related to oil well unavailability.

Scaling build-up is a result of the combination of a set of independent (or interacting) variables, such as temperature and water composition, which define the subsea environment. These factors need to be tracked in order to predict the amount of scaling that would be deposited. Having the scaling estimate, it is possible to determine the time to next predictive maintenance which aims at removing scaling that might have accumulated on the equip ment surface in an attempt of avoiding its failure. In fact, predicting the scale formation rate involves determining its functional mapping with relation to the influencing variables. However, this dependence function is generally unknown, non parametric and non-linear. Therefore, Support Vector Machines (SVM) is here used to model the dependence between environment variables and scaling deposition.

SVM is a learning method whose theory is based on statistical concepts. The main idea is to use a dataset to train an algorithm which is able to predict future outputs (scaling deposition) based on empirical inputs (set of influencing variables). In this context, SVM can be compared to Artificial Neural Networks (ANNs) that involve the Empiri

cal Risk Minimization principle which accounts

only for the errors in the training stage. On the con

trary, the training phase of SVM entails a convex

quadratic optimization problem which embodies the principle of Structural Risk Minimization that in turn minimizes the upper bound of the generalization error, with good performance even in cases of small training datasets. Additionally, the characteristics of the SVM training optimization problem enable the Karush-Kuhn-Tucker conditions to be necessary and sufficient to provide a global optimum, differently from ANNs that may be trapped on local minima. This paper precisely proposes that, from a set of empirical data, SVM can be trained in order to provide a model able to predict scaling deposition behavior over time. Given this model, it is possible to establish appropriate maintenance strategies that aim at cleaning the equipment surface in order to prevent its unavailability. In this context, SVM works as a valuable tool to anticipate the knowledge about system failures. An example of application of this methodology is provided considering scaling data obtained from simulated real environmental conditions of deepwater oil wells. For this example, after training stage, SVM was able to track scaling increase over time in order to foresee time when a scaling threshold is attained what is associated to a non-acceptable flow loss that would turn out the wellbore unprofitable. In order to do this, it was assumed a set x of variables is known for a given real environmental condition. These variables define the real scenario for which it is desired to find out how scaling goes during a finite window frame. Provided the scenario of interest it has been possible to predict scaling values and, thus establish a maintenance strategy through SVM. We also evaluate the uncertainty on scale growth and, then on the time to next predictive maintenance.

Scope and potential of applying artificial neural networks in reliability

prediction with a focus on railway rolling stock

Olga Fink & Ulrich Weidmann

Institute for Transport Planning and Systems, ETH Zurich, Switzerland

ABSTRACT

Railways have experienced a steady demand increase over the last years, and this is projected to persist. Due to increased service frequency and the interconnectedness of railway networks, the consequences of service disruptions can be very considerable. Maintaining and increasing a high level of availability and reliability by preventing or reducing malfunctions, failures, disruptions and delays is therefore essential for the efficiency and competitiveness of railway systems. This can be achieved by anticipating, planning, and manag ing malfunctions and disruptions, which requires an accurate prediction of malfunction conditions. A promising method for reliability prediction, which shows potential for further investigation, is artificial neural network (in the following referred to as “neural networks”). However, neural net works were applied in few studies of reliability prediction for railway rolling stock systems. Cur rently, there are few studies (Smith et al., 2010)of reliability predictions for railway applications with neural networks. Furthermore, the potential and the scope of applying neural networks in reliability prediction especially for railway rolling stock have

not yet been investigated systematically. The scope and potential of applying neural networks in reli ability prediction, with a special focus on railway rolling stock systems, are systematically derived in this paper.

Neural networks are applicable in reliability prediction for railway rolling stock systems in a supplementary way, especially in areas where other methods have limitations or achieve only a poor performance. In competing fields of application, the performance of neural networks for selected problems, depending on the quality of input data, is comparable or superior to state of the art methods. But they can also be applied complementarily to other methods, particularly to accelerate computations, improve performance, and to supplement or automate analyses or decisions. The major applications for railway rolling stock areas are approximation, categorization and association. The subcategories of categorization are classification and clustering. Classification is e.g., applicable for condition based monitoring, where neural networks are trained to classify the different states of the system based on combination of different describing parameters. Clustering is mainly applicable for pattern recognition for failure and malfunction failures. Association is especially applied for memorization purposes. Neural regression can be subdivided into static and dynamic regression. Whereas static regression is the most wide spread application field, dynamic regression implies more complex computation and is also the field with the most promising results. In this field, recurrent neural networks compete with other methods only to a certain extent and therefore provide additional functionalities and a boras scope of application. Neural dynamic regression is the field where there are few studies for reliability prediction. REFERENCE Smith, A.E., Coit, D.W. & Yun-Chia, L. 2010. “Neural Network Models to Anticipate Failures of Airport Ground Transportation Vehicle Doors.” Automation Science and Engineering, IEEE Transactions on 7(1): 183-188.

State estimation for nonlinear system diagnosis using multiple models:

Application to wastewater treatment plants

Anca Maria Kiss, Benoît Marx, Gilles Mourot & José Ragot

Centre de Recherche en Automatique de Nancy,
UMR—Nancy-Université, Vandœuvre-lès-Nancy, France

ABSTRACT

This article deals with the observer synthesis for uncertain nonlinear systems affected by unknown inputs. In order to design such an observer, the nonlinear system is represented under the Multiple Model (MM) formulation with unmeasurable premise variables. A Proportional Integral Observer (PIO) is considered and used for fault diagnosis using banks of observer to generate structured residuals. The Lyapunov method, expressed through Linear Matrix Inequality (LMI) formulation, is used to describe the stability analysis and to the observer synthesis. An application to a model of Wastewater Treatment Plant (WWTP) is considered.

In the field of the observer/controller synthesis, the extension of linear methods to nonlinear systems is generally a difficult problem. The multiple model (Murray-Smith and Johansen 1997) has received a special attention in the last two decades,

in order to overcome this difficulty. Then the MM approach is a mean to deal with nonlinear sys tems and to design observer for such systems and is a convex combination of linear submodels. The multiple model formulation is obtained by apply ing a method proposed in (Nagy, Mourot, Marx, Schutz, and Ragot 2010).

Most of the existing works, dedicated to MM in general and to observer design based on MM in particular, are established for MM with measur able premise variables (inputs/outputs), that repre sents a simplified situation. The MM under study in this paper is more general and involves unmeas urable premise variables depending on the state variables—requently met in practical situations— hat are not always accessible.

A proportional integral observer approach for uncertain nonlinear systems with unknown inputs presented under a MM form with unmeasurable premise variables is proposed in this paper. The state and unknown input estimation given by this

Univ Lille Nord de France, Lille, France

EMDouai, IA, Douai, France

ABSTRACT

In this article, we propose an architecture of supervision of a system who present switching dynamics. The knowledge of the system's model is limited i.e., the physical laws or differential equations that describe its behavior are unknown. In addition, the system has different operating modes. It switches between those modes according to demand. The only knowledge we have on this system is data collected from sensors by measuring its variables. The general purpose that we are after is the predictive maintenance of this system. The predictive maintenance requires a supervision architecture powerful enough to allow taking into account the specificity of this system. In order to achieve an efficient supervision on the system, we use the pattern recognition technique. This technique allows to model through classes the operating modes of the system. The system will then be modeled in classes reflecting its state of operation. The second part of the predictive maintenance strategy is the prognosis which goal is to predict the future state of operation but it wasn't aboard it in this article. The first step was to treat the data

collected from sensors. We did so by estimating functions which describe the different dynamics of the system on each range. The next step was to use a clustering algorithm, AUDyC, which makes it possible to treat those data in an auto-adaptive way, allowing the creation of classes and their online update. The observation of these classes showed the different dynamics in normal operating modes and, in presence of fault, these classes started drifting. At this point, it was necessary to differentiate between faults who affect all the dynamics of the system i.e., global faults and faults who affect only some dynamics i.e., local faults. Further on, indicators on the actual state of the system were computed. The calculation of these indicators is based on metrics between the evolving classes and their values reflected the presence of a failure. Finally, some perspectives were given on the elaboration of a control loop and its possible effects on the regulation of the system in failure. Another interesting proposition is to deepen the studies on the proposed supervision approach so that local and global faults can be monitored and diagnosed. This page intentionally left blank Fault tolerant control and systems This page intentionally left blank

Control allocation of k-out-of-n systems based on Bayesian Network

reliability model: Application to a drinking water network

P. Weber, C. Simon & D. Theilliol

CRAN—Nancy Université—CNRS UMR 7039,Vandoeuvre-lès-Nancy, France

V. Puig

Automatic Control Department—Technical University of Catalonia, Terrassa, Spain

ABSTRACT

In order to respect the growing of economic

demand for high plant availability and reliability,

fault tolerant control is introduced. The aim of

fault-tolerant control is to keep plant available by

the ability to achieve the nominal objectives in the

faulty case and/or to accept reduced performances when critical faults occur (Noura et al., 2009). In most safety critical systems, redundant components concept is considered. Particular cases of k-out-of-n (koon) systems have been developed to model various engineering systems. All these systems are over-actuated systems based on redundancy of actuators to increase the system reliability. Nowadays, one of the major problems in the dependability field is addressing the system modeling in relation with the increase of its complexity. A growing interest focused on Bayesian Network in the recent literature is presented to model the reliability of complex industrial systems (Weber et al., 2010). This modeling method seems to be very relevant in the context of complex systems (Langseth 2008). Bayesian Network is particularly able to compute the reliability taking into account observations (evidences) about the state of some components. For instance, the reliability of the system can be estimated and all its components knowing that a part of them are out of order.

This paper presents a new approach of control allocation based on the reliability of redundant actuators when failures occur. The aim is to pre

Design of fault tolerant control for nonlinear systems subject

to time varying faults

T. Bouarar, B. Marx, D. Maquin & J. Ragot

Centre de Recherche en Automatique de Nancy, UMR 7039—Nancy Université, Nancy, France

ABSTRACT

Generally speaking, there exists two strategies for faulty systems control: the passive strategy and the active one. In the case of the passive strategy, also called robust control, the controller design prob lem has been widely studied in the literature and many approaches have been proposed for linear and nonlinear systems. The objective is to ensure simultaneously the stability of the system and the insensitivity to certain faults. Nevertheless, robust control methodology concerns a specific class of faults characterized by a bounded norm. The active control or Fault Tolerant Control (FTC) has been introduced to overcome the passive control draw backs. Indeed, the FTC method allows improving the system performances for a large class of faults. The principal idea of this strategy is to reconfig ure the control law according to the fault detection and estimation performed by an observer to allow the faulty system to accomplish its mission.

Since the introduction of FTC techniques,
several works have been developed for linear and
nonlinear systems. This paper concerns the case of
discrete nonlinear systems represented by Takagi
Sugeno models.
In the last decades, Takagi-Sugeno nonlinear
systems [1] have attracted a great deal attention,
since they allow extending the linear systems the
ory to nonlinear ones. Thus, many problems deal
ing with stability, stabilization, observer design
and diagnosis have been widely studied. Never
theless, the FTC problem based on this kind of
model is not largely treated. Some works have been
introduced in recent years, for instance, trajectory
tracking FTC design approach for Takagi-Sugeno
systems subject to actuator faults has been devel
oped by [2]. Note that this approach concern the
Takagi-Sugeno systems with measurable premise
variables (i.e. premise variables depending on the
the input or the output).
In the other hand, when the premise variables are
unmeasurable (depend on the states of the system),

B. Conrard, V. Cocquempot & S. Mili

LAGIS-FRE CNRS 3303, Lille1 University, Villeneuve d'Ascq, France

ABSTRACT

This paper deals with the design of fault-tolerant control system thanks to the use of a structural model. The objective of the developed method is to determine the instrumentation scheme (sensors and actuators) of the controlled system which guaran ties to tolerate a given number of failures with the lowest cost. A structural model is used for that pur pose and allows various potential solution of instru mentation to be deduced and to be expressed as a set of required instruments. The design problem is formalized as an optimization problem that consists in searching for a subset of instruments that pro vides the best reliable system with the lowest cost. The novelty of that paper lies in taking into account different operating modes or discrete states of the process to be controlled, by introducing qualitative variables in the structural description.

STRUCTURAL MODEL AND ANALYSIS

A structural model describes the links between the physical quantities without the exact establishment of the physical equation. Despite the lack of infor mation, the analysis of models represented by a

bipartite graph or an incidence matrix, allows dif

ferent paths that go from the known variables to

the unknown variables to be deduced. with discrete states that define in which case the corresponding relations are valid. DESIGN AND OPTIMIZATION PROCESS Thanks to this analysis, for each variable (Γ) to be measured or controlled, a relation can be found about the required instruments (I) and can be expressed by a disjunctive normal form (DNF): Γ< = (I × ∨ … I y) ∧ … ∧ (I × ∨ … I z) According to the minimal number of faulty components (i.e. unusable constraints) that can be tolerated to reach each required variable, the previous relations can be transposed on constraints about the number of required instruments. Associated to a criterion of cost, the problem to solve takes the following form, which is a classical problem of optimization: Min N q n q E i m q E i 1 i m Σ Σ ( ) C Nq i i Σ ≥ ≥ ⎡ ⎨ ⎪ ⎪ ⎪ ⎩ ⎪ ⎪ ⎪ Nq n i 1 … The final result of the optimization phase is a set of instrumentation schemes with the lowest cost and which all satisfy the dependability constraints imposed by the designer. CONCLUSION This paper presents a relatively easy-to-use control system design method. With few information on the system model, i.e. by using a structural description, potential instrumentation schemes for a control system are deduced according to a given fault tolerance level and with a cost criteria. Moreover, qualitative variables are used to represent various operating modes or process states, which lead to a more accurate model of the process. physical variables known variables Q 1 Q 2 Q Output F 1 F 2 F Output

C 1 1 1 1

C 2 1 1

C 3 1 1

C 4 1 1

In this example, two ways allows Q Output to be esti

mated, be summed up by the following relation:

Q Output < = F Ouput ∨ (F 1 ∧ F 2)

This paper proposes to take into account

operating modes with the introduction of variables

Guaranteed localization using reliability of measurements in imperfect mobile sensor networks

F. Mourad & H. Snoussi

Institut Charles Delaunay (ICD), UMR STMR CNRS 6279,
Université de Technologie de Troyes (UTT), France

F. Abdallah

Laboratoire HEUDIASYC, UMR CNRS 6599, Université de
Technologie de Compiègne (UTC), France

C. Richard

Laboratoire Fizeau, UMR CNRS 6525, Université de Nice,
Sophia-Antipolis, France

ABSTRACT

This paper deals with localization problems in mobile sensor networks. It thus proposes a robust localization technique that works efficiently under imperfect circumstances. The proposed method assumes that the reliability of exchanged messages is known. Having several collected measurements, the method uses both the Dempster-Shafer and the interval theories to combine all available informa tion, and thus to make accurate decisions about sensors positions.

Mobile Sensor Networks (MSN) are networks composed of a large number of wireless devices, called intelligent sensors (Akyildiz, Su, Sankarasubrama niam & Cayirci 2002). These sensors have compu

tation, communication and sensing capacities. Due to their wireless nature, sensors in MSN are able to move in an uncontrollable manner (Shorey 2006). In other words, sensors change positions in a pas sive manner due to an external force. In such situa tions, sensors need to be localized regularly.

In this paper, we propose an original algorithm for sensors localization in imperfect circumstances. The proposed method is an anchor-based method where two types of sensors are considered: anchors, equipped with GPS and thus having known posi tions, and non-anchor nodes, unaware of their locations, and thus they need to be localized. To do so, nodes collect distance information from neigh boring anchors. Collected measurements mainly contain the anchors coordinates. The method assumes that the reliability of such measurements is given. In other words, in this paper, we do not propose a technique for computing measurements reliability. Collected information is then combined using the Dempster-Shafer (Smets & Kennes 1994) and the interval theories (Jaulin, Kieffer, Didrit & Walter 2001). If we consider a specific mobile node, the final solution would be composed of a set of boxes, each of which having a specific weight.

Leak detection in the lubrication system of an aircraft turbine engine

L. Rakoto & M. Kinnaert

Université Libre de Bruxelles, Brussels, Belgium

M. Strengnart & N. Raimarckers

Techspace Aero, Milmort, Belgium

ABSTRACT

This paper deals with a method for detecting leaks in the lubrication system of an aircraft turbine engine during flight. Leak detection in the lubrication system is usually performed by the monitoring of the oil level in the tank. However, the measurement of the oil level is affected by the oil consumption, the thermal expansion, the gulping and the attitude variation of the aircraft. The gulping represents the oil quantity which is not contained in the tank (i.e. oil hiding in the engine [pumps, pipes, sumps, etc.]).

In order to avoid the use of any additional sensor, a grey box model of the oil tank level variation is developed by exploiting experimental. Contrary to previous work [1], a single model is used for the entire operating range of the engine. Moreover, a systematic parameter estimation, using data recorded from the last flight, is developed to maintain the model accuracy despite the aging of the system. Measurements of the engine speeds, the oil tank

temperature and the aircraft attitude are processed by a time-varying Kalman filter, which is designed based on the former model, to provide estimation of the level rate variation. The innovation sequences of the Kalman filter are monitored by several statistical change detection algorithms to detect the presence of a leak in the lubrication system. Validation has been performed using data from an aircraft during normal flight. REFERENCE [1] Diez, E., 2008. Diagnostic et pronostic de défaillances dans des composants d'un moteur d'avion. Masters thesis, Université Toulouse. III - Paul Sabatier.

Prognosis applied to an electromechanical system: A nonlinear

approach based on sliding mode observer

D. Gucik-Derigny, R. Outbib & M. Ouladsine

Université Aix-Marseille, Domaine Universitaire de St Jerome, Marseille, France

ABSTRACT

In the last decades, diagnosis methodologies were

developed in order to detect, to locate and to iden

tify the faults. The proposed methodologies on diag

nosis were concerned by fault detection. The main

aim is the fault detection in the process. Hence, the

methodologies of the diagnosis are adapted for sit

uations after fault occurrence. Afterwards, results

were established considering the problem of pre

dictive diagnosis which are devoted to prediction

of the fault before its occurrence and as soon as

possible. This concept is interesting, however it can

be inadequate concerning the economic challenges

and for safety.

More recently, a new concept has emerged: the prognosis. The goal of this concept is to estimate the Remaining Useful Life (RUL) of systems and hence to forecast faults occurrence. This paper concerns model-based prognostic.

Throughout this work, it is assumed that the behavior of the considered technological process can be described using a multiple time scale model of the following form:

x f x u g x

y y x u

.

. = ϵ =

⎧

⎨ |

⎩ | (, ( ),) (,) (, ,) θ φ

φ = φ φ (1)

where x ∈ R n is the state of fast dynamic behav ior. θ ∈ R r denotes a parameter vector assumed to be a function of φ ∈ R q the state of damage state. u ∈ U ⊂ R m designates the input vector where U is a set of admissible controls. The ratio ϵ is that 0 < ϵ 1. y ∈ R p is the output vector. f, g, h are differentiable functions in adequate dimensions. f, h and the structure of g are assumed to be known. System (1) is used to describe simultaneously the behavior of the

process state and the evolution of the damage state. Moreover, the system expresses the interconnection of the two variables (i.e., process state and the damage) and it allows taking into account the time scale aspect induced by the difference of the dynamic behaviors. In fact, the process state is assumed to be with fast dynamic while the damage state is considered with slow dynamic. Here, the subsystem (1a) describes the behavior of the state of the system and is assumed to be well defined. However, only the structure of the subsystem (1b) is supposed to be known a priori. Generally, in the literature the dynamics for the damage state is supposed to be polynomial function. A main objective is to identify parameters of damage state dynamic behavior (1b). For that, the strategy consists in estimating unmeasured state for fast dynamic behavior subsystem based on the design of an unknown input observer. Hence, slow dynamic behavior state present in the fast dynamic behavior subsystem is led back to an unknown input. Unknown input sliding mode observer is designed to obtain accurate estimates for state, unknown input and dynamic of unknown input. Finally, parameters of slow dynamic behaviour are then identified. The problem of unknown input observers synthesis has attracted the interest of several authors and many results were proposed. In this work, a classical kind of finite time unknown input observer is applied to an electromechanical system for the problem of prognosis. From state estimate accuracy in finite time depends accuracy of parameter identification of slow dynamic behavior model and also the quality of the remaining useful life predictions. Here, our comparison is achieved on an electromechanical system.

R 2 wAC: Recursive redundancy with active comparison

J.G. de Chavarri, J. Mendizabal Samper, A. Villaro, S. Urcelayeta,

J.M. Blanco & A. Galarza

Ceit and Tecnun (University of Navarra), San Sebastian, Spain

ABSTRACT

A fault tolerant system is a system capable of

fulfilling its operation without considerable per

formance degradation and without data cor

ruption, in the presence of failure due to either internal or external causes. These systems are used in systems such as medical systems, aircraft and railway communications systems whose function ality is constrained in terms of Tolerable Hazard Rate (THR).

Safety standards set the maximum THR and define Safety Integrity Levels (SIL). SIL4 is the highest level according to IEC61508 and IEC50129. A SIL4 function implies that the THR of an error in the functionality is set between 10 -8 and 10 -9 f/h.

The origin of the errors that can affect the sys tem is considered random. Among the different possibilities, there is one especially important for electronic devices that incorporate S-RAM tech nology: Single Event Upset (SEU). A SEU is a change of the state or transient induced in a device by an ionizing particle such as cosmic ray or pro ton (Stott et al., 1998).

Safety critical applications require fault toler ant architectures where computing components present very stringent failure rates. This paper presents a novel programmable logic voter design pattern. Active components are used in the archi

tecture of this voter to improve reliability.

Many techniques can be used to develop fault

tolerant systems, most of them based on redun

dancy. In this case, a hardware redundancy is

needed because the component to be designed is a

hardware voter.

An active fault tolerant voter system is designed

combining the techniques N Modular Redun

dancy (NMR) (Kshirsagar and Patrikar 2009) and

Duplication with Comparison (DwC) (Johnson

1989). The advantages of the previous mentioned

techniques are exploited to improve the depend

ability of the voter and the disadvantages are

avoided to offer the best solution in three clearly

distinguishable system steps.

The components used in this design are based

Sensor and actuator faults estimation for Takagi-Sugeno models using

descriptor approach: Application to Fault Tolerant Control

M. Bouattour

Laboratory of Modeling, Information and Systems, University of Picardie Jules Verne, Amiens, France

Industrial Processes Control Unit, National Engineering School of Sfax, Sfax, Tunisie

M. Chadli & A. El Hajjaji

Laboratory of Modeling, Information and Systems, University of Picardie Jules, Amiens, France

M. Chaabane

Industrial Processes Control Unit, National Engineering School of Sfax, Sfax, Tunisia

ABSTRACT

This note proposes sensor and actuator faults esti

mation and Fault Tolerant Control (FTC) method

for Takagi Sugeno (T-S) fuzzy system. Based on

the descriptors systems technique, the idea con

sists in estimating the faults and then taking them

account in the control. The method is based on the simultaneous estimation of state, sensor and actuator faults and then the stabilization by static output feedback. The control and the observer gains are determined by Linear Matrix Inequalities (LMI) conditions. An example is used to show the effectiveness of the proposed strategy. Human factors and human reliability This page intentionally left blank

A model-based approach for the collection of human reliability data

S. Massaiu

OECD Halden Reactor Project, Halden, Norway

ABSTRACT

One of the major criticisms against Human

Reliability Analysis (HRA) is the lack of empirical

data to support its quantitative estimations. While

there is increased confidence around the quantifi

cation of executions failure probabilities, there is

still a great deal of uncertainty when it comes to

less well-defined situations and higher-level activi

ties, like diagnosis and decision errors: that is, the

conditions that characterize the history of indus
trial accidents. New methods (second-generation
HRA) have been developed to represent more
realistically these conditions. Unfortunately, these
methods strongly rely on expert judgment for
quantification, and although their use strongly
encourages event reviews and observation of simu
lated performance, the link between quantification
and empirical evidence is not always transparent.
This paper presents an approach aimed at pro
viding a traceable empirical base to quantifica
tion in second-generation HRA methods. The
approach is potentially applicable to other aspects
of the HRA process, such as scenario analysis and
error identification.
The idea is to use a domain-specific modeling
approach to convey empirical evidence into the
expert-judgment processes of HRA. The model
is the Guidance-Expertise Model (GEM) of crew
cognitive control, which provides the classifica
tion system for collection and retrieval of domain
specific data. The GEM model recognizes and
accounts for the dominant role of the emergency
procedures during disturbances. In other words,
explanation and prediction of operators' behav

ior under emergencies needs to describe how the procedures are used, since in these situations the operators control the plant largely, if not entirely, through the procedures. The GEM model follows a line of research in industrial settings that describe human performance in terms of distinctive cogni tive categories. Consistently with Jens Rasmussen's Skill-Rule-Knowledge taxonomy, the GEM model postulates two control modes, or ways of acting, that the crews display in controlling emergencies with procedures. In this paper we present a test of the ability of the model to identify regularities between environmental conditions (procedures), crew expertise (teamwork) and crew behaviors. The analysis is based on complex steam generators tube rupture events obtained from four Nuclear Power Plant (NPP) control room crews in the Halden Man Machine Laboratory research simulator. The test shows that the approach is capable of retrospectively identifying crew behaviors of interest for HRA (e.g., unexpected progressions in the procedures set, responses to cues and extraneous events) and relating these to observable performance conditions. At present stage, the environmental conditions are the procedures and the crews' expertise as measured by the quality of teamwork. The behaviors are not necessarily errors or failures, but represent generic types of crew activity that typically impact the performance of tasks, and as such are part of possible failure stories of emergency systems. Eighteen such behaviors are identified. The test also highlights environment-cognitionbehavior regularities. These are obtained by calculating: 1) the frequency of occurrence of the outcome behaviors in the different control modes and by procedural guidance type; and 2) the frequency of occurrence of positive and negative teamwork dimensions in the different control modes. Given the small sample size, no discussion of these relationships is made, but the results are presented for illustration. The main benefit of this approach is the possibility of collecting data on emergency operation behaviors and systematically relating them to observable features of the operational environment. These observed patterns could, in turn, constitute a source of empirical

support for assumptions made in predictive analysis of scenario evolutions and of system failure that refer to the same environmental characteristics.

Accidents in the gas distribution industry: Some consequences

of the introduction of new analysis criteria

G. Desmorat, P. Desideri & F. Loth

Pôle Maîtrise des risques, Gaz réseau Distribution Paris, France

F. Guarnieri & D. Besnard

Centre for Research on Risks and Crises, Mines ParisTech, France

ABSTRACT

The importance of the learning from past

experience process is crucial for today’s com

plex businesses. The difficulty of evaluating their

degree of organizational resilience and the social

and regulatory context imposes strict risk manage

ment policies, which drives the development of

new safety management tools. Consequently, the

development of efficient accident analysis tools is

needed. The process of learning from past experi

ence allows capitalization and exploitation of data

from event analysis in order to develop prevention

policies and barriers to protect the organization.

The design of such a process requires a choice of

paradigm. The most common paradigm is based

on dependability, which advocates a mechanistic

view of accidents and makes the individual one failure factor among many in the system. However, several major catastrophes have driven experts to reevaluate the basic tenets of these methods. This re-evaluation led to the adoption of the Human and Organizational Factors paradigm.

This paradigm is characterized by the idea that an accident is no longer simply a technical phenomenon. Operators' performance is then explained by the influence of the socio-cultural context. Accident analysis framed by Human and Organizational Factors therefore aims to explain people's performance in terms of a context that is prone to failure.

GrDF (Gaz réseau Distribution France) is a company specialized in the distribution of natural gas. Its network is 190,000 km long. The notable feature of this network is the level of exposure to threats such as structural damage due to public works carried out by external contractors. Here, there is a great need for learning from experience which must respond to the high safety standards the company must meet.

To meet this requirement, GrDF initiated a project which led to the creation of an analysis

grid based on some components of the CREAM method (Hollnagel, 1998). This will be discussed in detail in the presentation. The concept of Common Performance Conditions (CPC; Hollnagel, op. cit.) was used for the understanding of human and organizational factors. The work was carried out jointly with Mines ParisTech. This collaborative approach has allowed knowledge transfer to GrDF bodies responsible for safety management. That operator's failure is due to the negative influence of the context on performance is an ideological departure for a company shaped by the earlier paradigm of human fallibility. The analysis grid developed by GrDF encourages operators and field managers to adopt this new way of understanding human performance. This article will present the preliminary results of the grid. Two years of experience have identified several points of resistance and various factors leading to success. The first success factor lies in the interest of operators and local managers in the new tool. It can be taken as a sign that the break with the past has been fully accepted. However, the spirit of the method remains relatively misunderstood. This is illustrated by the persistence of practices influenced by the dependability paradigm. Two lessons emerge. The first is the critical role of generational and demographic issues in the success of an approach that requires such a major break from past practices. It is easier for young people to make the necessary change in how they see their role, compared to operators with a longer history within the company. The second key point is the importance of internal communication, which has played an increasingly important role over time. These two elements form the main points which help to avoid a drift away from original course of action. REFERENCE Hollnagel, E. (1998). Cognitive Reliability and Error Analysis Method. Oxford: Elsevier Science.

An approach to predict human reliability in manual assembly

B. Günnel, M. Schlummer & A. Meyna

University of Wuppertal, Germany

M. Schick, F. Heumeni & M. Haueis

Daimler AG, Sindelfingen, Germany

ABSTRACT

As a result of the severe competition in the auto

motive industry and the continuously increasing customer requirements concerning quality and price, companies are interested in providing a max imum level of quality while keeping their costs as low as possible. Quality and price are significantly influenced by the production of the vehicle itself as the quality, later to be experienced by custom ers, is generated here. Furthermore, a large propor tion of the production costs are caused in vehicle assembly.

Due to the fast-changing automotive market driven by continually changing versions of mod els, the assembly is carried out manually to a large extent in automotive production. The individual person who performs the assembly is very impor tant since he or she directly affects the quality of the products. To ensure high quality the produc tion system must be extremely reliable, which is determined by human reliability. Therefore it is very helpful to know which human actions or tendencies may reduce the quality of, or create a defect in, the finished product.

The aim of this study is to create an approach, which shall provide a quantitative prediction of human reliability in manual assembly. At present

the known methods for predicting human reliabil

ity, which use for their assessment task-, time- or

PSF- (Performance Shaping Factors) related quan

tification principles, are not practicable for vehicle

production. Thus a new approach has to be gen

erated that regards documents and failure data of

the vehicle assembly. Using mathematical and reli

ability methods to analyze the collected informa

tion of the assembly it is finally possible to predict

the expected failures in the assembly.

The assessment tool developed by this study

is an operation-based model which uses available

standardized documents from manual assembly,

Assessing the impact of domain-specific cognitive profiles

on the reliability of human operators in the railway domain

M. Arenius & O. Sträter

Fachgebiet Arbeits—und Organisationspsychologie, University
of Kassel, Kassel, Germany

M. Hammerl, M. Talg & K. Lemmer

Institute of Transportation Systems, German Aerospace
Center, Braunschweig, Germany

H. Franzmeyer & B. Milius

Institute of Railway Engineering and Systems Safety,
Technische Universität Braunschweig, Germany

ABSTRACT

Human cognition is tightly coupled to the context

in which it operates (Hollnagel, 2004). Thus, any model aiming at capturing the features of cognition relevant for human reliability should consider the nature of the connection between the mind and the working environment affecting and shaping it if valid conclusions on human behavior are to be derived.

The Cognitive Couplings address the principal ways in which human cognition is bound to the working environment (Sträter & Bubb, 2003). They constitute a classification scheme for man machine interaction in terms of types and levels of cognitive demand associated with a task.

By mapping a pattern of mental demands to the (often very technical) tasks at all levels, a cognitive profile with which the individual has to cope with is obtained, establishing a first link between working environment and its hypothesized effect on cognition.

In order to capture and ultimately quantify the actual effect on cognition and therefore performance, the human adaptive capacities towards these hypothesized configurations of cognitive demand have to be assessed by a model reflecting the coping strategies intrinsic to the cognition system

operating upon the profiles (Sträter, 2005). This

structured analysis of the domain-bound profiles

and their associated impact on cognition has given

valuable insights for different domains of work

(Arenius, Athanassiou & Sträter, 2010; Günebak,

Bayesian network modelling for fire safety assessment: Part I—a study of human reaction during the initial stages of a dwelling fire

D.B. Matellini, A.D. Wall, I.D. Jenkinson & J. Wang

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute,

Liverpool John Moores University, Liverpool, UK

R. Pritchard

Merseyside Fire and Rescue Authority, Liverpool, UK

ABSTRACT

Providing fire and rescue services is hugely complex

due to the sheer number of different potential sce

narios which must be covered. Not only are there

variations between the types of locations, for

example factories, vehicle tunnels, dwellings, etc.,

but there are also many different circumstances

within each type of location. Taking dwellings

for instance, there can be variations in terms

of size, design, building materials, geographical

location, fire safety arrangements, number of

occupants, activities of occupants, among others.

As for the occurrence of fire itself, each incident will be unique in terms of time of day, type of fire, state of occupants, fire cues, etc. What all these variations signify is that the potential magnitude of the next fire event and its consequences are gen erally unpredictable. Because of the complicated scenarios, unpredictability of outcomes, and high frequency of incidents, fire and rescue services have to be both capable and flexible in operation; however resources are limited and finding the opti mal way of managing fire and rescue services is a complex and ongoing task. This research aims to contribute in some way towards this cause.

Finding an effective and adaptable risk assess ment technique which can be applied to fire and rescue planning is an intricate challenge. Whatever the method, it must be capable of dealing with uncertainty both in data and the interrelation of variables, it must be adaptable in terms of being able to model various fire and rescue scenarios, and must provide practical outputs which can then be incorporated into strategic planning. Upon this background, this paper introduces the con cept of probabilistic modelling under uncertainty through the application of the Bayesian Network

Concept of operations for data fusion visualization

T.R. McJunkin, R.L. Boring, M.A. McQueen, L.P. Shunn,
J.L. Wright & D.I. Gertman
Idaho National Laboratory, Idaho Falls, ID, US
O. Linda, K. McCarty & M. Manic
University of Idaho, Idaho Falls, ID, US

ABSTRACT

Data fusion is a collection of techniques by which information from multiple sources is combined in order to reach a better inference. In considering the design of the Human-Machine Interface (HMI), the presentation of the fused data is optimized for end use. Such a design process ideally makes use of first principles and practical experience from human-computer interaction and user-centered design. Yet, extensive insights and experience with such systems remains elusive, and there is cur rently no specific guidance to help the designer of a data fusion system to present information in an optimized or usable manner. This paper outlines current efforts to create a style guide of design principles for the presentation of data fusion infor mation, specifically for a hybrid fuel production system and generally for a process control context. Process control involves an operator interacting

with a control system to ensure the effective and safe startup, operation, and shutdown of a production process. Process control can take the form of manufacturing and fabrication—including especially chemical processing—to energy production and distribution. The degree of operator interaction with the control room interface varies considerably. A modern, highly automated petrochemical production system may feature an operator in a primarily monitoring role. In contrast, an all-analog power plant control room may feature multiple operators to monitor and actively control energy production.

Current process control interfaces provide key indications on process and plant states such as temperature, flow, pressure, etc. These indications are typically provided for every available component sensor in the system. In analog process control interfaces, these sensor indicators comprise multiple panels across a control room, resulting in hundreds and sometimes thousands of indicators for the operator(s) to monitor. Digital control rooms typically employ the advantages of software windowing technology, allowing sensor readings to be displayed for only the system or components that are of interest, often coupled with an overview Piping and Instrumentation Diagram (P&ID). Data fusion may encompass

both sensor input and alarms. In terms of sensor input in a process control interface, data fusion represents the attempt to group multiple component sensor readings into a high-level system indication. For example, separate indications for temperature, flow, and pressure might be merged into a single gauge. For alarms, data fusion takes the form of aggregating multiple alarms into a single alarm. Two current approaches accomplish such aggregation: alarm filtering and root cause alarms. A predictor system includes the challenges of data fusion interfaces for existing sensor indicators—the tradeoff between displaying parsimonious indications and providing precise diagnostic information to the operator, and the challenge of down-selecting the most appropriate or relevant alarms. In addition, a predictor system presents new interface issues for data fusion. Most noteworthy of these issues is the fact that a predictor system is an uncertain indication. While the operator may assume a high degree of system integrity and sensor reliability with conventional data fusion, the operator is confronted with the new challenge that the predictor system provides a probabilistic, extrapolated outcome for the process control, but there is no guarantee that such an outcome will actually occur. Essentially, the predictor system must win and maintain operator trust. This paper presents a process that is being used to arrive at a style guide for data fusion interfaces in process control as well as for the inclusion of predictor system data in data fusion interfaces. Currently, no clear guidance exists to determine the optimized presentation of fused sensor data in process control. By employing a concept of operations approach to data fusion interface design, initial design guidance has been crafted.

Developing and evaluating the Bayesian Belief Network as a human

reliability model using artificial data

Y. Stempfel & V.N. Dang

Paul Scherrer Institute, Villigen PSI, Switzerland

ABSTRACT

A frequent assumption of Human Reliability

Analysis (HRA) methods is that Performance

Shaping Factors (PSFs) are independent in terms

of their effects on the human failure probability.

This work examines the Bayesian Belief Network (BBN) as a means to model the factors and to estimate failure probabilities when this assumption is set aside. The development and testing of the BBN, as well as the comparison of the BBN model with a more traditional model, is based on the use of artificial data sets. Artificial data refers to the generation of data with known properties, in order to test a modeling approach and evaluate its performance. In this case, the data represents a series of observations of performances, each with a set of PSF ratings and a record of whether a human failure event occurred. It is used to train a BBN and determine its parameters. The resulting BBN model's predictions of the failure probabilities are compared against the empirical (artificial) failure probabilities. In addition, the BBN model is compared against a traditional PSF HFE model; in this case, a model with PSF multipliers is selected.

The results show that the BBN model was able to capture the relationships among the factors and, in particular, to estimate the HEPs fairly accurately. The empirical HEPs to be predicted ranged

from 0.03 to 0.74. The maximum error for the set

of PSF configurations defined to be of most inter

est was 30%, for a configuration with very few

observations (26 observations in the overall sample

of 10000) and a probability of occurrence of 0.12.

The average absolute percentage error was 8%.

A key assumption of the artificial data was

that in addition to their individual effects on performance, some PSFs interacted producing an additional contribution to the HEP. In other words, their joint effect was more than the sum of their individual effects. The formalism of the BBN clearly supports the modeling of such interactions. To investigate whether this interaction term could be neglected, a multiplicative model was fitted to the data. As expected, it performed poorly on all configurations where more than one PSF was LTA (Less than Ade-quate). Third, the performance of the BBN with smaller data sets was evaluated. Instead of five sets of 2000 observations, five sets of 500 observations were used. A few of the HEPs estimated with the BBN model were moderately accurate in HRA terms (percentage error less than 50%). It was found that the critical determinants of the model performance, not surprisingly, were the inclusion of the relevant PSF configuration in the data set and the observation of some HFEs for these configurations. Among the strengths of the BBN is the ability to combine expert judgment with data within a structured framework. In this examination, expert judgment input to a BBN model was not used, focusing instead on learning from data. The performance of the BBN was favored by not including any distortions in the data (discrepancies in the PSF ratings in the data set resulting from unreliable ratings) or missing data. On the other hand, the error mechanisms were assumed to be completely unobservable. Expert judgment on the structure of the model and the observability of the error mechanism can be expected to increase the performance of BBN models. Consequently, treating these and other aspects of realistic data while incorporating expert judgment into the modeling process are important topics for future work.

Implementing of new methods for assessing human risk

in maintenance

R. Doležal

Department of Dependability and Risk, Technical University of Liberec, Liberec, Czech Republic

ABSTRACT

Popularization and actual implementation of new methods of assessing human performance in main tenance faces many challenges. In order to success fully fulfill their role, their real application has to be approved by company management and also have influence the organizational structure and provide the necessary new managerial control. This mana gerial control becomes a major obstacle to the implementation of these methods in practice. During the implementation of practically any methods for optimizing maintenance, we encoun ter the same problems and same questions from maintenance personnel. Often are identified criti cal decision of management with a much greater impact on effectiveness and safety of maintenance than the process that is “necessary to optimize”. They are also identified very critical relation ships with outside firms engaged in the main tenance of some equipment. Communication, sharing risk and the attempt to own profit of these

companies often adversely affects the reliability, maintainability and safety. In many accidents have been identified these problems as a key factor in negative course of accident scenario. Although the relationships of outside firms are under intense supervision—the supervision is not methodical and built on solid theoretical grounds, which are today already available.

Risk assessment includes risk identification, risk analysis and risk assessment. The organization should identify sources of risk, the impact of events and their causes and potential consequences. The aim of this approach is to create a comprehensive list of risks. List of identified risks should include a risk regardless of whether the organization is able or wants it to inspect and check.

For each identified risk must be developed also its criteria. These criteria should reflect values, goals and resources of the organization.

Complete list of accepted (decided) risks asso ciated with technology should be transparent tool for managerial control. This list can be entered into logical hierarchical tree, as well as other appropri ate graphic diagrams showing the flow of risks

R.L. Boring

Idaho National Laboratory, Idaho Falls, ID, US

ABSTRACT

Information foraging theory articulates the role of the human as an “informavore” that seeks information and follows optimal foraging strategies (i.e., the “information scent”) in finding meaningful information. This theory has been successfully applied to human-information interaction environments such as Internet use. There are considerable differences between consumer Internet surfing and operator interactions with control rooms in nuclear power plants. A major difference is that the information in control rooms has already been distilled to only the information that is relevant to some aspect of operations. Nonetheless, information needs vary considerably across different power and operation modes of the plant, and the operator needs to navigate to the most relevant information amid an abundance of plant indicators. This paper briefly reviews the findings from information foraging theory outside the nuclear domain and then discusses the types of information foraging strategies operators employ for normal and off-normal operations in the control room.

For example, operators may employ a predatory "wolf" strategy of hunting for information in the face of a plant upset. However, during routine operations, the operators may employ a trapping "spider" strategy of waiting for relevant indicators to appear. This delineation corresponds to information pull and push strategies, respectively, both of which are found in the control room. Yet, no studies have been conducted to determine explicitly the characteristics of a control room interface that is optimized for both push and pull information foraging strategies, nor has there been empirical work to validate operator performance when transitioning between push and pull strategies. This paper explores four examples of control room operators as wolves vs. spiders in terms of information foraging:

• Cases of information masking, in which the plant provides specific indicators of plant status, but these indicators may be absent or misleading. Such incidents are examples of operators following the wrong information scent or over relying on a particular patch of information—i.e., over-foraging. • Display layouts that optimize for foraging strategies in operator searches for information. Failing to provide indicators along a relevant foraging path may result in operators consistently overlooking or

ignoring these indicators. While in practice, this is not different than designing a good layout, information foraging offers a sound theoretical basis for explaining good display layout as one optimized for information search strategies. • Automation of plant functions, in which operator engagement is lost with some automation systems. By applying a varying process of push and pull information display, it is possible to help maintain operator engagement through creating a dynamic interaction between the plant and the operator. • Alarm response, in which current annunciator systems feature a high number of nuisance alarms, which drive operators down the wrong information path. Similarly, alarm flooding results in an overabundance of push information. The problem may be recast not simply as information overload but as information scent overload. The key to effective alarm systems may be the effective management of the information scent provided to the operator. Information foraging strategies are reviewed in terms of how they increase or decrease the operators' opportunity for successful operations. This paper concludesby proposing a set of research questions to investigate information foraging in control room settings.

Integration of human factors in project uncertainty

management, a decision support system based on fuzzy logic 1

S. Hassanzadeh, F. Marmier & D. Gourc

Université de Toulouse, Mines Albi, Centre Génie Industriel, Albi, France

S. Bougaret

Pharmaceutical R&D Management Consulting Company, Francarville, France

ABSTRACT

Project management involves making decisions

in a context of uncertainty. These decisions result

from some inference rules on some quantitative or

qualitative variables, with usually uncertain val

ues that come from different sources and could

become progressively complete and precise. Gener
ally, it is only at the end of the project that precise
and accurate values of most variables are available.
However, a project manager has to make decision,
throughout the different phases to make the project
evolves, even if the information is uncertain or the
inference rules are not strict.
It might be difficult to process all the uncertain
information and alarm signals in the decision
making process. In such circumstances, usually
the decision-maker adopts a reductive approach to
make a decision only based on the piece of infor
mation that is available and looks more important.
In doing so, the risk is that the decision is made
without some crucial information.
We propose a Fuzzy Decision Support System
(FDSS) that takes into account both quantitative
and qualitative variables and tolerates the lack or
imprecision of information. In this approach, a
sequence of decisions leads to a final choice, tak
ing progressively into account new information.
Human representation and reasoning mode are
modeled respectively by fuzzy sets and fuzzy infer
ence rules.
The basis of this approach is our definition

of uncertainty that includes both subjective and

objective aspects contributing to identification of

uncertainty. A typology of uncertainty generators

is then proposed that helps explore its sources.

The proposed typology is based on three axes:

subject (manager), object (project), and context

(organization). The main elements of the model are as follows: 1) input variables (criteria, parameters with different degrees of uncertainty) on which decision is based, 2) output or decision modalities which specify possible options, 3) inference rules (that are usually non-strict) to designate a modality of the decision to each combination of the values of input variables. The main steps of the proposed approach are as follows. First, the variables that influence decision are identified, collected, and organized according to the classes of the proposed typology of uncertainty generators. The typology helps complete the list of variables and gives the variables a structure. Second, a set of characteristics that describes each variable is established. Third, the availability of each variable according to different project's phases is studied. Fourth, the variables are evaluated and ordered according to the importance of their impact on the decision. Fifth, the inference rules are created, taking into account the order of the importance of the variables. An application case for a ski resort project illustrates the proposed method. The main characteristics of our problem are gathered in this case study: a series of decisions based on uncertain and dynamic information that becomes more accurate step by step. The application case is based on 3 × 3 formula, that is a strategy to help a guide decide whether to change his itinerary to avoid avalanches, developed by Werner Munter, a Swiss mountain guide. The results are compared with a naive decisional approach to cope with uncertainty and shows the proposed approach is effective.

1 This work was supported by the Foundation for an

Industrial Safety Culture (Fondation pour une Culture

de Sécurité Industrielle).

factors exploration

V. Rumawas & B.E. Asbjørnslett

Department of Marine Technology, Norwegian University of Science and Technology (NTNU),

Trondheim, Norway

ABSTRACT

This article is a part of a study which investigates human factors in marine design. The study was triggered by the fact that most accidents at sea were caused by human errors or human related factors (McCafferty & Baker, 2006, Moore, Bea & Roberts 1993). Some experts blame that less adequate design is one significant factor that lead to human errors (Meister, 1971, Reason, 1990, Perrow, 1999). A prior study shows that there are more than suffi cient standards and guidelines that regulate design ers to consider human factors in marine design (Rumawas & Asbjørnslett, 2010). The scope of this article is to check if the reality complies with the regulations, by doing field surveys. The Offshore Supply Vessels (OSVs) are taken as the sample of the study. An exploratory research was conducted by using qualitative approaches which includes observation method, interviews and discussions. Some problems were identifiedin previous study

(Hansson, 2006):

- A deckhand hit by the hook in the head
- Person squeezed between moving containers
- A deckhand fall against a hose
- Person slip or twisted a foot
- Fall caused by slippery deck or obstacles
- Fall down the ladder
- Collision between vessel and installation.

Collisions and contacts were some of the most severe incidents recorded, while accidents on the deck during loading unloading at sea were one of the most frequent. Some improvements in the ves sel's design are identified, such as increasing the height of bulwarks or side walls to prevent water on deck, installing automated cargo securing system, and developing hose securing system. Some efforts in the operating procedures are also recognized, likeforbid 'cherry picking', the five-hundred meter safety zone restriction,voyage planning and no deckhand is allowed to help suspended cargo. A set of guidelines is published to ensure and improve the safety of offshore supply vessels operations

Participant motivation in experiment of emergency operating procedures

F. Song

Shanghai Nuclear Engineering Research & Design Institute,
Shanghai, China

S. Xu & Z.Z. Li

Department of Industrial Engineering, Tsinghua University,
Beijing, China

ABSTRACT

Operators in emergency response are often

subjected to high pressure and fear of accidents.

It is highly expected that in an emergency related

experimental study, such pressure and fear could

be simulated. However, this is very difficult since

participants of the experiment know well that

their performance will not cause any catastrophic

consequences. Except possibly introducing anxiety

and flurry, the pressure and fear would make the

operators more accountable and responsible and

thus would try their best effort in task perform

ance. It was hypothesized that participants could

be motivated to make their best effort during an

experiment, so that the experiment results would

more likely to represent human performance in

emergency response.

The objective of this study was to examine

whether motivation by performance-based pay

ment could improve the performance of partici

pants in the experiment of computerized EOPs of

Nuclear Power Plants (NPPs).

Totally nineteen participants were recruited to participate in the between-subjects experiment. They were arranged into two groups: fixed pay ment group (10) and performance-based payment group (9).

The experiment platform of the SGTR (Steam Generator Tube Rupture) procedure was devel oped by Microsoft Visual Basic™ and Microsoft Access™. Time pressure was applied and simu lated by using a clock at the up-right corner of the screen showing the left operation time of the cur rent step. Operation time and error for each step of the SGTR procedure were recorded automatically for later data analysis. Dependent variables include average procedure completion time and error rate. The participants were aware of their errors because of the termination of current trial, and could have a subjective feeling of their completion time, but no information on their overall performance and the corresponding payment were provided during the test. It is surprising that the performance, either error rate or completion time, under the performancebase payment method seemed to be even a little worse than the fixed payment method, although statistical analysis indicated that the differences were not significant. The standard deviations associated with the performance-based payment method were greater than those with the fixed payment method. One explanation to this phenomenon is that the group with the performance-based payment method might be distracted by considering the payment, and thus showed worse performance under the condition that there was certain time pressure. Motivation by performance-based payment did not show its supposed positive effect on improving the performance of the participants, but it seemed to cause the participants unable to concentrate their effort on performing the emergency operating procedure. This study may suggest the

application of time pressure and determination of suitable payment—to be good for the participants but not based on performance, in an emergency related human factors experimental study.

Pendulum shifts, context, error, and personal accountability

H.S. Blackman & O.V. Hester

Center for Advanced Energy Studies, Idaho National Laboratory (INL), ID, US

ABSTRACT

In recent years the quality of human performance causal investigations has drastically improved. A variety of processes, tools and techniques have been developed and applied across many indus tries. What has resulted is a balanced and deeper understanding of why a specific event occurred and why a given individual acted in a certain way. Prior to this advent, these analyses were primarily focused on who took what action and then simply remediating that individual—often through train ing, procedure modification and/or some form of punitive measure.

What was long overlooked was the contribu tion of the machine system, organization system, and specific situational context to the event itself. Today INL spends a great deal of effort studying these aspects of events to identify existing (Latent) Organizational Weaknesses (LOW), and to under

stand the context of the event itself, in order to fully appreciate what was in the mind of the person(s) involved. INL efforts to look at human error as a symptom that is systematically connected to features of people's tools, tasks, and operating environment has assisted it in progressing toward a culture where the reporting of events and near misses is more common, and individuals feel empowered and safe in doing so, ultimately resulting in better performance and safety for the organization. These efforts have also helped INL think about the issue of individual accountability and culpability in a new way that takes into account many of the situational and organization factors that influence human behavior—continually moving toward what has been termed a "just culture." Within a just culture, "an atmosphere of trust exists where employees are encouraged, even rewarded, for providing essential safety-related information—but in which they are also clear about where the line must be drawn between acceptable and unacceptable behavior." (Reason 1997).

INL emphasis on latent organizational weaknesses (LOWs) has created a new problem:

a tendency to attribute all undesired behaviors to LOWs; this "over correction" has unintended consequences. It has

led the organization away from the human component that includes personal accountability and understanding the intrinsic elements of why undesired behaviors occurred. This occurs when investigators explain “what” people failed to do or should have done without explaining why an individual did what they did. Investigators may stop short of asking those final “tough” questions and instead superficially apply tools and processes that lead to more antiseptic and easy answers. Further, it diminishes expectations for institutional honesty and accountability and inhibits organizational learning. Not every event or incident is due to a weakness in the organization; often, a lapse, omission, or error by one person or a very few people results in degradation of the safety envelope, process disruption, a near miss or even injury. Humans make errors, and a balanced accountability for those errors is a necessary part of a just culture. If a human error is mislabeled as a LOW, the resulting remedy potentially fails to address the true cause. Both safety and institutional honesty can be weakened as a result. The goal is to achieve a balance in understanding LOWs and the human component of events (including accountability) as the INL continues its shift from a culture of fear (where people are afraid to report due to unjust reprisal and action) to a reporting culture (where people are accountable and interested in making a positive difference—and want to report because information is handled correctly and the result benefits both the reporting individual and the organization). This paper discussed our model for understanding these interrelationships; the initiatives that were undertaken to improve overall performance. REFERENCE Reason, James. 1997. Managing the Risks of Organizational Accidents. Ashgate Publishing Company.

Quantitative retrospective analysis of CREAM in maritime operations

Z.L. Yang & J. Wang

Liverpool Logistics, Offshore and Marine (LOOM) Research Institute, Liverpool John Moores University, UK

ABSTRACT

Modern shipping activities are carried out via a

highly sophisticated man-machine system within

which technological, social and environmental fac

tors often contribute to the occurrence of human action failures. Due to the high risks caused by such failures, human reliability analysis (HRA) has always been a serious concern of maritime safety analysts. However, the problems of subjectivity and lack of data, together with the complexity of operator behaviour involved, have weakened the applicability of well-established HRA methods (i.e., Cognitive Reliability and Error Analysis Method (CREAM)) in the maritime context. The prospective quantification process of a Cognitive Reliability and Error Analysis Method (CREAM) (Hollnagel, 1998), normally producing an interval approximation analysis result, cannot provide a quantitative point estimate of the consequences of human performance on maritime system safety. This paper therefore develops a generic methodology in which the prospective analysis of CREAM is modified to facilitate the quantification of maritime human failures by effectively incorporating both fuzzy evidential reasoning and Bayesian inference logic. The kernels of the proposed framework are to use evidential reasoning to establish fuzzy IF-THEN rule bases with belief structures and to employ a Bayesian inference mechanism to aggre

gate all the rules associated with a seafarer's task for estimating its failure probability. To realise this aim, a five step HRA methodology is developed to include: 1. Construct a rule base to model the relations between the CPCs and four COCOMs. 2. Assign belief degrees to the four control modes. 3. Use BN to adjust CPC dependency. 4. Aggregate rules using Bayesian reasoning. 5. Validate the model developed. Consequently, the framework can be used to model the relationship between the nine Common Performance Conditions (CPCs) and the four control modes in the Contextual Control Model (COCOM) in a realistic and systematic way. The multiple-input multiple-output rule concept, together with evidential reasoning, makes estimation of human failure probabilities reasonable in a way of being sensitive to the minor changes of fuzzy input. It also makes it possible to realise the instant calculation of human failure probabilities in specific task analysis onboard ships. The advantages of the newly developed method are shown through the illustrative example of analysing an oil tanker COP shutdown scenario. The outcomes of this work can also provide safety engineers with a transparent tool to realise the instant estimation of human reliability performance for a specific scenario/task.

Tailoring the HEART technique for application in the rail industry

W.H. Gibson, C. Dennis, K. Thompson & A. Mills

RSSB, London, UK

B. Kirwan

EUROCONTROL, Bretigny, France

ABSTRACT

Human error is a key contributor to risk in both

existing and future railway systems. Human Reli

ability Assessment (HRA) can be used to assess

human performance and to better understand

the contribution of human performance to risk.

Human error quantification can be a critical ele

ment in HRA. One approach which continues to be used and adapted across industries is the Human Error Assessment and Reduction Technique (HEART). It has been identified that developing an understanding of how the HEART approach can support quantification in the rail context, would provide benefits in terms of more efficient, and greater consistency in, assessments. This approach was selected in preference to developing a new rail-specific quantification technique, as it means that there are less significant issues with technique validation. This initial project reported in this paper had a particular focus on train driver tasks, although the method is designed to be generic for rail tasks. The paper particularly focuses on the HEART Generic Task Types.

The review of Generic Task Types has aimed to define the HEART GTTs in the context of a generic model of human performance and train driver tasks. This process has led to the removal of some existing GTTs and addition of new GTTs. The EPC review has been based around grouping the EPCs into topic areas and reviewing the EPC set against performance shaping factors used in other techniques. Users will also be supported through the development of guidance on potential overlaps between EPCs, and between GTTs and EPCs, and fuller definitions and guidance for GTTs, EPCs and estimating the assessed proportion of affect. The revised approach will be presented to technique users as a

paper-based manual with an excel calculation sheet. In addition, guidance will be developed which aims to define the strengths and limitations of the approach and place it in the wider context of human reliability assessment. Detailed plans for delivery of this information to the GB industry will be developed based on consultation with industry stakeholders. Testing of the usability of the tool with users is also planned. Quantified risk assessment or probabilistic safety assessments, and the use of human reliability assessment are not mandated for the GB rail industry. There will therefore not be a mandated requirement for the tool to be used within the industry. However, human error quantification forms a component of a range of safety assessments, and the GB industry-wide safety risk model is a quantified risk assessment which includes human error probability data (www.safetyriskmodel.co.uk).

Task Analysis and modelling based on Human-Centred Design

approach in ATC work

S. Inoue & Hisae Aoyama

Air Traffic Management Department, Electronic Navigation Research Institute, Tokyo, Japan

K. Yamazaki

Department of Design, Chiba Institute of Technology, Chiba, Japan

K. Nakata

Informatics Research Centre, University of Reading, Reading, UK

K. Furuta

Department of Systems Innovation, The University of Tokyo, Tokyo, Japan

ABSTRACT

To accomplish the mission smoothly, we need to

have good cooperation with human partners and

artefacts in a complex systems. In particular, it

is a critical factor to establish good relationships between human partners and artefact systems.

This type of system is also the work of Air Traffic Control (ATC). The tasks involved in ATC make heavy demands on the information processing capacities of air traffic controllers. Air Traffic Controllers are expected to continue maintaining the safety of the air space and maintaining air traffic flow to run smoothly in such a complex systems. As the work and tasks of controllers become more complex and the volume and types of information required to carry out these tasks become increasingly larger and more complex, the need for systems that are designed to support controllers becomes greater. In this situation, the cognitive aspects of ATC have not yet been studied sufficiently, in particular with regard to teamwork settings, and no consistent measures for ATC performance assessment have been established either. Controller teams are presently in charge of ATC; it is expected that good team cooperation can contribute to reducing their workloads and preventing human error. Team cooperation processes, however, have not yet been understood well compared with individual cognitive processes. Thus, we need

to understand the details of the basic functions

of the air traffic controller tasks in the system,

in order to design more reliable interfaces and

training programs for the controllers. Moreover,

to be of use, supporting systems require an accu

rate model of the controller’s behaviour. In this

research, we focused on the task analysis of air

traffic controllers in actual en-route ATC in an experimental activity based on a Human-Centred Design approach. We discuss the method of design to develop a system of human consciousness, especially for Air Traffic Controllers. And then, we attempt to help a good understanding of the knowledge structure and logical relations of ATC expertise. Though the HCD process is defined with ISO13407 or ISO9241-210(2010) shown in Figure 1, in this paper, we try to consider the method of using the analysis technique based on the distributed cognition which is devised as a method of the analysis to understand the situation. In order to design the system that can assure system safety, enhance usability, and support human reliability in the future, the idea of HCD process can help a developer’s engineer for considering the feature in the control system operation and the intention of the controller. In this paper, firstly, we propose the observation survey technique that can obtain the result of the survey in which effectiveness is high in the process of the human centred design that can be simply executed compared with a conventional technique. Moreover, we attempt to analyze and model interactions that take place in current en route ATC work based on distributed cognition. Distributed cognition is one of the analysis methods in ethnomethodology that serves as a framework for understanding interactions between people and technology so as to inform the design of interactive systems (Hollan et al., 2000). We have taken the activity of a cooperative team of en route controllers as the unit of analysis from cognitive process perspective. We discuss the application of ethnographical analysis in en route controllers’ work as team, and report on findings from ethnographical analysis.

Hollan, J., Hutchins, E. & Kirsh, D. 2000. Distributed

Cognition, ACM Trans. on Computer-Human Inter

action, Vol. 7 (2), 174–196. ISO 9241-210:2010. Ergonomics of human system interaction - Part 210: Human-centred design for interactive systems (formerly known as 13407), International Organization for Standardization (ISO), Switzerland.

Teamwork competencies required by members of integrated operations

teams in the petroleum industry

A.B. Skjerve & G. Rindahl

Institute for Energy Technology, Halden, Norway

ABSTRACT

Introduction of the operational concept Integrated

Operation (IO) by petroleum companies operating

on the Norwegian Continental Shelf implies an

increased use of distributed teams (IO teams) in

operation of petroleum installations.

To develop teamwork training programs for

members of IO teams, it is necessary to understand

what teamwork competencies IO team members

need to work proficiently as a team. This paper

accounts for the development of the MAITEC

model. The model comprises what is suggested to

be ten main attributes of IO teamwork competence:

IO-mindset, IO team-technology competence, team

leadership, inter-personal relations, inter-positional

resources, personal resources, communication,

shared situation awareness, mutual trust, and deci

sion making (see Figure 1).

These ten teamwork competencies are taken to

jointly constitute the central part of the teamwork

competence, i.e., the skills, knowledge and attitudes, required to work in an IO team. The teamwork competence attributes are distributed across four layers, centering on the attribute decision making. The model assumes that the attributes at the outer layers are needed to achieve practical excellence in an IO setting with respect to the attributes located at the inner layers. The MAITEC model was developed based on a literature survey. The survey comprised 30 papers on co-located teamwork, distributed teamwork, and/or teamwork in offshore operation. It was structured in three parts. The first part aimed at identifying generic attributes of teamwork competence, and was based, mainly, on studies of co-located teams. The second part focused on establishing attributes of teamwork competence based on studies of distributed teams. The last part aimed at understanding the attributes of teamwork competence required in offshore operations. The content of the MAITEC model was assessed in an empirical study. The research questions were: 1) Do the attributes of teamwork competence contained in the MAITEC model adequately cover the competencies observed in practice? 2) Are the inter-relationships between the attributes of IO teamwork competence sufficiently pronounced to validly use a layered structure in the MAITEC model? The study was based on observations of 19 morning status meetings in an IO team, across the period 2008–2010. The outcome of the empirical study did not disprove the significance of the attributes contained in the MAITEC model, nor did they indicate that the layered structure was not valid. The next step will be to further assess the MAITEC model based on date obtained in other teamwork settings of IO teams.
REFERENCE Skjerve, A.B. 2009. IO Teamwork Training. In: A.B. Skjerve & M. Kaarstad (eds.), Building Safety. Literature Surveys of Work Packages 2 and 3, IFE/HR/F2009/1388, 94–143. Halden: Institute for Energy Technology.

Figure 1. The MAITEC model of the main attributes

of IO teamwork competence (Skjerve, 2009).

The development and application of CARA—a HRA tool

for Air Traffic Management systems

B. Kirwan & A. Kilner

Eurocontrol, Bretigny, France

W.H. Gibson

RSSB, London, UK

D. Piccione

FAA, US

M. Sawyer

TASC Inc, Washington DC, US

ABSTRACT

Air Traffic Management (ATM) is a highly human-centred operation, with air traffic controllers handling live traffic every day. It is also a very safe industry, with a very low accident rate. In the coming decade there will be significant developments in ATM infrastructure and automation, in an effort to improve efficiency and capacity given the anticipated growth rate in Europe and the US in air traffic. It is essential that such high human performance and safety levels are maintained. This paper documents the CARA HRA approach for the ATM industry.

This paper charts the development and application of a Human Reliability Assessment (HRA) tool called CARA (Controller Action Reliability

Assessment). CARA is thematically based on the

HEART and NARA HRA approaches, rendered

into the ATM context and populated with data

from the air traffic industry, both from live opera

tions and high fidelity human-in-the-loop simula

tion studies. The tool has been applied to several

early safety cases, and has been found to be useful. At present the tool supplants the widespread use of engineering judgement, and the avoidance of quantifying the human element in many system change proposals, and so offers an advance in safety capability for the industry. CARA has recently been proposed as a way forward in the EUROCONTROL/FAA Action Plan 15 White Paper on Human Performance and Safety, which has recently received tacit endorsement by the European Aviation Safety Agency (EASA). The CARA approach is already documented and exists on the web. http://www.thinkresearch.co.uk/HRA/ index.html The paper describes CARA and the data underpinning it, as well as early applications in both Europe and the USA, the first an aircraft landing (‘Approach’) study, the second data communications for arrival route and taxiway instructions, showing the types of insights gained and how they help designers. The case for using CARA, and for it becoming part of the safety risk management ‘machinery, as well as further development needs, are outlined in the paper.

The meaning of human performance data observed from simulator

studies on human reliability analysis

Jinkyun Park & Wondea Jung

Korea Atomic Energy Research Institute, Daejeon, Republic of Korea

ABSTRACT

It is well perceived that several key factors are

crucial in securing the safety of socio-technical sys

tems, such as Nuclear Power Plants (NPPs).

Of them, the importance of human performance related problems has been demonstrated over the past several decades through well publicized events (Forester et al., 2009). Accordingly, extensive effort has been continuously spent on understanding why the performance of human operators deviates from certain expected level (i.e., human error). In the case of NPPs, one of the main activities to answer this question is to carry out a Human Reliability Analysis (HRA).

Unfortunately, although there are significant benefits in conducting HRA, many people have criticized the quality of HRA results because of a lack of available data (Boring 2009; NEA 2009). Subsequently, in many countries, the use of full scope simulators has been regarded as one of the most cost- and effort-effective alternatives to unravel this problem. In other words, the full-scope simulator is very useful tool for understanding human behaviors that can result in human per formance related problems, since it allows HRA practitioners to systematically observe human behaviors in coping with a hypothetical accident (Boring 2009, Forester et al., 2009, NEA 2009). Thus, it is possible to anticipate that a set of serv

iceable data or insights that are indispensable for conducting HRA can be elicited from simulators. However, the use of human performance data observed from simulators is still careful because

The right HRA model for the right HRA application

V. Fauchille

IRSN, Fontenay-aux-Roses, France

ABSTRACT

In order to have its own expertise, IRSN develops level 1 and level 2 PSA models for each reactor series operated by the French utility EDF. Human Reliability Analysis (HRA) data are obtained from two HRA methods: PANAME in case of level 1 PSAs and HORAAM in case of level 2 PSAs.

- PANAME evaluates the probability of failure of an operating team that carries out Emergency Operating Procedures (EOPs);
- HORAAM evaluates the probability of failure of the emergency response organization on the basis of operating guides which calls for actions once certain criteria are reached indicating core damaged.

The article briefly presents both HRA methods and highlights the strong points of each of them. Afterwards, the article focuses on level 2 PSAs

and the Severe Accident Management Guide (SAMG).

After core melt, there are two types of human actions:

- “Immediate actions” that can be performed immediately because they don’t need the expertise of the national emergency response organization. Mainly these actions consist in a confirmation of corrective actions already defined in the EOPs. The quick execution of these actions may reduce the consequences of the accident. To implement these actions, operators only need the permission of the Local Management Command Center.
- “Delayed actions” that need the expertise of the National Emergency Organization. The implementation of delayed actions requires somehow a risk analysis to draw the benefits and the drawbacks of the considered actions.

The main difference between SAMG immediate actions and SAMG delayed actions is a need for expertise.

HORAAM predicts Human Error Probabilities (HEPs) given a number of factors which affect human and organizational reliability:

- the time available,

Three Human Reliability Analyses under the MERMOS light

P. Le Bot & H. Pesme

EDF R&D, France

ABSTRACT

In the recent ongoing works about Human Reliability Analysis (HRA), the International HRA Empirical study is a major step. This OECD project has been performed with Halden laboratory and fourteen HRA teams from several countries. EDF R&D's team was one of the French contributions with the MERMOS HRA method.

The goal was "to develop an empirically-based understanding of the performance, strengths, and weaknesses of the methods". As contributors to the study, we have learnt a lot of lessons about our own method and about the other HRA methods.

Since the study was focused on the comparison of different HRA analyses of the same Human Failure Events (HFE), it allowed us to better understand the theoretical and practical specificities of the other methods.

The goal of this paper is to attempt an exercise of comparison of the analyses with four HRA methods: MERMOS, CESA-Q and CBDT

THERP. CESA-Q has been used by the Paul Scherrer Institute's team (from Switzerland) and CBDT-THERP has been used by the EPRI team (from USA). We try to highlight the different assumptions and characteristics of modelling of the three methods by rewriting the CESA and CBDT-THERP analyses of one HFE of the International Study within the form and structure of MERMOS analyses.

Indeed we argue that the MERMOS analyses structure allows to describe the other methods analyses since with the structure of "failure scenarios" it has a larger level of modelling and less hypotheses of modelling. The exercise shows the strengths and the weaknesses of each method in the same light. It allows to illustrate the differences between first generation HRA methods as THERP and second generation HRA methods as MERMOS and CESA-Q, regarding the way the different methods use the input data, the assumption they make about human failure and why they differ or not in their quantification. The conclusion is that this transposition of the CESA and the CBDT-THERP analyses into the MERMOS frame is feasible and is a great help indeed to compare these methods, regarding the concepts and the quantification process. One important result is hat for these four methods we can describe several independent "scenarios" of failure even if the description is more or less precise depending on each method. Then for the four methods the HEP (probability of HFE failure) is the sum of the probabilities of all these quantified failure scenarios. We think that this presentation of results through failure scenarios is an explicit way of describing failure. Another result is that

this exercise gives us good cues to improve MERMOS: by adding a PSF item in the frame of the MERMOS structure we have a good frame to be compared to many other HRA methods, which are based on PSFs. We think that the specificity of the MERMOS failure scenarios is an advantage because it explicits how PSF can combine to lead to failure. REFERENCE Lois, E., Dang, V.N., Forester, J.A., Broberg, H., Massaiu, S., Hildebrandt, M., Braarud, P.Ø., Parry, G., Julius, J., Boring, R., Männistö, I. & Bye, A. International HRA Empirical Study—Phase 1 Report: Description of Overall Approach and Pilot Phase Results from Comparing HRA Methods to Simulator Data, HWR-844, Halden Reactor Project, Halden, Norway and NUREG/IA-0216, Vol. 1., U.S. Nuclear Regulatory Commission, Washington, DC, (2009).

Towards a unified human reliability model

P.A. Baziuk, S. Rivera & J. Nuñez Mc Leod

Instituto CEDIAC, Universidad Nacional de Cuyo, Mendoza, Argentina

ABSTRACT

The two fields included in the study of human

reliability (human behavioral science and engineer

ing) have not been integrated sufficiently. Follow

ing this line, this article works towards a unification

of the present models of human reliability, includ

ing the cognitive aspects and the last conception of

the human cognition cycle.

In the attempt to integrate the several overlap

ping models require that each of the models be

appropriately adjusted. The adjustments done are:

a. For error modes models (commission and

omission errors): are include in the fail of some

of the three process (sensorial, perceptive or

cognitive).

b. For error levels models (input, mediation and output errors): are considered as cuts in the conduct cycle, because of internal or external factors.

c. For skill-, rules- and knowledge-based behavior model: is include in the different activations and responses of the conduct cycle.

d. For slips, lapses, mistakes and violations model: lapses are considered as a fail in the cognitive process, slips can occur by a fail of any of the three process and mistakes are a fail of the cognitive process.

The information included in the unified model is:

a. The concept of limited cognitive resources

b. The concept of cycle process

c. The concept of supervisory attention system

d. The concept of problem space in problem solving

e. The knowledge from expert judgment-based models

Therefore, human error can be defined as a cut of the cycle process of behavior, produced by a dif ference between the cognitive resources required

by the task and the cognitive resources available

A complete probabilistic spare parts stock model under uncertainty

J. Lonchampt & K. Fessart

EDF R&D Division, Chatou, France

ABSTRACT

The classic way to optimize the number of spare parts for a population of components is to consider the failures as a Poisson process (Hadley & Whitin, 1963) and to calculate the number of spare parts that minimizes the costs or maximizes the Net Present Value of supplying spares. This approach has two weaknesses in the case of spare parts for major components:

1. The Poisson process for modelling failures assumes that the components are not experiencing ageing and that the failure rate is constant. It also assumes that the transient behaviour of the spare parts stocks, may be ignored. The fact to ignore the transient state in the optimization of the number of spares may lead to some wrong decision such as an oversized stock that generates useless holding costs or purchasing costs or an undersized stock that may generate unavailability.

2. One of the specificity of major maintenance tasks is that they are unlikely to be carried out several times during a plant life-time, that is to say the probabilities of the events that would lead to maintenance are very low. Moreover the failure consequences are often high. This is why mean indicators may not be sufficient as they often don’t represent the residual risk. The fact to only consider mean values of indica tors is in some case not sufficient for decision making, as a mean positive value may hide the fact that it is most probable that the indicator is negative. This is why it is important to provide complete probabilistic distributions in order to help decision making taking into account risks through enhanced indicators, such as the stand ard deviation, the probability that the indicator is negative (therefore making a strategy non profitable) …

For these reasons EDF R&D developed a

A framework for selection of test method for safety critical valves

E.B. Abrahamsen

University of Stavanger, Stavanger, Norway

W. Røed

Proactima AS, Norway

ABSTRACT

In the European oil and gas industry hydrocarbons are transported long distances in pipelines. In order to reduce the severity of potential hydrocarbon leaks to the atmosphere safety critical valves are normally installed. It is vital that such valves close on demand, and to assure this, the valves are nor mally tested periodically. Several test methods exist, and the choice of test method should be made in the test planning phase. The alternative methods test different properties of the valve in terms of valve functions and associated failure modes. The potential consequences of performing the test, for example in terms of production loss and costs, may also vary greatly from one test method to the next. Also the reliability of the test varies greatly between the test methods. Additionally, some test methods introduce emission of greenhouse gases to the atmosphere and challenges with regard to the safety of the personnel performing the test. Due to the above, the ideal test method is the one that balances the gained information by carrying out the test with the potential negative consequences of performing the test. To obtain this balance, the test method decision should be based on a structured approach. In this paper we suggest a qualitative framework that can support test method decisions for safety critical valves. The main focus of the framework is large hydrocarbon pipeline inventories. The framework is, however, general and can be adapted to other hydrocarbon systems onshore and offshore as well.

A maintenance strategy for systems subject to competing failure modes

due to multiple internal defects and external shocks

I.T. Castro

Department of Mathematics, University of Extremadura, Spain

ABSTRACT

The deterioration of a system is the irreversible accumulation of damage through of its lifetime. A degradation relevant stochastic model is the threshold model where the system fails whenever its degradation level reaches a critical threshold. Besides degradation failures, systems may also be subjected to external shocks which may lead to failure. Lemoine and Wenocur may have been the first to consider these two competing causes of failures and these models are called Degradation Threshold-Shock models (DTS-models).

Frequently, in the deteriorating systems litera ture, the degradation of the system is an unique measure modeled as a stochastic process. Castro et al., and Kuniewski et al., analyzed a system subject to multiple defects. Each defect follows a degradation process and the system fails when the deterioration of one of these defects exceeds a fail ure threshold.

This paper analyzes a maintenance policy for a DTS model assuming the system is subject to

multiple internal defects. Internal defects initiate following a Non-Homogeneous Poisson Process (NHPP). Gamma processes model the degrada tion of each defect. External shocks arrive to the system and they are catastrophic with probability 1 – p and non-catastrophic with probability p.

An age-based maintenance strategy is developed in this presentation. Under this strategy, a preven tive replacement is performed when the age of the system exceeds the value T. Corrective replace ments are performed after a degradation failure or after a catastrophic shock. Minimal repairs are performed after a non-catastrophic failure. Costs are associated with the different maintenance actions and the objective is to determine an value of T that minimizes the expected cost rate. Under the assumptions of nondecreasing intensities for the arrival of defects and external shocks, the opti mal value of T is obtained analytically.

Figure 1 shows a simulation of the expected cost rate versus T for a set of parameters. Inter nal defects arrive following a NHPP of intensity

A new modeling framework of component degradation

P. Baraldi, A. Balestrero & M. Compare
Energy Department, Politecnico di Milano, Italy

E. Zio

Energy Department, Politecnico di Milano, Italy

Ecole Central Paris-Supelec, France

L. Benetrix & A. Despujols

EDF R&D, Chatou, France

ABSTRACT

In this work, we address the problem of building a model in support of maintenance optimization, when the only available information comes from experts. This situation, very common in indus trial contexts, calls for the development of novel modeling solutions. In fact, the information elic ited from experts is subjective, qualitative and very often in implicit form; thus, it needs to be properly interpreted, represented and propagated through the model. To do this, the present work resorts to the theoretical framework of fuzzy logic, due to its capability of dealing with imprecise variables and linguistic statements.

From the modeling point of view, we resort to the concept of ‘effective age’ to take into account the influence of the environment on the compo nent degradation process, which may evolve faster or slower than chronological time in adverse or favorable working conditions, respectively. The

effective age is here considered alike a physical

variable that is representative of the health state

of the component, in the same way as the crack

length may be used to indicate the degradation

state of a mechanical component. Under this

concept, the objective of degradation modeling

becomes the identification of the relations between the operating conditions of the component and its effective age. On the other side, the practical view undertaken in this work of building a degradation model based only on the expert's information requires that such model gives due account to the two following modeling constraints: 1. The degradation process is a discrete-states process, in recognition of the fact that experts are more familiar with this way of thinking of the degradation mechanisms. 2. There is no stochastic model available to describe the degradation behavior in normal operating conditions. The degradation model is then embedded in a Monte Carlo scheme, in which a large number of trials or histories (i.e., random walks of the system from one configuration to another) are simulated. Averaging all the relevant quantities upon the entire mission time, we evaluate a set of useful indicators (i.e., the mean unavailability of the component) which constitute the basis to assess the performance of a given maintenance policy. Finally, we show how the proposed methodology can be applied in practice, by way of a real case study dealing with a medium voltage test network.

A Petri net model of aircraft maintenance scheduling

D.R. Prescott

University of Nottingham, Nottingham, UK

ABSTRACT

This paper addresses the Time-Limited Dis

patch (TLD) of aircraft (FAA Memo 2001, SAE

ARP5107 2005). TLD is a maintenance methodol

ogy that allows aircraft dispatch with known faults

present in the engine control systems for a limited period of time, see Figure 1. This allows aircraft operators to take advantage of the inherent reli ability of system components and utilise system redundancy to enable maintenance to be scheduled at such a time that maintenance disruption can be minimise.

Important aspects of TLD and the associated certification requirements are discussed. A Petri Net (PN) model of the application of TLD to a sys tem is presented, which builds on work presented by Prescott (2011). PN provide a flexible, graphi cal and mathematical framework for dynamic sys tem modelling (Murata 1989, Schneeweiss 1999). The developed model is modular, with modules which relate to different aspects of processes relat ing to the application of TLD to a system, such as component failure and repair, maintenance scheduling in the event of revealed and unrevealed failures and maintenance after system failure. The PN model addresses one of the key disadvantages of previously-developed MC simulation models (Prescott & Andrews 2006, 2008) because it is eas

Figure 1. TLD—a fault occurs at t 1 and dispatch is allowed with that fault until t 2 . t 1 t 2 t dispatch

interval

A simulation model for complex repairable systems with inter component dependencies and three types of component failures

J. Malinowski

Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

ABSTRACT

This paper presents an attempt to construct a possibly general framework for simulating reliabil ity behavior of complex systems. The concept stems from the research carried out by the author on the reliability of commodity transportation networks (e.g. power distribution networks), but it can also be applied to other types of systems. So far many simulation models have been designed for complex systems reliability analysis. However, most of them have drawbacks which include: restrictive assump tions (e.g. components independence, exponential times-to-failure and/or times-to-repair, repairs started immediately after failures' occurrences), narrow applicability (only to special classes of systems), or poor correspondence to real-world systems.

The author sought to construct a reliability model free of those shortcomings. This model is built on several basic assumptions that make it

close to reality. First, failures of the system's com
ponents have impact on the functioning of other
components, thus inter-component dependencies
exist within the system. Second, three types of
failures are distinguished—intrinsic (due to a com
ponent's wear), propagated (induced by other com
ponents' failures), and caused by external factors.
Third, failed components are replaced or repaired
by a limited maintenance personnel, thus it may
happen that a maintenance action does not start
immediately after a failure occurs, which makes
it necessary to manage a repair queue. Fourth,
functioning components are under (variable) load
which causes their wear. The wear level of a com
ponent influences its failure and repair rates.
For the purpose of mathematical description
the components are assigned two types of states—

reliability (binary numbers) and operational (integer numbers). The system's functioning is described by two vector-valued stochastic processes, X = {X 1 (t), …, X m (t)} and Y = {Y 1 (t), …, Y m (t)}, which represent the evolution of reliability and operational states of individual components over time, where m is the number of all components. The reliability state 1 represents an operable component, 0 – a failed one. If a component is operable then its operational state is positive and it specifies the component's load. If a component is failed then its operational state is non-positive and it specifies the component's place in the repair queue. The load on an operable component is assumed to depend on other components' reliability states. Over time, a component accumulates wear which depends on the

component's load history. Thus X i (t) = 1 if the i-th component is operable at t, otherwise X i (t) = 0. Furthermore, Y i (t) > 0 if X i (t) = 1, where Y i (t) is a function of X j (t), j≠i, while Y i (t) = -q if X i (t) = 0, q being the i-th component's place in the repair queue, where q = 0 for a component currently under repair. Two types of repair are distinguished—minimal and complete. A component after a complete repair is as good as new, i.e., it has zero wear. A minimal repair does not reduce a component's wear, i.e. the wear remains as it was just before the failure occurred. Modeling failure-repair process with the use of two types of states—reliability and operational—is the author's own concept which significantly facilitates the simulation of that process. This is because Y is a deterministic function of X whose evolution is fairly simple to simulate. In the Appendix two illustrative examples are given. The first one shows how the processes X and Y evolve in case of a simple system. The second— how data obtained by simulation are used to estimate certain reliability parameters of a power distribution network.

A study of the effect of imperfect inspection on the efficacy

of maintenance for a non-repairable system with a defective state

M.D. Berrade

Departamento de Métodos Estadísticos, Universidad de Zaragoza, Zaragoza, Spain

P.A. Scarf

Salford Business School, University of Salford, Salford, Manchester, UK

C.A.V. Cavalcante

Department of Production Engineering, Federal University of Pernambuco, Recife, Brazil

ABSTRACT

In this paper we consider a repairable system that

is subject to imperfect inspection. Our aim is to

explore the efficacy of inspection in circumstances

in which it is subject to error. The system may be in one of three states: good, defective or failed, and the system is operational while in the defective state. The purpose of inspection is to prevent failure by allowing the replacement of the system while in the defective phase. However, if inspection is poorly executed then inspection may not be economic. Failure is detected as soon as it occurs. We present a model in which the system undergoes inspections at instants kT, k = 1, 2, …,M to detect if it has entered into the defective state. If so, the system is replaced by a new one with a cost c_m. If the system fails, a cost c_r, with $c_m << c_r$, is incurred. In addition false positive and false negative inspection can occur. A false positive occurs when the inspection says the system is defective when in fact it is good. A false negative occurs when the inspection says the system is good when in fact it is defective. In the latter case, a failure can subsequently occur and such a failure would be due to the poor quality of inspection. In this paper we assume that there is no opportunity to gain other information apart from that derived directly from the inspection and thus a false positive leads to replacement of the system

with cost c m . The maintenance policy is completed

with a preventive replacement at MT with cost c m

provided that at an earlier moment there has not

been a false alarm, or a failure, detection of the

Adaptive condition-based maintenance models for deteriorating

systems operating under variable environment and indirect condition

monitoring

K.T. Huynh, A. Barros & C. Bérenguer

Institut Charles Delaunay and STMR UMR CNRS 6279—Université de technologie de Troyes, Troyes, France

ABSTRACT

With the development of engineering structures,

maintenance operations play an important role

in efforts to improve the durability, reliability and

maintainability of industrial systems. The dis

semination and the expansion of instrumentation

techniques and sensor technologies impulse the

integrating of diversified monitoring information

in describing the system health and providing reli

able condition-based maintenance decisions. The

present paper deals with the efficient use of differ

ent types of covariate information in modeling and

optimising condition-based maintenance policies

for a deteriorating system operating under variable

environment.

Specifically, we aims to build a general degradation/measure model for a system subject to fatigue crack growth phenomenon. The degrada tion model of crack growth is basically described by a deterministic physical law of Paris-Ergodan, and then the randomness is incorporated into the model to preserve the stochastic nature of deg radation process (Cadini et al., 2009). Since the system operates under variable environment, the speed and variance of crack growth is driven by environment states (i.e., external covariates which can be directly observable with reasonable accu racy). Moreover, the crack depth is considered to be hidden and can be only accessed through inter nal covariates which are diagnostic results of an indirect non-destructive inspection by ultrasonic technique. Such a model can describe most realis tic aspects of single-unit systems operating under variables environment: physical characteristics of degradation phenomenon, relation among the real degradation and covariates (internal or external), as well as the nature of measurement approaches (direct or indirect). This model is therefore hope fully realistic, and offers a good case study for dis cussion about the relevance of different types of

monitoring information in maintenance decision

making.

In the framework of the system under consider

An optimal periodic preventive maintenance policy of a deteriorating

system subject to a bivariate state process

R. Ahmadi & M. Newby

School of Engineering and Mathematical Sciences, City University, London, UK

ABSTRACT

In this paper we present a new approach to

preventive maintenance policy for a stochastically

deteriorating system which is subject to repair

and maintenance. The failure state of the system

is determined by the failure probability measure described by a general stochastic

process (damage process) X with monotone paths

and a virtual age process V induced by repair. The

structure of the optimal maintenance strategy is

formed under periodic inspection policy. The dam

age state of the system is revealed by inspections

at periodic times. At inspection times the deci

sion maker with respect to the failure state proc

ess R t V(,X) and the decision thresholds § r , § f that

respectively refer to the preventive partial repair

and replacement rule has disposition to perform

a repair. The repair action updates the virtual age

of the system: the virtual age process V is adjusted

(imperfect repair), left unchanged (minimal repair)

or reset to that of a completely restored system

(perfect repair).

The critical threshold § r is used as definition of

partial repair action. If the system state process

R t

V(,X) crosses the boundary § r a partial repair is

made. The acceptance performance of the process

is limited by the critical level § f , (0 < § r < § f < 1). The

threshold § f is the level at which failure and replace

ment occur. The replacement action (renewal)

is determined by the first hitting time to the fail

ure threshold § f . The problem is to minimize the

long-run average cost subject to the system param

eters given periodic inspection policy. Because the

Application of RFMEA to risk analysis of maintenance

of electric facilities

M. Ko & T. Nishikawa

Toshiba Corporation Research & Development Center, Japan

ABSTRACT

It is often difficult to detect risks with the severe

losses which rarely occur by evaluating RPN

(Risk Priority Number) with FMEA or expected

loss with FMECA. Risk Failure Mode and Effect

Analysis (RFMEA) is an FMEA which is added

the function to evaluate such a risk. In this study,

we applied RFMEA to risk analysis of mainte

nance of electric facilities, and we identified high

risk tasks in Maintenance process.

Maintenance process is divided into 5 sub proc

esses, which are Order Acceptance, Schedule Plan

ning, Preparation of Manuals, Field Work, and

Reporting. From a result of risk analysis, we found

that over 80% of high risk failure modes were listed

in the Schedule Planning and Field work. And the

number of high risk failure mode of Schedule

Planning was as same as that of Field work while

both process had almost same number of tasks.

This means the Schedule Planning has high risk

tasks more than others.

In RFMEA, there are 4 parameters for risk cal

culation. The explanations of each parameter are

below.

Occurrence : The number of failures in a predetermined
period.

Detectability : According to the conditional probability
of the failure affecting the equipment or the workers,
given the occurrence of the failure.

Crisis Rate : According to the conditional probability of

the worst-case scenario, given the occurrence of the failure affecting the equipment or the workers.

Combined representation of coupling effects in maintenance processes of complex engineering systems

V. Volovoi & R. Valenzuela Vega

School of Aerospace Engineering, Georgia Institute of Technology, Atlanta, GA, US

ABSTRACT

Modern engineering systems consist of thousands of components; developing a coordinated maintenance policy for such systems presents a challenge from the complexity perspective due to the coupling among individual maintenance schedules for each component. The focus of this paper is on opportunistic (economic) maintenance and induced failure, as both of these coupling mechanisms are caused by competing risk phenomena. Modeling the maintenance process of an individual component, even if it includes modern condition-based considerations, can be described by a relatively small number of distinct states. In contrast, creating a system level model that captures all relevant coupling leads to a state-space explosion; an implementation of such models is either not feasible at all or very expensive. To address this issue, the present paper explores the idea of developing component

level models that incorporate the aggregate effects of other components by providing a compact sta tistical representation of the combined influence of all other system components on a given compo nent. This approach is analogous to the mean-field theory used in physics to avoid explicit description of pair-wise interactions. An analytical method based on asymptotic considerations is developed for combining effects of multiple components into a single Weibull distribution (inspections intervals are assumed to be smaller than the Weibull scale). Specifically, so-called “winning ratio” γ parameter is introduced that measures the odds that one of the components fail first within an interval of interest (given that both components fail during this interval). It is shown that in the practical range of interest this parameter shows very little sensitiv ity with respect to the scale of Weibull distribution (see Figure 1) In fact, it tends to a simple ratio determined by the shape parameters of Weibull distributions γ = ß 1 /(ß 1 + ß 2). This enables to evaluate a “weighted average” of multiple ratios when a component competes with many components, and select a matching Weibull shape parameter of the opportunity distribution. Finally, the scale parameter for the opportunity distribution is evaluated based on the total changes of failure during that interval. The accuracy of this approach was demonstrated for representing the combined effect of Weibull distributions. In particular,

it is shown that the proposed method provides a superior match to the combined distribution in the relevant time range as compared to standard methods of approximating a distribution (e.g., matching moments or maximum likelihood). The resulting approximation of the targeted function does not provide a good global match for all the range, but instead targets the left tail of the distribution, which is the most relevant for the realistic maintenance scenarios. It was further shown that a combination of lognormal distribution can be well approximated by a Weibull distribution as well. Figure 1. Scale sensitivity for race ratio γ when the first component follows Weibull distribution with shape ß = 2 and scale θ = 5 for different shape values. Interval of interest is unity. 0 2 4 6 8 10 0.0 0.2 0.4 0.6 0.8 1.0 γ θ β=0.5 β=1.0 β=2.0

Developments of time dependencies modelling concepts

T. Nowakowski & S. Werbińska-Wojciechowska

Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

One of the concepts which provide useful means

of modelling the effect of periodic inspections on

the failure rate of repairable technical systems is

a delay time concept, developed by Christer et al.,

see e.g. (Christer 1982, Christer & Waller 1984a,

Christer & Waller 1984b).

Delay-time models can be used for decision

making, for example choosing the optimal main

tenance and inspection interval with minimization

of cost or system downtime.

The delay time concept defines a two-stage

process for a component. First, a fault which has

developed in the system becoming visible at time

u from new with probability density function, pdf g(u), if an inspection is carried out at that time. If the fault is not attended to, the faulty component fails after some further interval h which is called the delay time of the fault and is described by probability density function, pdf f(h) (Fig. 1). During period h there is an opportunity to identify and prevent failure.

Once these two distributions are known, there is possible to model the reliability, operating costs and availability. The variables u and h depends upon the inspection technique adopted, see e.g. (Christer & Waller 1984a, Christer & Waller 1984b).

Presented paper is organized as follows: in the

Figure 1. Time-delay modelling concept.

Dynamic grouping maintenance strategy with time limited opportunities

Phuc Do Van, Florent Brissaud, Anne Barros & Christophe Bérenguer

Troyes University of Technology, Institut Charles Delaunay & UMR CNRS STMR, Troyes, France

Keomany Bouvard

Volvo Technology, Lyon, France

ABSTRACT

In the framework of grouping maintenance strategies for multi-component systems with

positive economic dependence which implies that combining maintenance activities is cheaper than performing maintenance on components separately, a major challenge of the maintenance optimisation consists in joining the stochastic processes regarding to the components (time-dependent probabilities of failure) with the combinatorial problems regarding to the grouping of maintenance activities. While a long term or infinite planning horizon can be assumed to solve this problem in case of stable situations, dynamic models have been introduced in order to change the planning rules according to short-term information (e.g., failures and varying deterioration of components), using a rolling (finite) horizon approach (Wildeman, Dekker & Smit 1997). This approach is however applicable only when maintenance durations are neglected. From a practical point of view, the system may be stopped during maintenance of its components, maintenance durations should therefore take into account, especially when the system unavailability cost rate is expensive. Moreover, each component is assumed to be preventively maintained only one time within the scheduling interval. This assumption seems to be not relevant since a system may be

composed of different components with different life time cycles, maintenance frequencies of com ponents are thus different. For example, engine oil has to change more frequently than driving belt on a heavy vehicle. The first objective of this paper is to develop the rolling horizon approach by tak ing into account both the preventive maintenance durations and the occurrences of maintenance operations in the considered scheduling horizon. Moreover, in presence of opportunities with limited durations in which some maintenance activities could be executed with reduced mainte

Dynamic maintenance requirements analysis in asset management

R.A. Dwight & P. Gordon

University of Wollongong, Wollongong, Australia

P.A. Scarf

University of Salford, Salford, UK

ABSTRACT

In this paper we propose that maintenance requirements analysis should be considered in the context of a dynamic business environment. Consequently, maintenance requirements analysis must be designed to adapt to changing asset cir cumstances. Furthermore, this adaptation should

be multi-dimensional. In one dimension a review should be adapted to events in the life of the asset; that is, there should be an appropriate review of the maintenance program in response to the changing circumstances of an asset. In another, second dimension, the review for an asset should be adapted to the resources available in the organi zation for maintenance planning; that is, there should exist within the organization flexibility to choose the scope and the depth of the analysis in the review. Yet a further, third dimension is infor mation available to conduct the review.

While the notion of a dynamic review process is not new, other review processes, for example that advocated by IEC 60300-3-11 presuppose that a formulaic approach to the analysis has previously been conducted and to a large extent should be repeated. Our suggestion is that the approach must be tailored to all of the dimensions set out here. Furthermore, in the first and third dimensions, an organization should have in place a system that triggers a review of the maintenance program for an asset as events in the life of the asset occur. Typical events in the life of an asset that would trigger a review are: acquisition; installation and

testing/trials; modification; end of warranty; the

outsourcing of maintenance; switch to in-house

maintenance; accident findings that implicate

maintenance; repeat failures that implicate mainte

nance; new maintenance technique available; new

resources available for maintenance; downgrade;

re-deployment; retirement; cannibalization; scrap

ping. Typically, such events will not occur over time

with a fixed frequency. Periodic review, say every n

years, may therefore not be ideal. The decisions about when to review and how much resource to allocate to a review might be formalized hierarchically within a decision tree. This would prioritize high value assets for which there is scope to change maintenance practice and for which information exists as a basis for a thorough review. Otherwise one would advocate a lighter touch. Statutory requirements, for example, may mean there is little opportunity to modify inspection frequency. Also, documentation of changes to the maintenance requirements needs to be mandated and based on updates to an existing master document. Our ideas are put forward understanding that normal logic and some standard practices may go some way to satisfying our criteria for a sensible approach to maintenance program review. Equally it is observed from the literature and also from practice that too often a laborious and slavish adherence to standardized approaches to maintenance requirements analysis persists and mitigates against the potential improvement to maintenance programs that would be achieved by focusing efforts on the appropriate application of the basic logic of maintenance requirements analysis to the assets that would benefit from such detailed attention. Conversely ad-hoc reviews driven by ‘kneejerk’ reactions to calamitous events should invoke both the logic of maintenance requirements analysis and be recorded as a review of the existing documented analysis and resulting maintenance program. An advantage of the less rigid review is that it can be very responsive and targeted inexpensively and easily at a single component. An overly formal process supports retention of the status quo because it is too hard to mount a case for review. It can also become a box-ticking exercise. It can

also encourage maintenance personnel to run double systems where they do not actually follow the formal program. Through this paper, we aim to indicate how organizations might take a more flexible approach to the application of maintenance requirements analysis.

Failure risk analysis and maintenance effectiveness in a windturbine

according to its history of unavailability and applied maintenance

M.A. Sanz-Bobi, R.J.A. Vieira & X. Montilla

Comillas Pontifical University, IIT—Institute of Technological Research, Madrid, Spain

ABSTRACT

The industrial sector at present is in a dynamic process continuously improving the products produced or services supplied and their quality. The cost-effective and efficient use of their available assets is crucial in the current context, and the efficient application of maintenance and asset management techniques are the most important instruments used to reach these objectives (Anders et al., 2007, Scheider set al., 2006). All these techniques require information about the life of the assets in order to make decisions regarding maintenance planning and the future use of assets.

Many approaches have been developed over the last decades to analyze different aspects of the life of the equipment or assets used in an industrial process. Also, many maintenance models have

been proposed over a long period of time nor
mally centered on preventive maintenance models
(Jardine & Tsang 2006). They have been refined in
several aspects and, in particular, some proposals
of imperfect maintenance models can be found in
(Nakagawa 1988, Bartholomew-Biggs et al., 2009,
Liu & Huang, 2010.). All these models are basi
cally based on unavailabilities occurred, failure
rates and maintenance times.

This paper proposes a new maintenance model,
inspired from the imperfect maintenance mod
els, able to characterize the effectiveness of the
maintenance applied and the risk of failure. This
model named MAOL is based on the historical
information of events including both unavailabili
ties and maintenance times. MAOL integrates an
evaluation of possible failure risk of a windturbine
according to the historical unavailabilities which
have occurred with an analysis about the effective
ness of the maintenance applied. MAOL supplies
important information about the effectiveness of
the maintenance applied and an evaluation of pos
sible unavailability risks. The information required
by the MAOL model is obtained from an analysis
of historical information using a tool which was

Functional and economic obsolescence of assets in network utilities

according to different environmental factors

J.F. Gómez

School of Engineering, University of Seville, Spain

V. González & Luis Barberá

Industrial Management PhD Program at the School of Engineering, University of Seville, Spain

A. Crespo

Associate Professor of Industrial Management School of Engineering, University of Seville, Spain

ABSTRACT

Maintenance in Network Utilities, such as distribution companies of water, electricity, gas, telecommunications, etc, customer oriented organizations, has to take into consideration the reliability of the assets among different areas of distribution. The same type of equipment could operate under different environmental conditions in dissimilar areas depending on, for example, temperature or humidity. These variations could accelerate the deterioration of the asset, called “obsolescence” whose implications have to be evaluated in terms of costs. Maintenance contributes with its activities to extending asset life minimizing the failures, and so to reducing the obsolescence, which is defined as one of the key negative

drivers of property depreciation and has the poten
tial to have a significant and immediate impact upon
the investment value of property in all operating sec
tors. For that reason, the estimation about perform
ance according to the service life of the assets has
to contain an obsolescence analysis, even generat
ing warnings when the total costs during the asset
lifecycle are exceeded or deviate from the prevision.
There are four main causes of obsolescence: func
tional related to changes within the uses of the assets,
economic referring to the cost of continuing to use
the assets, technological related to the efficiency of
recommendations or obligations such us changes on
Health and Safety laws or on social ecological ten
dencies. According to this, maintenance activities are
linked to the functional and economic obsolescence,
keeping the asset value in a physical sense but also
in an economic sense. There is a time-dependent
relationship between obsolescence analysis and the
reliability-based analysis according to functional fac
tors. On the other hand, economic obsolescence is
related to assets depreciation according to the finan
cial value of such assets to the business. In this study,
we will use reliability-based analysis to calculate the
Impact of maintenance on the replacement investment under

technological improvement

T.P.K. Nguyen, T.G. Yeung & B. Castanier

Ecole des Mines de Nantes, Nantes, France

ABSTRACT

The investment decision is clearly a strategic objective of a company as it defines its future competitiveness and the potential large costs incurred. This decision must, to ensure optimality, be based on the maximum information available in the company. However, we can summarize the motivations leading to an investment by the estimated performance (technical and economic) gap between the current system and competing technologies available on the market, taking into account budgetary opportunities. Numerous models for optimizing the investment decision were proposed in the economic, management science and operations research areas but few of them tackle the strong stochasticity and the uncertainty of the costs and the associated revenues. On the other hand, an unexplored important area in the investment problem under technological improvement is the impact of maintenance policy, maintenance defined here in complement to the replacement as a partial repair of the system. In fact, maintenance option

not only helps us to maximize the profitability of the available asset, but also allows us to prolong its economic life for waiting the apparition of better technology in the near future.

Therefore, we propose a model that considers the impact of maintenance on the investment decisions in a new or improved asset, based on information about the profitability of the current asset and the technological environment. The profitability is modeled a stochastic process defined by both the technical performance of the asset, and the uncertainty of market. Let assume that the technical performance is decreasing in the deterioration state of the asset. Furthermore, a new technology is characterizes by its non decreasing probability of being available into the market, its degradation characteristics and also its stochastic purchase cost function. For maintenance processes, we also consider the dependency of its cost and its efficiency on the deterioration state of asset that is characterized by profit parameter.

Finally, we propose to model the optimization

Integrating production and maintenance planning for a parallel

system with dependent components

M. Nourelfath

Université Laval, Québec, Canada

E. Châtelet

Université de technologie de Troyes, Troyes, France

ABSTRACT

In practice, production and maintenance planning activities are usually performed independently. Therefore, it cannot be guaranteed that the obtained plans are optimal with respect to the objective minimizing the total maintenance and production cost. The integration of PM and production decisions may reduce not only the interruption time, but the total expected cost also. For highly reliable equipment, PM schedules may be performed at a lower frequency (monthly, quarterly or even semi-annually). As a result, PM activities should be integrated with tactical production planning. The objective of this paper is to develop an integrated production and PM planning model dealing with tactical aggregate production planning decisions. At the tactical level, it is often dealt with items from a product family viewpoint. A product family is defined as a grouping of end items that share a common manufacturing set-up. Set-up is the process of actually converting the equipment. This may be achieved by adjusting the equipment

to correspond to the next product family or by changing non-adjustable “change parts” to accommodate the product family. As already suggested by the Total Productive Maintenance approach, the successful implementation of a maintenance program requires that its tasks be considered as parts of the production plan rather than as interruptions to that plan. Within this in mind, we consider that preventive maintenance activities are performed by machine operators responsible of set-up activities. The set-up activities are achieved at the beginning of planning periods. Thus, knowing that the production and maintenance requirements share common labour and time resources, PM tasks can be advantageously integrated to these set-up activities at the beginning of planning periods. In this case, because PM tasks are executed by machine operators responsible of set-up activities, the time and the cost of PM actions will be clearly lower than interrupting production to PM tasks during a production cycle. Unlike some existing models, we do not assume that the components are stochastically and economically independent. We rather deal with the problem of integrating preventive maintenance and tactical production planning, for a production system composed of a set of parallel components, in the presence of economic dependence and common cause failures. The latter correspond to events that lead to simultaneous failure of multiple components due to a common cause. We use the β-factor

model to represent common cause failures. This means that we assume two possible causes for system failure: the independent failure of single components, and the simultaneous common cause failure of all components. The suggested preventive maintenance is a T-age group maintenance policy in which components are cyclically renewed all together. Furthermore, between the periodic group replacements, minimal repairs are performed on failed components. We are given a set of products that must be produced by this parallel system in lots during a specified finite planning horizon. The objective is to determine an integrated lot-sizing and preventive maintenance strategy of the system that will minimize the sum of preventive and corrective maintenance costs, setup costs, holding costs, backorder costs and production costs, while satisfying the demand for all products over the entire horizon. A method is proposed to evaluate the times and the costs of preventive maintenance and minimal repair, and the average production system capacity in each period. For each chosen PM solution, the problem is solved as a multi-product capacitated lot-sizing problem. We show how the formulated problem can be solved by comparing the results of several multi-product capacitated lot-sizing problems. For large-size problems, a heuristic algorithm is proposed for the preventive maintenance selection task in the integrated planning model. Numerical examples are used to illustrate the potential benefits of using the proposed approach.

Maintenance effect modelling and optimization of a two-components

system

W. Lair & R. Ziani

Direction de l’Innovation et de la Recherche, SNCF, Paris, France

S. Mercier

Laboratoire de Mathématiques et de leurs Applications, Université de Pau et des Pays de l’Adour, Pau, France

M. Roussignol

Laboratoire d’Analyse et de Mathématiques Appliquées, Université Paris Est, Champs sur Marne, France

For a railway infrastructure like SNCF (French

National Railway Society), maintenance of the infrastructure is a major task because a failure causes delays and client dissatisfaction. Moreover, failures increase maintenance cost. The SNCF has hence initiated research in order to model the involved systems, in view of some improvement in their preventive maintenance. This article deals with a two-components system used at the SNCF. Both components have two failure modes and the system functioning mode makes the components dependent. This system is presently submitted to a periodic preventive maintenance policy. The aim of this paper is to study the eventual benefits pro vided by some adjustments on this periodic policy. The nature of the system is not revealed because of confidentiality issue.

To ensure the proper functioning of the sys tem and to prevent undesirable events to occur, a preventive maintenance action is annually under taken. During a maintenance action, the SNCF agent replaces the broken components if any and adjusts the working components. The data base at our disposal only provides information on the maintained components, which complicates the estimation of the unmaintained components

life-time distribution. Models exist which separate the intrinsic degradation from the maintenance actions effect. One of them is the ARA 1 (first-order Arithmetic Reduction of Age) model described in (Doyen and Gaudoin 2004). We propose a slight modification of this model which we call the first order Arithmetic Reduction of Age with Bertholon Adaptation (ARABA 1) model.

The modelling of the maintained system, with two dependent aging components regularly adjusted cannot be made with classical tools such as Markov jump processes with finite state space. We here propose to use Piecewise Deterministic Markov Processes (PDMP). Those processes are

Multicriteria paradigm and Multi-objective Optimization on maintenance modeling

C.A.V. Cavalcante & A.T. de Almeida
Federal University of Pernambuco, Brazil

ABSTRACT

Maintenance planning consists of the process of taking into account the failure behavior of an item, the consequences of failure and possible actions that could effectively translate everything into a management systematic in order to provide some improvement for the system. This meaning of

maintenance planning is very old. McCall (1965) argues that the techniques used to analyze mainte nance problems are necessarily included within the theme of decisions under uncertainty. The general structure of these problems has the elements that are characteristic of models of decision theory. Since then, many changes have occurred and more concerns have appeared on the management of maintenance activities (Kobbacy & Murthy, 2008). Therefore, the formalization of the decision proc ess is facing the challenge of dealing with multiple objectives in order to provide a broader view for the decision-maker. Consequently, we have seen many papers in the literature promising a better approach in order to support the decision maker by taking into account multiple objectives. The prob lems are that sometimes the use of the multicriteria and the multi-objective approaches do not follow consistent steps, some mistakes have been found in some applications and sometimes the problem is treated as having multiple objectives but only one aspect is taken into account or the decision maker is not considered.

Thus, in this paper we discuss in general terms a suitable structure for models to support main

tenance planning; situations where the MCDA

(MultiCriteria Decision Aiding), the field that

comprises the multicriteria and multiple Objective

Optimal preventive maintenance schedules using specific genetic

algorithms and probabilistic graphical model

I. Ayadi, L. Bouillaut & P. Aknin

Laboratory of Land Transport Networks Engineering and Advanced Computer sciences,

French National Institute for Transport Development and Risk Sciences and Technologies,

University of Paris-Est, France

P. Siarry

Lissi—Laboratory of Images, Signals and Intelligent Systems, University of Paris-Est Créteil, France

ABSTRACT

Equipments used in industrial environments such

as production lines, engineering or mass transport

system, are generally complex, multi-components

and Multi-States Systems (MSS). These equip

ments are subject to degradation mechanisms

caused by operating conditions/environment

(temperature, vibrations …). In addition to these

degradation mechanisms, the deployed mainte

nance policy affects directly the dynamics of the

occurrence of failure states. Given this situation,

we should consider establishing Preventive Main

tenance (PM) strategies to ensure an adequate trade-off between system availability and its main tenance costs.

Solving this issue requires a prior modeling of the system degradation. This modeling must represent faithfully the evolution of the operat ing states of a multi-components system, dur ing time. Given that, an evaluation model of PM policies can be considered, inorder to look for the optimal schedules of the PM. A com mon way, in PM optimization, is to assume algo rithms relying on classical degradations modeling approaches like deterministic models, stochastic processes or Markov chains. These approaches allowo ptimization algorithms to go faster, but they require, necessary, exact knowledges of deg radation processes or strong assumptions about so journ-time distributions. This limitation can be overcomed by the use of a particular struc ture of Probabilistic Graphical Temporal Model named Graphical Duration Models (GDM).

GDM allows to represent duration models of MSS, regardless of the exact nature of their so journ-time distributions.

This work can be divided mainly into two steps.

The first one proposes an utility model for the evaluation of maintenance policies. This model is mainly based on the GDM. It involves essential parameters like maintenance probabilities, utilities or system availability. In the second step, two Genetic Algorithms (GAs) were developed. They seek for the optimal PM schedules. The 1st one named GA 1 seeks for periodic schedules contrarily to the 2nd one, GA 2 , which look for non-periodic schedules. GA operators are redesigned according to the specific characteristic of the problem. Figure 1 summarize the preventive maintenance optimization solving process. To demonstrated the applicability of the proposed methodology, a Distribution Fluid System (DFS) has been chosen as case study. This approach provides good results and allows a specific analysis of the weight of the different parameters of the utility function. Figure 1. Preventive maintenance scheduling procedure using a genetic algorithm. System reliability and maintenance costs parameters investigation System dynamic probabilistic modelling Utility model for maintenance policies evaluation Genetic Algorithm for optimal preventive maintenance policy Optimal preventive maintenance schedules Objective function Maintenace schedules

Optimal prognostic maintenance planning for multi-component

systems

A. Van Horenbeek & L. Pintelon

Catholic University of Leuven, Heverlee, Belgium

ABSTRACT

Many models and methodologies to predict the

Remaining Useful Life (RUL) of a component

or system are investigated nowadays. However,

decision making based on these predictions (RUL)

is still an underexplored area in maintenance man

agement. The real value of this prognostic infor

mation for scheduling maintenance actions on

multi-component systems with different levels of

dependence between components is not yet quantified. The link between prediction algorithms and decision making based on the resulting remaining useful life distributions should be established. The objective of this paper is to optimally plan maintenance for a multi-component system considering different levels of dependencies (economic, structural and stochastic dependence as defined by Nicolai & Dekker (2007)) based on prognostic information. By doing so the added value of this prognostic information (RUL) in maintenance planning and decision making is quantified. This is achieved by constructing a stochastic discrete-event simulation model, which optimizes maintenance action scheduling, based on prognostic information on the different components. A multi-objective optimization is performed by taking into account both cost and availability criteria as the maintenance objectives. Considering cost and availability as two separate objectives makes it possible to adapt and find the optimal maintenance policy according to the business environment at the time of decision making. A genetic algorithm is used to search for the optimal maintenance schedule which takes into account the predicted deterioration of

all components. The added-value of scheduling

maintenance actions based on prognostic informa

tion is determined by comparing this maintenance

policy to five other conventional maintenance

policies, which are: corrective maintenance, block

based and age-based preventive maintenance,

offline condition-based maintenance and online

condition-based maintenance.

A multi-component manufacturing system is

investigated as a real life case study to illustrate the ability of the prognostic maintenance policy to react to different and changing deterioration patterns and dependencies between all considered components. To quantify the effect of different levels of dependencies between components on the optimal maintenance schedule a dependence parameter α, which ranges from 0% to 100%, is introduced. This parameter α reflects the advantage on cost and downtime of performing maintenance on multiple components at once compared to maintenance on a single component. A cost comparison between different maintenance policies for the multi-component manufacturing system with different levels of dependence between components is performed, which clearly shows the added value of prognostic information in maintenance decision making (Fig. 1). In this way an optimal maintenance policy is guaranteed all of the time and not only over time.

REFERENCE Nicolai, R.P. & Dekker, R. 2007. Optimal Maintenance of Multi-component Systems: A Review. Complex System Maintenance Handbook, Springer London: 263-286.

Figure 1. Total expected cost versus dependence parameter α for all considered maintenance policies.

Optimization of redundancy and imperfect preventive maintenance

for series-parallel multi-state systems

M. Nourelfath

Université Laval, Québec, Canada

E. Châtelet

Université de Technologie de Troyes, Troyes, France

ABSTRACT

This paper formulates a joint redundancy and imperfect preventive maintenance planning optimization model for series-parallel multi-state degraded systems. Non identical multi-state components can be used in parallel to improve the system availability by providing redundancy in subsystems. Multiple component choices are available on the market for each subsystem. The status of each component is considered to degrade with use. It is assumed that the system can consecutively degrade into several discrete states, which are characterized by different performance rates, ranging from perfect functioning to complete failure. The latter is observed when the degradation level reaches a certain critical threshold such as the system efficiency may decrease to an unacceptable limit. In addition, the system can fail randomly from any operational or acceptable state and can be repaired. This repair action brings the system to its previous operational state without affecting its failure rate (i.e., minimal repair). The used preventive maintenance policy suggests that if the system reaches the last accept

able degraded state, it is brought back to one of the states with higher efficiency. System availability is defined as the ability to satisfy consumer demand that is represented as a piecewise cumulative load curve. A procedure is used, based on Markov proc esses and universal moment generating function, to evaluate the multi-state system availability and the cost function. The objective of the newly devel oped optimization model is to determine jointly the maximal-availability series-parallel system struc ture and the appropriate preventive maintenance actions, subject to a budget constraint. A large size numerical example is used to illustrate the proposed approach. As the number of possible solutions and the number of subspaces are huge for this example, and it is then impractical to use an exhaustive enu meration method, a heuristic approach is suggested to solve the formulated problem. This heuristic is based on a combination of space partitioning,

Predicting rail geometry deterioration by regression models

F.P. Westgeest & R. Dekker

Erasmus School of Economics, Erasmus University Rotterdam, The Netherlands

R.H. Fischer

Faculty of Technology, Policy and Management, Delft University of Technology, Delft,

The Netherlands

ABSTRACT

The Eurailscout measurement train is regularly used by the rail infra manager ProRail as well as by the maintenance contractors to assess the railway track geometry deterioration data on characteristics like scant, horizontal, vertical alignment. So far these data have only be used to determine whether maintenance is directly needed. After a long data processing phase we are able to compare measurements on same segments in time. We applied statistical regression techniques to assess the influence of environmental characteris tics, like subsoil, tonnage and underlying objects. The regression analysis on the degradation data

KPI KPI Switch Tampingobject D − · − · − 0 87 1 07 0 36 0 10 0· − 19 1 . . . . . Non tampingobject Monoblock i bl k Subs − + · + · 0 16 0 15 0Tw n oc· + 07 . . . oilclay Tonnageg p− +0 03. or· u ε

KPI D is the estimated KPI value for the degrada tion model. The standard errors in all coefficients were small (0.06 in the fixed term, 0.02 to 0.04 in all other terms except 0.01 for the tonnage term). We can see that the constant parameter is negative, which can be expected when no positive values are included. It indicates the yearly deterioration. The

coefficient of the lagged KPI value, KPI −1 , is larger

than 1, which means that the quality of observations

with higher lagged KPI values decrease less than

observations with low lagged KPI values. If it

would be 1 than the present quality would not

have any effect on the drop. The variables Switch,

Probability distribution of maintenance cost of a repairable system

modeled as an alternating renewal process

T. Cheng & Mahesh D. Pandey

Department of Civil and Environmental Engineering, University of Waterloo, Waterloo, Ontario, Canada

J.A.M. van der Weide

Department of Electrical Engineering, Mathematics, and Computer Science, Delft University of Technology,

Delft, The Netherlands

ABSTRACT

Critical engineering systems, components and

structures in power plants, chemical processing

industry, and automotive industry are vulnerable

to failure due to damage caused by shocks or

over-stress that occur over the service life of the

system. The failure occurs when the damage in the

system exceeds its capacity. To maintain reliability

of such systems, periodic inspection and preven

tive maintenance programs are implemented by

engineers.

In most of the literature, maintenance optimiza

tion is based on minimization of the asymptotic

cost rate, because the renewal theorem provides a

simple expression for its computation. The asymp

totic cost rate is equal to the expected cost in one

renewal cycle divided by its expected length or

duration.

The asymptotic formulation has a wide appeal,

because it basically reduces the stochastic renewal

process model to the first failure problem. However,

this simplification may not be realistic for many

engineering systems with a relatively short and finite

operating life. The expected maintenance cost in a

finite time horizon is only discussed in a few papers

(Christer & Jack 1991, Pandey, Cheng & van der

Weide 2010, Cheng & Pandey 2011).

This paper presents the derivation of the

probability distribution of maintenance cost of a

Robustness of maintenance decisions: Uncertainty modelling

and value of information

A. Zitrou & T. Bedford

Department of Management Science, University of
Strathclyde, Glasgow, UK

A. Daneshkhah

Department of Statistics, Shahid Chamran University, Ahvaz,
Iran

ABSTRACT

Maintenance optimisation models are essentially concerned with the minimisation of the overall maintenance cost—usually expressed as the aver age cost per unit of time (cost rate). The cost rate depends on a number of parameters related to reli ability and cost aspects of the system. Like in any kind of model, here as well, studying the sensitivity of the model output with respect to the changes in the model parameters (e.g., reliability parameters) is of great interest. Typical methods for sensitivity analysis include the brute-force approach (where the effect of a number of deviations from the parameter in question is examined directly) and variance-based methods (where the contribution of each parameter to the variance of the output is determined analytically). Sensitivity analysis is important because if the cost-calculations are not sufficiently robust, use of the maintenance model can lead to optimization recommendations that are themselves not robust. However, the variance based methods will not necessarily highlight this problem. In this paper we use the concept of the Expected Value of Perfect Information (EVPI) to perform decision-informed sensitivity analysis.

EVPI calculations allow us to identify the key parameters of the problem and quantify the value of learning about certain aspects of the system. This information is of great importance within a maintenance context, where decisions may not only relate to replacement timings, but also to accumulation of information about aspects of the system, like the ageing process. Unfortunately, decision-theoretic sensitivity analysis within a main tenance optimisation context is very demanding: the computation of expected utility requires the use of numerical integration techniques. Following from the work of Oakley (2009) this paper presents sensitivity analysis by using Gaussian process emu lators. This approach is more suitable for complex models like this, as it allows for sensitivity analy sis to be performed by using a smaller number of model runs. To illustrate this methodology, we are using two maintenance settings: the first setting concerns a one component system subject to age-replacement policy and the second setting describes a multi component system subject to block-replacement policy. In both settings the challenge is to identify the maintenance timings (critical age or periodic interval) that minimise the cost rate. Based on a GP emulator process, we have derived both point and interval estimates of value of learning, and explored how the optimal decision may vary. Figure 1 portrays the expected cost of the different maintenance options for the age-replacement model, assuming that a parameter can be known completely before a decision about the critical age is made. EVPI-based sensitivity analysis allows for the identification of the parameters with the highest learning

value and can ensure not only that maintenance decisions are sufficiently robust, but also that processes like further testing or training are economically justified. REFERENCE [1] Oakley, J. (2009). Decision-theoretic sensitivity analysis for complex computer models. Techno-metrics 51(2), 121-129. Figure 1. Expected utilities when θ i is completely known before the maintenance decision. 1 2 3 4 -2 -1.5 -1 -0.5 η T12 T13 T14 T15 T16 T17 30 32 34 36 38 -1.15 -1.1 -1.05 -1 -0.95 -0.9 β 1 2 3 4 -1.06 -1.04 -1.02 -1 -0.98 θ 2 2.5 3 3.5 4 -1.15 -1.1 -1.05 -1 -0.95 δ

Semi-Markov processes for coverage modeling and optimal maintenance

policies of an automated restoration mechanism

H.C. Grigoriadou, V.P. Koutras & A.N. Platis

Department of Financial and Management Engineering, University of the Aegean, Chios, Greece

ABSTRACT

In this paper, a two unit computer system is considered. The system consists in one operational and one standby unit, with imperfect coverage and an automated restoration mechanism, which is a switching device setting in operation the standby unit when a failure occurs on the primary unit. The units are affected by failures depending on random environmental factors and consequently the failure rates can be assumed as constant. Therefore, cor rective maintenance is considered for each of the units. On the other hand, the automated restora tion mechanism is affected by failures depending mainly to the frequency of use and simultaneously

by the time spent at the standby mode. Hence, for the automated mechanism preventive maintenance at constant time intervals is considered. Neverthe less, when a failure occurs on the switching device corrective maintenance takes place.

In such a system, when a failure occurs at the operational unit, the restoration mechanism may be in a failure mode and hence unable to accomplish the switching procedure. In this case, the system is switched to the standby unit manually. Such phenomena can be prevented by adopting preven tive maintenance. Since, preventive maintenance can be performed while the system is in operational mode, it is of critical importance to distinguish the optimal maintenance frequency. The optimal maintenance frequency aims to prevent failures that may occur during the maintenance of the switching device.

The modeling of imperfect coverage is based on the probability of success for the automated restoration mechanism. Firstly, the system is mod elled by a Semi-Markov process since the time to maintenance for the restoration mechanism is

Université de Technologie de Troyes, Institut Charles Delaunay, FRE CNRS2, Troyes, France

C. Paroissin

Université de Pau et des Pays de l'Adour, Pau Cedex, France

We consider a multi-component deterioration system whose condition can be summarized by a scalar ageing variable. The mean deterioration rate is supposed to be an unknown function of the life time. The ageing variable increases with the sys tem's deterioration and the failure occurs as soon as the system state crosses a known fixed threshold called failure threshold.

As an example of such system we can consider the steel structures such as bridges, tanks and pylons which are exposed to outdoor weathering conditions. In order to prevent them from cor rosion they are protected by an organic coating system. Unfortunately, the coating system itself is also subject to deterioration. To have a better monitoring procedure the area affected by corro sion can be divided in sub-areas and the deteriora tion of each sub-area can be separately monitored and maintenance action is to be done as soon as the maximum of all deterioration exceeds a fixed threshold. In (Nicolai 2008) this example is consid ered and a stochastic process is proposed to model

the deterioration.

In this paper the scalar ageing variable is mod

elled by a non-homogeneous gamma process with

unknown parameters, see (van Noortwijk 2009).

It should be recalled that gamma process is a posi

tive process with independent increments. It implies

frequent occurrences of tiny increments which

make it relevant to describe gradual deterioration

due to continuous use such as erosion, corrosion,

concrete creep, crack growth, wear of structural

components. Furthermore, the gamma process

allows feasible mathematical developments. It has

been widely applied to model condition-based

maintenance.

The system is periodically inspected and at each

inspection time three decisions can then be taken

(preventive maintenance, corrective maintenance

Simple Non-Markovian models for complex repair and maintenance

strategies with LARES+

Max Walter

Lehrstuhl für Rechnertechnik und Rechnerorganisation,
Technische Universität München, Germany

In recent publications (Walter, Gouberman, Riedl,

Schuster & Siegle 2009; Walter & Lê 2011) we have

introduced the ‘language for reconfigurable sys

tems plus (LARES+)', a modeling language for quantitative dependability evaluation of fault tolerant systems. When compared to traditional state based methods like stochastic Petri nets or process algebras, LARES+ can be learned more quickly, and model creation requires less time and is less error-prone. In particular, the only formalisms used in LARES+ are state machines and Boolean terms; both are well-known in most engineering disciplines. Moreover, LARES+ models can be constructed by stepwise refinement, are modular and hierarchic as well as easy to modify, and allow for re-using sub-models. In our previous work, we have shown the applicability of LARES+ to complex examples taken from the literature.

So far, the stochastic process defined by a LARES+ model is restricted to a homogeneous continuous time Markov chain (CTMC). Thus, all timed transitions in a LARES+ model must follow exponential distributions. While this can be accurate for modeling the failure behavior of components with constant failure rates, it clearly is a gross approximation when modeling failures of components which are subject to wear-out, or deterministic time intervals such as repair times, maintenance

intervals, or the duration of reconfiguration. Thus,

LARES+ cannot be used for the evaluation and

optimization of maintenance strategies, where

these aspects are of crucial importance.

Therefore, this article proposes an extension of

LARES+ which introduces transitions with non

exponential timing behavior (e.g. deterministic or

SIS-design automation by use of Abstract Safety Markup Language

K. Machleidt & L. Litz

Institute of Automatic Control, University of Kaiserslautern, Kaiserslautern, Germany

T. Gabriel

Institute of Automatic Control, University of Kaiserslautern

Currently with: Bayer Technology Services GmbH, Leverkusen, Germany

ABSTRACT

Failure tolerant Safety Instrumented Systems

(SIS) contribute to companies' profitability. Oper

ational requirements need to be considered in SIS

design in addition to safety requirements defined

by Safety Integrity Level (SIL). Consequently, the

task to design SIS for given safety requirements

is extended to provide best possible operational

performance.

SIS are widely applied in process industry and

the machinery sector to make potential hazard
ous applications safe. Faults of SIS can result in
severe accidents. The SIL requirements derive from
IEC 61508 (2010) and related international safety
standards. SIL requirements involve architectural
constraints, quantitative, and qualitative require
ments. Qualitative requirements regulate work
processes and procedures in each phase of the
SIS life cycle and are not treated here. In contrast,
the other two SIL requirements directly impact
SIS design. The architectural constraints regulate
the Hardware Fault Tolerance (HFT)—a design
parameter for the hardware redundancy level of
the SIS. The quantitative requirements involve SIS
unavailability modeling and calculations.
In this publication the design process of SIS is
analyzed and SIL requirements as well as opera
tional requirements are elaborated. It is explained
that formal SIS design is superior to manual SIS
design. The Advanced SIS Design Approach is out
lined as a new formal multi-stage procedure for
computer-aided SIS design. It provides the most
advantageous SIS configuration for a given appli
cation taking into account user-defined demands.
The architectural constraints defined for SIS by

international standards are formally interpreted to

be applicable to the formal procedure. Contrary,

conventional manual SIS design produces less

advantageous SIS due to simplifications consider

ably reducing the number of potential configura

SPAMUF: A behaviour-based maintenance prediction system

Pedro Bastos

Instituto Politécnico de Bragança, Bragança, Portugal

Isabel Lopes

Universidade do Minho, Escola de Engenharia, Guimarães, Portugal

Luís Pires

Instituto Politécnico de Bragança, Bragança, Portugal

ABSTRACT

In the last years we have assisted to several and

deep changes in industrial manufacturing. Many

industrial processes are now automated in order to

ensure the quality of production and to minimize

costs. Manufacturing enterprises have been

collecting and storing more and more current,

detailed and accurate production relevant data.

The data stores offer enormous potential as source

of new knowledge, but the huge amount of data

and its complexity far exceeds the ability to reduce

and analyze data without the use of automated

analysis techniques.

The industrial production has suffered con
siderable changes, becoming more complex, con
tributing to this a need for increased efficiency,
greater flexibility, product quality and lower costs
(Bansal, et al., 2004).

Maintenance process is usually performed by
integration of maintenance and process engineering
functions at the phase of selection and application
of machines and equipment; and also through pro
active actions on those machines and equipments
that will necessarily passes by preventive and
predictive maintenance (Palmer 1999).

Nowadays, the amount of data generated and
stored during industrial activities exceeds the
capacity to analyze them without the use of auto
mated analysis techniques. Thus, in the late 80’s
emerged the area of Knowledge Discovery in
Databases (KDD), using models and data mining
techniques for extract useful knowledge, patterns
and tendencies previously unknown, in a autono
mous and semi-automatic way (Apte, et al., 2002).

The paper addresses an organizational archi
tecture that integrates data gathered in factories
on their activities of reactive, predictive and pre
ventive maintenance. The research is intended to

develop a decentralized predictive maintenance

system (SPAMUF—Prediction System Failures

Spare parts provision for a maintained system with a heterogeneous

lifetime

P.A. Scarf

University of Salford, Salford, UK

C.A.V. Cavalcante

Federal University of Pernambuco, Recife, Brazil

ABSTRACT

We consider an inspection and replacement policy

for a simple system comprising a single component

installed in a socket. The component has a mixed

lifetime distribution, so that a component may be

weak or strong, reflecting perhaps the possibility

of poor installation. When the component fails

the system fails and the component is subject to

a replacement. A common assumption for the

majority of maintenance policies studied is that a

spare component is available whenever the origi

nal component is replaced. We relax this assump

tion and suppose that the replaced component is

overhauled and returned to the spares inventory.

We further suppose that the system is subject to

age based replacement. Our aim is to simultane

ously optimize the age at preventive replacement and the stock level. In so doing, we focus on the effect of component heterogeneity on cost and system availability taking account of the maintenance policy and inventory related factors. Component heterogeneity is regarded here as a surrogate for the quality of maintenance.

The simultaneous optimization of inventory and maintenance policy is not new. Much of the benefit of the joint optimization of preventive replacement and spares provisioning may be due to the fact that the requirement for spares under a periodic replacement policy is predictable. Ordering times and stock levels can then be better planned. However, if the effectiveness or quality of replacement (and hence maintenance) is uncertain then demand for spares may be more erratic. Our paper makes a contribution by investigating the effect of such variation in maintenance quality. It is related to recent work on maintenance quality (Scarf and Cavalcante, 2010). It is also related to work of Armstrong and Atkins (1996) who look

Department of Production and Quality Engineering, Norwegian University of Science and Technology

Trondheim, Norway

ABSTRACT

The reliability of Offshore Wind Turbines (OWT) has posed new challenges due to the complex nature of operations due to its location in sea. The weather is heavily influencing the availability of wind turbine for power due to the access and logistic issues. One way to address such operational challenges is to devise ways to approximate the ongoing state of the component. When the state is demanding to take some action, then it is impor tant to devise the strategy regarding when to access the wind turbine depending upon the weather forecast. The decision regarding conducting any corrective action will depend on the condition of the component and if the state is critical but the weather is harsh, then to wait. This waiting time will depend on the duration of bad weather and the severity of the component.

Maintenance and renewal of OWT poses new challenges due to number of factors like marine environment, weather conditions, and uncertain ties regarding new failure modes and mechanisms.

To address these issues, it is proposed to evalu

ate the state of the component (gearbox) using

the gamma process or phase type distribution. The

determination of effective failure rate, renewal rate

and the frequency of inspection will depend upon

the current state of the component and then the

next action will be suggested keeping in view the

present condition. So for undertaking such action, it is proposed to determine the effective failure rate and renewal rate as function of state and the maintenance interval. Furthermore, two separate limits has been defined to calculate the effective failure rate and the renewal rate. So we have put specially focus on degradation modeling of OWT components where the state information is used to determine when to perform maintenance and renewal taking into accounts the fact that the OWT will be unavailable in randomly distributed periods of times due to the weather conditions. The model includes maintenance and renewal costs, cost of loss production, and a simple weather window model. The proposed scheme is implemented on the gearbox which has the highest downtime in case of failure. After determining the optimal maintenance interval, then a simple weather model has been introduced. The modeling framework has been proposed how to formulate the strategies if the duration of harsh weather will coincide with the optimal maintenance intervals. Two strategies, either to advance or delay the maintenance activity, have been suggested and their formulation has been proposed. Furthermore, it has been suggested how to link these two strategies as the function of condition and maintenance interval. It is expected that the efficient maintenance of gearbox will enhance the availability of OWTs in a better and cost effective way.

The analysis and conversion of warranty maintenance tasks

for a power plant

B.M. Alkali

Glasgow Caledonian University, Glasgow, UK

P. McGibney

Moneypoint Coal-fired Power Generating Station, Kilrush Co.
Clare, Ireland

ABSTRACT

A new scrubber plant in an existing power generating plant is considered in this study. The plant has a two year warranty maintenance tasks to be observed during operation. The main aim of this project is to examine the warranty period main tenance task list and propose adequate methods for assessing the preventive maintenance task in order to improve the whole maintenance process. Statis tical approach is used to give an insight with refer ence to equipment status and a modeling approach is proposed to also assess maintenance information defined by experts with the focus on availability of systems in the context of actual operating regimes. A full review examination of each preventive main tenance task is conducted using expert judgement elicitation to ensure accuracy in all aspect of the task. This study focuses on the power plant's criti cal equipment. The Booster fans have been identi fied as critical equipment as they are vital to the plant process. Failure Mode and Effect Analysis (FMEA) is conducted on the power plant Booster Fans. A quantitative model structure is proposed

that could give an insight about equipment failure

pattern to review the maintenance warranty tasks.

We started our investigation by identifying

where warranty and maintenance are carried out.

We examine maintenance schedule and explore

maintenance modelling options. The process of

modelling is to aid in determining the duration time

between each maintenance task to ensure a more

efficient process. The reviewed task investigated is

to be populated on to CMMS. Engineering judge

ment is often applied to bridge the gap between hard

technical evidence and unknown characteristics of

a technical system, (Cooke & Goossens, 2004).

Intuition and judgement permeate engineering

analysis from very basic decisions and techniques

to adapt to more complicated assessment, (see

Otway & Winterfeldt 1992; O'Hagan et al., 2006).

This investigation is conducted in conjunction

with the information elicited from the Front Line

A block replacement policy for a bivariate wear subordinator

Sophie Mercier

Laboratoire de Mathématiques et de leurs Applications,
Université de Pau et des Pays de l'Adour, France

Michel Roussignol

Laboratoire d'Analyse et de Mathématiques Appliquées,
Université Paris-Est Marne-la-Vallée, France

ABSTRACT

In case of a system submitted to an accumulative random damage, classical stochastic models are compound Poisson processes and Gamma proc esses, which both are increasing Lévy processes, see [1], [3] or [4] e.g. Such classical wear models typically are univariate. However, the deterioration level of a system cannot always be synthetized into one single indicator and several indicators may be necessary, see [2] for an industrial example. In that case, a multivariate wear model must be used to account for the dependence between the different univariate indicators of the system. Another con text where multivariate wear models are required is the case of different systems submitted to common stresses, which make their wear indicators depend ent. Multivariate increasing stochastic models hence are of interest in different contexts. We here propose to use multivariate increasing Lévy proc esses (or multivariate subordinators) as multivari ate wear processes.

Considering bivariate subordinators as bivari ate wear processes, the aim of this presentation is to revisit a classical block replacement policy within this new context, with the optimization of

a cost function as an objective. A system is hence

considered, with deterioration level measured by a

bivariate subordinator. The system is not continu

ously observed. It is perfectly and instantaneously

repaired periodically at a given cost. If the system

A Monte Carlo approach for evaluation of availability and failure intensity under g-renewal process model

O. Yevkin

Dyadem International Ltd (has been acquired by IHS), Toronto, Canada

ABSTRACT

Several models have been developed for imperfect

repairs that assume that the component is “better

than old but worse than new” following the repair.

One of the most attractive among them is the

g-renewal process introduced by Kijima & Sumita

(1986). The process is characterized by repair effec

tiveness parameter q, defining a virtual age of the

unit at the given time after several repairs. Unfor

tunately, there is no closed form solution of corre

sponding g-renewal equation except the case when

the system is “same as old” after restoration (q = 1)

or for special (exponential) underlying failure dis

tribution functions. Different approximate meth

ods have been developed for other cases. The most

general among them is the Monte Carlo approach introduced by Kaminskiy & Krivtsov (1998). The method was used for estimation of the expected number of repairs in warranty data analysis (Kaminskiy & Krivtsov, 2000; Yanez et al., 2002). In the present paper, we have generalized and implemented the Monte Carlo algorithm for evaluation of other reliability characteristics like unavailability and failure intensity (frequency of failures), which are also very important in main tainability and its cost efficiency analysis (Vaurio, 2003). In addition, these reliability parameters are main inputs for system components, for example represented as basic events in a fault tree by mode ling a system behavior. It is very important to have an efficient algorithm to define input at the com ponent level. Therefore, some improvements of the Monte Carlo algorithm (including multithread ing approach) are considered in the paper as well. The accuracy of the algorithm has been evaluated by calculating standard error and comparing the result of calculation with exact solution in the case when q = 1.

Underlying Weibull distribution function is considered in the provided numerical examples,

however the algorithm can be easily applied to

any types of distribution of underlying func

A new criterion for design of brittle components and for assessing

their vulnerability to brittle fracture

M.T. Todinov

Oxford Brookes University, Oxford, UK

ABSTRACT

Unlike ductile fracture, brittle fracture occurs

suddenly, proceeds at a high speed and in order to

progress, there is no need for the loading stress to

increase. Brittle fracture also requires a relatively

small amount of accumulated strain energy. These

features make brittle fracture a dangerous failure

mode and require a conservative design criterion.

Vulnerability to brittle failure initiated by flaws,

is a common type of mechanical vulnerability,

caused by an unfavourable combination of sev

eral factors—existence of a defect with a critical

size, missing the defect by the non-destructive

inspection, unfavourable location of the defect in

a highly stressed zone of the component and unfa

vourable orientation of the defect with respect to

the local stresses. To improve the safety of loaded

brittle components, and to reveal the vulnerability

to brittle fracture which has often materialised as high-impact failures, a new, mixed mode, conservative failure criterion has been proposed.

The new conservative design criterion incorporates the worst possible orientation of a flaw with size just below the detection threshold of the inspection method. The new criterion has a simple analytical form and can be used as a solid basis for design of brittle components and for revealing their vulnerability to brittle fracture.

It is assumed that the component under consideration contains a globular flaw with a worst-case size, equal to the threshold flaw size of the non destructive inspection technique. It is also assumed that around the globular flaw, a sharp penny shaped crack has been initiated, with size equal to the size of the flaw.

The proposed new design criterion is superior to all existing methods used in the design of brittle components. It can also be applied for determining the degree of vulnerability to brittle fracture. Suppose that the distribution of the principal stresses is known from a finite-elements solution. Testing the vulnerability of the component then reduces to going sequentially through all finite elements, applying the new design criterion and verifying whether a defect with a threshold size will cause brittle failure. The ratio of the number of finite elements where brittle failure ‘has been initiated’ to the total number of finite elements is a measure for the degree of vulnerability to brittle failure. An important part of the paper is the optimal allocation of a fixed

budget towards a non destructive inspection, to achieve a maximum reduction of the risk of brittle failure. We present for the first time an efficient exact solution of the optimal budget allocation problem, based on an efficient dynamic programming algorithm. No constraints have been imposed on the functions defining the amount of removed risk. In this respect, the classical definition of risk has been challenged. It is argued that for a single failure occurrence, the classical definition of risk, as a product of the probability of failure and the average value of the consequences given failure, is inadequate. For a single failure occurrence, the distribution of the consequences of failure is sampled only once, and there is no guarantee, that the realization of the consequences will be close to the mean of the consequences. As an alternative, a new risk measure has been introduced—a combination of the average expected potential loss and the squared positive deviation from the mean of the consequences towards higher values.

Application of competing risks and generalized renewal processes

in reliability analysis

R.J. Ferreira, M.C. Moura & E.A.L. Droguett

Center for Risk Analysis and Environmental Modeling, Department of Production Engineering,

Federal University of Pernambuco, Recife, Brazil

P.R.A. Firmino

Department of Statistics and Informatics, Rural Federal University of Pernambuco, Recife, Brazil

ABSTRACT

In Risk and Reliability Analysis, the behavior of

failure is of a great importance, given its impact on

longevity of a System or Component (SC). Also,

the occurrence of failure is related with costs—loss

of production, expansive maintenance actions and

acquiring new components.

In these cases, the best way to prevent high val

ued events is to construct an optimum maintenance

policy regarding the failure behavior. However,

between programmed preventive maintenance, the

system can have failures and these failures occur

in a random way. The literature presents several

models to model the failure behavior regarding

corrective actions. Between them, one can cites the

virtual age models, which are capable of analyze

the failure distribution via a concept called virtual

age—what is the status of the SC after repair or

how good the SC had returned after repair? This

is measured through a parameter called renewal

parameter presented on Generalized Renewal

Processes, one of the virtual age models.

Preventive actions are also modeled by several

models or methodologies. One can cite Competing

Risks (CR) models, which are capable to model

not only failure times, but also the group of fail

ure modes that can cause failure events. This

analysis can be done through the study of a

pair of observation (Y, J) where Y is the event

Early detection of change-point in occurrence rate with small

sample size

Laurent Bordes, Christian Paroissin & Jean-Christophe Turlot

Université de Pau et des Pays de l'Adour, Laboratoire de Mathématiques et de leurs Applications—UMR

CNRS 5142, Pau, France

ABSTRACT

We address here the problem of deciding if either n consecutive independent inter-event times (i.e., the time that elapses between two consecutive failures) have the same distribution or if there exists some $k \in \{1, \ldots, n\}$ such that the common distribution of the first k inter-event times is stochastically larger than the common distribution of the last n − k inter-event times. It is the so-called change-point detection problem.

Many change-point detection methods are based on classical maximum type statistic. To detect a change-point on a sample having small size we have to face two problems. The first one is that it is difficult to base a decision on large sample properties of involved statistics since it is well known that the convergence rates of maximum type statistics is rather low. The second problem is that statistics are generally not free of the underlying distribution of the sample (under the null hypothesis of "no change-point") which prevent to determine test critical values through Monte Carlo methods.

Here we propose several methods that overcome

the later problem and that do not require neces

sarily a parametric assumption on the underlying

distribution.

Let us denote by X 1 , ..., X n the n inter-event

durations available at the calendar time t. These

random variables are assumed to be independent,

but one wants to test whether they are identically

distributed or not. The main scheme of the pro

posed methodology is as follows:

1. split the sample into two subsamples: (X 1 , ..., X k)

and (X k+1 , ..., X n) for k ∈ {m, ..., n−m};

2. compute the homogeneity test statistic for each

splitting;

3. use all homogeneity test statistics to take a

decision.

Decision can be either that no change

point occurs or that a change-point occurs at

k∗ ∈ {m, ..., n−m}. For the two subsamples (X 1 , ..., X k) and (X k+1 , ..., X n), assume that one can apply a given homogeneity test. We denote by S n,k the corresponding statistic that aims to measure the “distance” between the two subsamples parent distributions. From all these statistics, we suggest three types of global test based on the n−2 m + 1 statistics: 1. maximum-type: M S S n m k n m n k n k = ( ) max var ; , , ≤ 2. χ 2 -type: χ n n k n k k m n m S S 2 2 = ( ) Σ , , var ; 3. quadratic-type: Q n T = Σ S − S n n 1 , where S n = (S n, m , ..., S n, n−M) T and Σ is the covariance matrix of S n . For the homogeneity test for comparing two consecutive subsamples, we consider the four following statistics: 1. test based on

likelihood ratio; 2. test based on empirical failure rate ratio; 3. test based on Mann-Whitney statistic; 4. test based on precedence statistic. The two first statistical tests require the assumption that the inter-event durations are exponentially distributed while the two last statistical tests are nonparametric. Numerical studies were carried out to compare the power of the various proposed tests. These tests are then applied to a real data (typical feedback data from a transportation company).

Fine exact methods of safety, security and risk engineering

D. Prochazkova

Institute of Security Technologies and Engineering, Faculty of Transport Sciences,

Czech Technical University, Praha

ABSTRACT

The human system safety represents a well-ordered

set of human measures and human activities that

provides human system security and sustainable

development; by analogy it holds for other systems

(Prochazkova, 2007 a). Because the human system

dynamically behaves, the set of human measures

and human activities must be also well proactively

and strategically managed. Because a lot of tasks

cannot be solved precisely, the engineering disci

plines must be applied. The engineering is the wide

discipline that solves problems from their insight,

over proposal of solution up to realisation under

given conditions. It is drawing force of human

development because it also solves problems that

are heavily exactly soluble. For this it uses the

creativity of human individuals and approaches denoted as good practice (good engineering prac tice). At present it goes from system approach and for ensuring the present aims that are safe utility, safe community, safe region etc. It uses special dis ciplines that are in the paper briefly described. All engineering disciplines need to know critical items, i.e., items related to real processes and determined by site and time co-ordinates, and are based on negotiation with risks. The risk is for engineering practice well expressed as probable size of losses, damages and harms on followed assets that are caused by a given disaster with specified size and that are rescheduled for certain time unit (usually 1 year) and certain territory unit. At advisement in practice we distinguish whether the risk realisa tion goes on steadily by same way or variously in dependence on immediate site and time conditions of assets. The principal attributes of each risk are uncertainty and vagueness, and therefore, the paper deals with their sources. The classical statistical methods as computation of dependences, time series analyses and cluster analyses do not fulfil the demands necessary for work with data having dif ferent accuracies in different time periods, incom

pleteness and inhomogeneity, and therefore we must

apply special methods as fault tree, process models,

extreme methods, fuzzy techniques etc. and differ

ent approaches from precise deterministic, through

Prochazkova, D. 2007 a. Human System Safety (in Czech).

Ostrava: SPBI, 139 p. ISBN 978-80-86634-97-5.

Prochazkova, D. 2010 b. Application of SWOT Analy

sis and of Selected Types of Case Studies at Selection

of Model for Strategic Territory Safety Management (in Czech). Zilina: ENVIRO, STRIX ann. Gillian 2010, ISBN 978-80-89281-56-5, 348–384. Prochazkova, D. 2011 c. Methods, Tools and Techniques for Risk Engineering (in Czech). Praha: CVUT, in print. p. 289.

Importance measures and common-cause failures in network reliability

C. Tanguy

Orange Labs, Carriers and Networks, Issy-les-Moulineaux, France

ABSTRACT

We consider the influence of common-cause

failures on a few of the most popular—Birnbaum,

Improvement Potential, Risk Achievement Worth,

and Fussell-Vesely—importance measures in the

context of the reliability of network connections.

We first show how the well-known definitions can

be simply extended to systems undergoing com

mon-cause failures, and show how calculations

can be performed for networks made of identical elements. Different models of common-cause failures are then implemented in order to assess the changes of importance measures. A case study of a simple network architecture constituted by 9 nodes and 14 links allows to infer the expected behavior for larger configurations.

In many network reliability studies, com ponents are usually assumed to fail independ ently of each other. This is not always realistic. Common-Cause Failures (CCFs) certainly occur, and it is important to assess their influence on the availability of a connection (it can actually increase or decrease). Importance factors such as the Birnbaum, Improvement Potential, Risk Achievement Work, Fussell-Vesely factors are crucial to the system designer since they provide information on the parts of the system that must be updated/improved in order to increase the sys tem's performance. However, their definition relies on the independent behavior of all the elements. We investigate the possible influence of CCFs on the ranking of the network elements, in comparison with what happens when elements are statistically independent, as is mostly assumed. We first provide

generalizations of several well-known importance

factors that apply when correlations between ele

ments occur. Then we study the possible rank

ing changes in a case study (see Figure 1), where

the medium-sized meshed network is a reason

able starting point to a better understanding of

large systems. The four importance factors men

tioned above are calculated exactly for each of the

fourteen elements, and ranked for three different

models of CCFs, namely the β-factor model, the

binomial failure rate model and the degenerate p 6 p 1 p 2 p 3 p 4 p 7 p 8 p 9 p 10 p 11 p 12 p 13 p 14 p 5 S T Figure 1. Network configuration of Walter et al. Figure 2. Variation of the numerator of the Fussell-Vesely importance factor as a function of β, for the fourteen links. 0.0 0.2 0.4 0.6 0.8 1.0 0.0000 0.0001 0.0002 0.0003 0.0004 0.0005 0.0006 I FV β multidimensional normal distribution—a particular case of the Gaussian copula—in order to detect possible general behaviors. An example is given in Figure 2, which displays the Fussell-Vesely importance factor when the common-cause failures are described by the β-factor model. It shows a general increase of this factor for all the elements, when β goes to 1 (the fully correlated configuration). However, the relative ranks of two elements do not necessarily change. This seems to be quite characteristic: adding CCFs to the description of a system does not profoundly change the ranking of the elements, when compared to the standard “independent behavior” result: “important” elements remain so. This study also shows that the ranking offered by the “family” of Birnbaum, Improvement Potential, and Risk Achievement Work factors differs substantially from that offered by the Fussell-Vesely one.

Multivariate Gumbel distributions for Reliability Assessment

B.J. Leira & D. Myrhaug

Department of Marine Technology, NTNU, Trondheim, Norway

ABSTRACT

A bivariate Gumbel distribution is established based on transformation of an existing bivariate Rayleigh distribution, see Rice (1944, 1945), Longuet Higgins (1986), Goda (1976), Kimura (1980), Tayfun (1990), Myrhaug et al. (1995). Application of this distribution in relation to reliability assessment of marine structures is subsequently addressed. An example of a linear combination of the two basic variables which are Gumbel distributed is fur ther considered in connection with a mono-tower structure.

The role of the Gumbel distribution in con nection with reliability assessment of marine structures is discussed for the case of multiple “iso chromatic” response processes.

Comparison with another class of bivariate Gumbel distributions (Gumbel Type A, see Gumbel (1958), Johnson and Kotz (1972)) is also made.

Nonparametric predictive inference for reliability of a series of subsystems with multiple component types

A.M. Aboalkhair

Department of Mathematical Sciences, Durham University, Durham, UK

Department of Applied Statistics and Insurance, Mansoura University, Mansoura, Egypt

F.P.A. Coolen & I.M. MacPhee

Department of Mathematical Sciences, Durham University,
Durham, UK

ABSTRACT

The nonparametric predictive inference (NPI) approach to system reliability explicitly reflects that limited knowledge about reliability of components, resulting from testing, leads to dependence of the reliabilities of components of the same type in a system. Coolen et al. (2011) presented NPI for reliability of a single voting system consists of multiple types of components. They are assumed to all play the same role within the system, but with regard to their reliability components of different types are assumed to be independent. The information from tests is also available per type of component. This paper presents the NPI approach for systems with subsystems in a series structure, where all subsystems are voting systems that can have components of the same types. As NPI uses only few modelling assumptions, system reliability is quantified by lower and upper probabilities, reflecting the limited information in the test data. The results are illustrated by examples, which also illustrate important aspects of redundancy and diversity for system reli

ability. It is particularly logical to focus attention

on the NPI lower probability in the examples, as it

can be considered to be a conservative inferenc.

EXAMPLE

Two different systems, each having components of

T = 2 types A and B, are considered. The first is a

k-out-of-24 system with m a = m b = 12. The second

consists of L = 2 k i -out-of-12 subsystems in series

configuration with m m m m a b a b 1 1 2 2 6= = = . The

NPI lower probabilities for the event that a system

functions successfully are presented in Table 1, for

different test data and some different values of k,

k 1 and k 2 . It is clear that the system reliability, as

measured by this NPI lower probability, increases

sub-stantially for decreasing k or k 1 and k 2 , so if

fewer of the 24 components have to function, and

also for increasing numbers of tested components

if these were all successful. If all components in

the system must function the reliability tends to be Table
1. NPI lower probabilities for two different systems. n s
Sys1 k = 21 Sys2 k 1 = 10 k 2 = 11 Sys1 k = 22 Sys2
k 1 = 11 k 2 = 11 Sys1 k = 24 Sys2 k 1 = 12 k 2 =
12 1 1 0.059 0.041 0.036 0.027 0.006 0.006 2 2 0.173 0.123
0.110 0.086 0.020 0.020 3 3 0.294 0.214 0.196 0.155 0.040
0.040 2 0.023 0.014 0.012 0.007 0.001 0.001 5 5 0.500 0.382
0.360 0.292 0.087 0.087 4 0.110 0.070 0.057 0.040 0.005
0.005 10 10 0.783 0.650 0.640 0.547 0.207 0.207 9 0.416
0.292 0.263 0.199 0.038 0.038 8 0.160 0.099 0.079 0.055
0.006 0.006 20 20 0.944 0.855 0.862 0.783 0.391 0.391 24 24
0.964 0.890 0.900 0.829 0.444 0.444 30 30 0.980 0.923 0.935
0.876 0.510 0.510 very small for cases where some
components failed in the tests, which is logical as the

test information only provides weak support for this event. For both these systems, the lower probabilities in the two final columns are identical as in these cases the systems only function if all 24 components function. The other cases give different results due to the different system configurations. For example, 22-out-of-24 system functions for more combinations of failing components than two 11-out-of-12 subsystems in a series configuration, for example the former system still functions if there are two failing components both in the same subsystem, in which case the latter system would not function. This explains why the entries related to the first system (Sys1) are greater than those for the corresponding cases, with k 1 + k 2 = k, related to the second system (Sys2). REFERENCE Coolen, F.P.A, Aboalkhair, A.M. & MacPhee, I.M. 2011. Diversity in system reliability following component testing, Journal of the Safety and Reliability Society 30, pp. 75-93.

Numerical method for the distribution of a service time of a structure

subject to corrosion

Adrien Brandejsky, Benoîte de Saporta & François Dufour

INRIA, Team CQFD, France

Charles Elegbede

Astrium, France

ABSTRACT

We propose a numerical method to compute the

service time of an aluminum structure subject to

corrosion. This example is provided by Astrium.

The structure is part of a strategic ballistic missile

stored in a nuclear submarine missile launcher

and is therefore submitted to strong reliability

constraints. We study the loss of thickness by cor

rosion and more precisely, the distribution of the

service time of the structure: the time taken by the thickness loss to reach a critical threshold. We model the evolution of the thickness loss by a hybrid process belonging to the class of piece wise-deterministic Markov processes (PDMP) introduced by M.H. Davis in (Davis 1993). The service time of the structure is thus an exit time for the PDMP. Our approach is based on the special structure of the PDMP, namely the fact that the only source of randomness of the process is a dis crete time Markov chain. We propose a suitable discretization algorithm for this Markov chain based on quantization. For details on the quan tization algorithms, the interested reader may consult (Pagès, Pham, and Printems 2004) and the The approximation we propose may be eas ily implemented. Furthermore, and this feature is an important advantage over standard methods such as Monte-Carlo simulations, it is flexible with respect to the threshold we consider. Indeed, in practice, one begins with the preliminary computa tion of the quantization grids that only depend on the dynamics of the process, in our case the corro sion evolution equation. These grids are stored off line. Next, our method yields, in a very simple way,

an approximation of the law of a wide range of service times. This flexibility allows, for instance, to modify the critical threshold and obtain the law of the new exit time with very little further com putation. Eventually, we stress the fact that our whole study is rigorous since we provide proofs of convergence of the algorithm in (Brandejsky, de

On generalized shot noise-type stochastic failure model

J.H. Cha

Ewha Womans University, Seoul, Republic of Korea

M. Finkelstein

University of the Free State, Bloemfontein, South Africa

ABSTRACT

We discuss a reliability model that reflects the dynamic dependency between system failure and system stress induced by environmental shock process. Standard assumptions in shock models are that failures of items are related either to the cumulative effect of shocks (cumulative models) or that they are caused by shocks that exceed a certain critical level (extreme shocks models). In this paper, we present useful generalizations of this setting to the case when an item is deteriorating itself, e.g., when the boundary for the fatal shock magnitude is decreasing with time.

Shock models usually consider systems that

are subject to shocks of random magnitudes at

random times. Traditionally, one distinguishes

between two major types: cumulative shock mod

els (systems break down because of a cumulative

effect) and extreme shock models (systems break

down because of one single large shock). Some

Sumita (1984), Sumita & Shanthikumar (1985),

Gut (1990), Mallor & Santos (2003), Finkelstein (2008), Cha & Finkelstein (2009), Finkelstein & Marais (2010). A combination of these models was investigated by Gut & Hüsler (2005), where the failures were due either to a cumulative effect, or to a single, fatal shock. In this paper, we are somehow in the framework of the latter setting generalizing it to the case when a system itself (apart from the shock process) is deteriorating with time. However, mathematically, our approach is closer to the paper by Lemoine & Wenocur (1986) (see also Lemoine & Wenocur, 1985) and is based on considering the shot noise process-type stochastic intensity as a model for shocks accumulation. In Lemoine & Wenocur (1986), the system cannot fail directly from a critical shock. However, in many cases, systems can fail due to a shock of a great magnitude. Thus the main goal of our paper is to generalize the model in Lemoine & Wenocur (1986) to the case when a system can also fail due to a fatal shock with the magnitude exceeding the time-dependent bound, which is more realistic in practice. Some illustrative examples are also discussed.

Probabilistic prognosis of a system: Application to a pneumatic valve

A. Lorton

EADS-Innovation Works, ICD—Université de Technologie de Troyes, UMR STMR—CNRS, France

M. Fouladirad & A. Grall

ICD—Université de Technologie de Troyes, UMR STMR—CNRS, France

ABSTRACT

In the aeronautic industry, the optimisation of the maintenance process is one of the main research goal for economical, ecological and industrial purposes. An interesting approach consists in using Condition-Based Maintenance (CBM) to act on the system based on its current state and before its failure. It requires the computation of the remaining time before this failure occurs, called the Remaining Useful Life (RUL) of the system (see (A. Saxena 2010)). This computation is what we called a prognosis problem. In the present paper, we consider a probabilistic model-based prognosis. The probabilist framework indeed allows to take into account the uncertainties inherent in this problem (unknown degradation process, forecast on some future conditions, complex system, …). The model-based aspect provides a natural way to integrate expert knowledges on the physical behaviour of a system.

We first define our prognosis problem in mathematical terms, and propose a methodology to solve it for specific cases. We consider a stochastic process Z = (Z t) t∈R , modeling the degradation state of the system through time. The RUL at a prog

nosis time t, namely RUL t is then define as the

smallest time s after t when the system is consid

ered as useless. Since z is a stochastic process, the

RUL t is a random variable for each t. A first idea

is to compute its cumulative distribution function.

However, to specify a prognosis for a particular

system, it is essential to integrate the informa

tion available through monitoring or inspections.

A prognosis result adapted to each situation is

then the conditional distribution function of RUL t

with respect to the observation process.

We then propose a way to approximate this

Reliability of the power electronic components by their dynamical

simulation in real working conditions

Jérôme de Reffye

Pi-Ramses Cy, Versailles, France

ABSTRACT

The actual forecast of the reliability of the

electronic components is based on methods

using analytical formulations established from

experimental data. An upgrading processing was

operated from the MIL HDBK 217 to the FIDES

methodology. But these approaches give only

the reliability of components without functional

analysis.

Moreover these approaches supply only param
eters of reliability that are smoothed by the data
processing of the return of experiment and the
used empirical formulations. The rates of failure
that are supplied suffer a bias between the system
in which the components work and the systems
that are the origin of the reliability data.
In a same way the variance of the rates of fail
ure is made of the uncertainties of the data of the
return of experiment and these data are unknown.
If one needs only rough results on parameters of
reliability such methods are useful because they are
very easy to use. But if we want to analyse the reli
ability of a real system as control-command sys
tem and its real characteristics in operation such
methods are inappropriate.
It becomes very important to know the prop
erties of electrical networks and the conditions
of work of the power semi-conductors in these
networks to estimate really the parameters of reli
ability of the power electronic systems. This is the
reason why we propose an approach of the reliabil
ity of the electronic systems based on the physical
knowledge of the behaviour of the components of

these systems. The electronic cards are analysed

Scenario analysis and PRA: Overview and lessons learned

Diego Mandelli & Tunc Aldemir

Nuclear Engineering Department, The Ohio State University, OH, US

Alper Yilmaz

Photogrammetric Computer Vision Laboratory, The Ohio State University, OH, US

ABSTRACT

The recent trend to use a best estimate plus uncertainty (BEPU) approach to nuclear reactor safety analysis [1] instead of the traditional conservative approach can produce very large amounts of data. Hence, the need for methodologies able to handle high volumes of data in terms of both cardinality (due to the high number of uncertainties included in the analysis) and dimensionality (due to the complexity of systems) arises. Clustering methodologies [2] offer powerful tools that can help the user to identify scenario groups that are representative of the data and, hence, can reduce the effort involved in data analysis. By scenario clustering we mean two actions:

- Identify the scenarios that have a similar behavior (i.e. identify the most evident classes)
- Decide for each event sequence to which class it

belongs (i.e., classification)

In the past few years, the Nuclear Engineering Program at The Ohio State University has been involved in the development of such clustering methodologies and algorithms. The specific type data under consideration are those generated using the Dynamic Event Tree (DET) [3] approach for nuclear power reactor transients described by a large set of state variables (i.e., tempera ture, pressure of specific nodes in the simulator)

Small failure probabilities and copula functions: Preliminary studies on structural reliability analysis

E.A. Tamparopoulos, P. Spyridis & K. Bergmeister

BOKU University of Natural Resources and Life Sciences, Vienna, Austria

ABSTRACT

In the present study, the concept of copula functions is used for the construction of multivari ate models. Moreover, an evaluation of the struc tural reliability approach is attempted with respect to the uncertainty owing to assumed correlation coefficient values. Based on a probabilistic analysis of a particular construction system, the problem of evaluating small failure probabilities is discussed in the light of the aforementioned uncertainty.

A stochastic analysis of a single anchor under tension, failing with concrete cone breakout, shown in Figure 1, is considered as a case study. The system's ultimate load can be calculated by means of two correlated concrete parameters, namely the modulus of elasticity E_c and the fracture energy G_f. The effect of various dependence models can be then demonstrated either by calculating the ultimate load value for different predefined failure probabilities, or by calculating the probability of failure for various assumed system loads. In order to evaluate the significance of the underlying dependence structure, three different bivariate models, built upon the theory of copula functions, with Pearson's correlation coefficient $r = 0.5$, and

Figure 1. Single concrete anchor failing with concrete cone failure.

Structure decision making for MSS refrigeration system

Ilia Frenkel & Lev Khvatskin

Center for Reliability and Risk Management, SCE—Shamoon College of Engineering, Beer Sheva, Israel

Anatoly Lisnianski

Reliability Department, The Israel Electric Corporation Ltd., Haifa, Israel

ABSTRACT

Supermarkets suffer serious financial losses

because of problems with their refrigeration sys
tems. Principal refrigeration system includes 4
basic elements: compressors, evaporators, thermo
expansion valves and roof top condensers with
blowers. Due to the system's highly integrated
nature, a fault in a single unit can't have detrimen
tal effects on the entire system, only decrease of
system cooling capacity. Failure of compressor
or axial condenser blower leads to partial system
failure (degradation of output cooling capacity) as
well as to complete failures of the system. We treat
refrigeration system as Multi-State System (MSS),
where components and systems have an arbitrary
finite number of states. According to the generic
MSS model (Lisnianski et al., 2010), the system
can have different states corresponding to the sys
tem's performance rates, which are discrete-state
continuous-time stochastic processes.
In this paper, a generalized approach is applied
for decision making for multi-state supermarket
refrigeration system structure. The approach is
based on the combined Universal Generating
Functions (UGF) and stochastic processes
method for computation of availability, output
performance and performance deficiency for

multi-state system.

We consider a typical refrigeration system that is used in one of Israeli supermarkets (Frenkel et al. 2010). The system consists of 2 identical subsys tems: main and reserved. Each subsystem consists from 2 elements: block of 4 compressors and block of 2 axial condenser blowers. The way to growth availability of the system is to replace block of 2 axial condenser blowers on the block of 3 axial condenser blowers. One should compute reliability indices for these two possible structures and make the decision—what structure is more appropriate. Calculation reliability indices (availability, out put performance and performance deficiency) for

The Inverse Gamma process for modeling state-dependent deterioration processes

M. Guida

Department of Electronic and Computer Engineering, University of Salerno, Fisciano, Italy

G. Pulcini

Istituto Motori, CNR, Naples, Italy

ABSTRACT

The Gamma process model is widely used for describing non-decreasing deterioration processes over time mainly due to its mathematical tracta bility (see, e.g., Bagdonavičius & Nikulin (2000)).

The property of “independence of increments”, however, confines the use of this model to deterioration mechanisms where the probability distribution of deterioration increments depends on the current time t and not on the current state of the unit at time t.

Although the description in terms of the degradation level as a function of time, say {W(t), t ≥ 0}, is the usual “direct” way of modeling a deterioration mechanism, it makes also sense (e.g., for reliability evaluations) to consider the “inverse” process {T(w), w ≥ 0}, i.e., the process of the first time for reaching the degradation level w. It is worth noting that, when the “direct” process {W(t), t ≥ 0} is a purely state-dependent process (i.e., a process where the distribution of degradation increments depends only on the current state w of the item at the time t and not on the current age t), the “inverse” process {T(w), w ≥ 0} has “independent time increments”. Then, the Gamma process model could be appropriately used to describe the process {T(w), w ≥ 0} and, in such a case, the deterioration process {W(t), t ≥ 0} is an Inverse Gamma process where the distribution of degradation increments only depends on the current state of the unit

(Harlamov, 2006).

This paper proposes non-stationary Inverse

Gamma processes for modeling state-dependent

deterioration processes with non linear trend. The

(conditional) distribution of the deterioration

growth ΔW over a generic time interval (t 0 ,t 0 + δ T),

given the current state w 0 at the time t 0 is derived in
a

closed form. The distribution of the time for reach

ing a given deterioration limit w max , as well the resid

ual lifetime and the residual reliability of the unit,

given the current state, are also provided. Maximum

likelihood estimates of the parameters which index

The method of safe 4D flight trajectory prediction in
controlled

airspace

M. Piatek

Polish Air Navigation Services Agency, Warsaw, Poland

A. Stelmach

Warsaw University of Technology, Faculty of Transport,
Warsaw, Poland

ABSTRACT

A number of trajectory modeling methods have

been proposed to automate air traffic conflict

detection and resolution (Kuchar, Yung 2000),

several of which had been in use or under opera

tional evaluation. Most of described modeling methods have been built from a foundation of structured routes and evolved procedures. The proposed model aims the issues of modeling a safe 4D flight trajectory of aircraft in a future controlled airspace where the structured routes will be used only in high density traffic areas and the airspace free of predetermined routes will be used to manage traffic flows.

The elaborated method of planning the 4D trajectory allows to:

- verify the separation of the aircrafts,
- check the separation of the trajectory from the elements of the airspace,
- set a different flight trajectory in order to avoid a potential midair collision or in case there is no possibility for take-off or landing with given flight parameters,
- set all trajectories in such a way that the aircrafts landing in the same airports would enter the controlled airport area keeping appropriate separations,
- set all trajectories with minimum total fuel consumption and with the smallest number of changes in the flight parameters (direction, alti

tude and speed).

The proposed model of controlled airspace

(Piatek M., 2010) includes randomly planned air

routes as well as criteria of choosing safe and sepa

rated flight trajectories. Modified Dijkstra algo

rithm (Dijkstra, 1959) has been used for model

implementation.

The elaborated concept aims at increasing the

capacity of the sectors responsible for operational

planning in future and current structures of the

controlled airspace, maintaining the safe and

Process oriented simulation framework for Common-Cause Failure

assessment

E. Bejdakic, M. Krauß & H.-P. Berg

Bundesamt für Strahlenschutz (BfS), Germany

ABSTRACT

Dependent failures, in particular so-called Com

mon Cause Failure (CCF), are extremely impor

tant in reliability and safety analysis due to their

potential to lead to a simultaneously loss of sev

eral redundant systems or components. Therefore,

consequences of common-cause failures are one of

the major issues in probabilistic safety assessment,

not only of nuclear power plants, and must be ade

quately treated to minimize an underestimation of

reliability. Experience from numerous probabilistic safety assessments has shown that, especially for highly redundant systems in nuclear power plants, common cause failures can dominate the results of these assessments such as the core damage fre quency or large early release frequency. Depend ing on the studies considered and especially the design of the respective nuclear power plant ana lysed, failure of several components can contrib ute between twenty and more than eighty percent to the system unavailability which is correlated to the calculated value of the core damage frequency in case of nuclear power plants. Due to the small number of observed events resulting from identi fied common cause failures, it is difficult to assess this issue in the short run. It is therefore necessary to gather data over an extended period of time and test various models against that data.

Process Oriented Simulation framework (POS) (?) is an approach for quantification of component unavailability caused by common-cause failures. It can be seen as an extension of the Binomial Fail ure Rate model (BFR) (?, ?) and was introduced in the 1990s. POS model uses Monte Carlo simu lation technique to compute the unavailability of

components. The POS model distinguishes explic

itly between immediate and delayed failures and it

does not assume that all components are affected

by the Common Cause (CC). Instead, it treats the

number of components affected by CC as a sto

chastic variable. Further, the POS model has the

ability to model various relevant stages of the CCF

process, hence the name of the model. In this paper,

we use the standard Maximum Likelihood Estima

tion (MLE) method and apply it on accumulated

isolating slide valve data from German nuclear

The unique signal applied to weapon system safety design

L.Y. Xiao, J. Li, B. Suo & S. Li

Institute of Electronic Engineering, China Academy of Engineering Physics, China

ABSTRACT

Because of the safety of weapons is very important,

many safety design methods have been produced.

The fuze safety system pays an important part in

the weapon safety design. In general design method,

multiple environmental signal and safety switch are

used to achieve safety goal. This will lead to com

plex of the system, and the quantization of the

safety failure rate is made difficult. Then, there is

an integrated concept to approach the above men

tioned problems: an arming signal, which can not be generated in normal or abnormal environment, should be found, the probability of whose acciden tal occurrence is low and the quantization of which is easy. And this can be called the “unique signal”.

The UQS methodology provides resistance to various threats that might be present in abnormal environments, in particular significantly reducing vulnerability to non-random threats, while opti mizing resistance to random threats.

The unique signal is a binary sequence the ele ments of which are all taken from the set I = (A, B), marked C k , having a length marked n. And this is a pseudorandom sequence. If the accidental occur rence probability of C k is P (C k) and ε is a small enough positive number, C k is a unique codes whose occurrence probability is smaller than ε and ε is the maximum occurrence probability.

The UQS codes consist of three elements: event, pattern and length. The UQS pattern refers to the particular sequence, where lies the core of the uniqueness of the UQS codes. And an UQS pat tern is supposed to meet the following selection criteria:

a. the number in the event As and event Bs are

equal or seem to be equal to each other;

b. the number of the event pairs (AA, AB, BA, BB)

are equal or seem to be equal to each other;

c. the recurring event string (run-length) should

be as short as possible, where the length of the

maximum run cannot exceed 4 and the inversed

UQS codes and the complementary codes are

tested with the maximum run-length;

Uncertainty analysis via failure domain characterization: Polynomial

requirement functions

L.G. Crespo

National Institute of Aerospace, VA, US

C.A. Muñoz, A.J. Narkawicz, S.P. Kenny & D.P. Giesy

NASA Langley Research Center, Hampton, VA, US

ABSTRACT

This paper studies the reliability of a system for

which a parametric mathematical model is avail

able. The acceptability of the system depends upon

its ability to satisfy several design requirements.

These requirements, which are represented by a set

of inequality constraints on selected output met

rics, depend on the uncertain parameter vector p.

The system is deemed acceptable if all inequalities

are satisfied. The constraints partition the uncer

tain parameter space into two sets, the failure

domain, where at least one of them is violated, and the safe domain, where all of them are satisfied. The reliability analysis of a system consists of assessing its ability to satisfy the requirements when p can take on any value from a prescribed set. The most common practice in reliability analysis is to assume a probabilistic uncertainty model of p and estimate the corresponding probability of failure. Sampling-based approaches (Niederreiter 1992, Kalland Wallace 1994) and methods based on asymptotic approximations (Rackwitz 2001) are the engines of most of the techniques used to estimate this probability.

Reliability assessments whose figure of merit is the probability of failure are strongly dependent on the uncertainty model assumed. Quite often this model is created using engineering judgment, expert opinion, and/or limited observations. The persistent incertitude in the model resulting from this process makes the soundness of the reliability analyses based on failure probabilities questionable. Furthermore, the failure probability fails to describe practically significant features of the geometry of the failure event. Some of these features are the separation between any given point and the failure domain, the location of worst-case uncertainty combinations, and the geometry of the failure domain boundary. This paper proposes an uncertainty analysis framework based on the characterization of the uncertain

parameter space. This characterization enables the evaluation of the features listed above, the approximation of the failure and safe domains and the calculation of arbitrarily tight bounds to the failure probability. A significant thrust of this research is the generation of sequences of inner approximations to the safe and failure domains by subsets of readily computable probability. These sequences are chosen such that they almost surely fill up the region of interest. The strategies proposed, which are only applicable to requirement functions having an explicitly known polynomial dependency on the uncertainty, are based on Bernstein expansions and sum of squares programming. Some of the most prominent features of the methodology are the substantial desensitization of the calculations from the uncertainty model assumed as well as the accommodation for changes in such a model with a practically insignificant amount of computational effort. The companion paper (Crespo et al., 2011) proposes strategies with the same goal but applicable to unrestricted requirement functions.

Uncertainty assessment in semi Markov methods for Weibull functions distributions

M. Zajac & A. Kierzkowski

Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Dependability indices like reliability and related measures, as availability, maintainability, failure rate, mean times, etc., are very important in design, development and lifetime analysis of real systems. It is worth to point out that there is an assump tion that during the calculation of the dependabil ity contributors for technical objects that are under investigation, probabilities of transition between states or sojourn times' probabilities are exponen tial. Many causes, for example, lack of informa

tion, small sample sizes, or inaccurate assessment of data may result in the model assumptions being violated. In some cases, when exponential distribu tion is assumed, there is also possibility to assess factors according to different distributions, like Weibull, Erlang, etc.

Probabilities of transition between states and availability belong to the fundamental character istic of reliability. The discrete-time case can be obtained from the continuous one, by considering counting measure for discrete time points. However we consider that important is to make it separately for this case, since an increasing interest is observed in practice for the discrete case. There are attempts to calculate factors with continuous-time in liter ature, however calculations are prepared using exponential functions distributions. In engineering practice it very important to obtain accurate results without using strong simplifications.

The paper consists of discussions about the possibility and about the reason of carrying out these calculations, which is made by the application of simple models of the Markov and Semi-Markov processes, where there are attempts of use of continuous time in these calculations. Discussion

is based on hypothetical exponential and non exponential sojourn times' probabilities. Valuation of these methods is based on the comparison of availability and probabilities of transition values when using exponential and Weibull functions distributions. Previous experience presented in

An engineering and psycho-social integrated approach for Work-Related Stress (WRS) assessment and management

P. Citti
Università degli Studi "G. Marconi" di Roma, Rome, Italy
M. Delogu, A. Meneghin & F. Pagliai
Università degli Studi di Firenze, Florence, Italy

ABSTRACT

According to the Framework Directive 89/391/EEC, all employers have the duty of protecting the occupational safety and health of all workers. As suggested by the ECJ interpretation, that also concretely refers to the WHO definition of "health" ("a state of complete physical, mental and social well-being"), this duty also applies to work-related stress problems. The Framework Agreement on work-related stress of 8 October 2004, and the EU Council Resolution of 25 june 2007 confirmed and clarified the strong EU commitment to ensure health and safety at work, effectively facing work

related stress. Work-related stress problems may be handled within an overall process of risk assessment, through a methodological approach fitted for specific work-related stress risk features. Although traditionally associated to engineering, the risk assessment and process optimization methods increasingly find their application in very different contexts. Since each set of objects and people interacting with each other can be considered a system and that any sequence of activities aimed at achieving a goal can be regarded as a process, it follows that the theories and techniques developed for quality systems can become effective in very diverse fields of expertise. Furthermore, the more complex the systems become and the more processes affect the human sphere, the more it is necessary to overcome the anachronistic disciplinary boundaries.

Therefore the challenge was to look at the work related stress as a process whose variables, once identified, could be measured, analyzed, evaluated and optimized using the correct sequence of process analysis traditional tools.

This contribution pertains to the development and the outcome of an analysis and opti

mization approach performed to assess the risks of work-related stress inside the University of Florence, Italy. The activities have been led by a cross-curricular committee (quality engineering,

Applying the safe place, safe person, safe systems framework to the healthcare industry

O. Lasaki, A.-M. Makin & C. Winder
The University of New South Wales, Sydney, Australia

ABSTRACT

Makin's original Safe Place, Safe Persons, Safe Systems approach provided a strategic OHS man agement tool, derived from the literature and underpinned by the creation of a comprehensive hazard profile of the organisation in question (Makin and Winder, 2008; 2009). The original framework, consisting of sixty elements was trans formed into an assessment tool, trialed and vali dated by peer review, then applied to eight case studies, spanning different industries ranging from construction to manufacturing. It was suggested that this approach could be used universally across these industries.

Historically, the healthcare industry at the turn of the twentieth century had adopted the safety management model of high-risk profile industries

such as aviation and the nuclear industry at a time when injuries due to negligent behaviour and procedural errors were high. However, at the time of this transition, many authors had argued that the direct adaptation of safety initiatives from high reliability organisations in high risk industries to healthcare would be deficient owing to the difference in culture between industries. The subsequent framework that emerged has been referred to as being "fragmented," as a higher priority is given to patient safety than worker safety.

The focus of the present study was to conduct a literature review of safety management within the healthcare industry in order to provide a comprehensive hazard profile, identify and assess the current trends, the prevailing culture, and barriers to improvement interventions. It also sought to clarify if there was a fragmented framework and to find out what fed this pattern. The study uses the Safe Place, Safe Persons, Safe Systems assessment tool as a guide for reviewing the literature systematically, to perform a gap analysis of the current management strategies and to examine the characterisation of the hazard profile attributed to the healthcare industry in Makin's original work

and the efficacy of the assessment tool in its use

Applying the safe place, safe person, safe systems framework to the management of biohazards

A. Bamford, A.-M. Makin & C. Winder

The University of New South Wales, Sydney, Australia

ABSTRACT

Biological hazards (biohazards) are present from exposure to infectious micro-organisms, toxic substances of biological origin, and plants and animals. Animals are among the few animate objects with which workers interact, placing them in a special class of workplace hazards. Working with, or in the presence of, animal(s) requires special attention to the unique hazards they pose.

This study describes the application and evaluation of the Safe Place, Safe Person, Safe Systems framework (Makin and Winder, 2008; 2009) to the management of biohazards encountered when working with animals, with a purpose of examining the efficacy and suitability of the framework.

This study consisted of a review of the literature on biohazards in animal-related professions, typically in the context of veterinary practices and zoos, and their management in the workplace. This is a new area where the model has not been previ

ously applied.

Risks associated with working with animals

were found to be divided into three categories:

direct physical risks, infectious diseases from ani

mals (zoonoses); and hypersensitivity risks.

The framework brings together the merits of

the three main control strategies that have emerged

for dealing with workplace hazards (namely safe

place, safe person and safe systems) to ensure that

an OHS MS has been carefully constructed and

customised to the individual organisation.

For Safe Place elements, aspects that were

considered important were: (i) workplace design

and function, including access/egress, plant and

equipment, ergonomic evaluation, maintenance;

(ii) common workplace hazards, such as hazardous

chemicals, manual handling, noise and of course,

biohazards; and (iii) systems for non-routine situ

ations and adverse events, such as security and

emergency planning.

For Safe Person elements, aspects that were

considered important were: (i) obtaining good per

Cognitive, affective and behaviour outcomes of a safety training

program

L.O. Duarte

Santa Casa da Misericórdia de Lisboa, Lisbon, Portugal

S.A. Olea

Universidad León, León, Spain

S.A. Silva

ISCTE-IUL Instituto Universitário de Lisboa, Lisbon, Portugal

ABSTRACT

Safety training is a key intervention strategy for developing systems, methods and actions that allow more and better safety performance and con tributes for changing or developing organizations safety culture.

Moreover, training is well recognized as essential for improving and supporting people safety com petencies and actions (e.g., KSAO—knowledge; skills; attitudes and others). For instance, it is expected that training increase safety knowledge (e.g., learning about risks), perceptions (e.g., safety climate), attitudes (e.g., satisfaction with safety), and behaviours (e.g., compliance and participa tive behaviour). Therefore, it should contribute for individuals cognitive, affective and behaviour change.

Although there is already a consistent body of research showing safety training positive effects

and important issues for improving its efficacy (e.g., Colligan & Cohen, 2004; Burke et al., 2006) only very few studies assessed multiple and across time effects for a specific safety program. The present study intends to fulfil this gap.

Departing from Kirkpatrick seminal work (e.g., Kirkpatrick & Kirkpatrick 2006) and most update knowledge about training (e.g., Aguinis, 2009; Ford, Kraiger, Merritt, 2009) and safety train ing (e.g., Burke et al., 2006) a pre-post test design study was used to assess the outcomes of a safety program.

The study was conducted in four phases which include: 1) initial assessment conducted 15 days prior to training (covering safety perceptions, attitudes and behaviours); 2) evaluation of safety knowledge one hour before the start of training;

Manual handling operations risk assessment

A.R. Burcíaga-Ortega & J.R. Santos-Reyes

Safety, Accident, Risk & Reliability Analysis (SARACS) Research Group, SEPI-ESIME, IPN, Mexico

ABSTRACT

It is believed that every year more than 2 million people die from occupational accidents or work related diseases. Moreover, there are 270 million

occupational accidents and 160 million cases of occupational disease (ILO, 2010). On the other hand, these figures vary enormously between countries, economic sectors and social groups. Furthermore, deaths and injuries take a particu larly heavy toll in developing nations, where large numbers of people are engaged in hazardous activities such as agriculture, construction, log ging, fishing and mining, etc. (ILO, 2010). Muscu loskeletal Disorders (MSD) constitute the largest category of work-related illness in developed and developing countries, and are a major source of pain, disability, restricted activity, lost work days, reduced productivity, and costs to industry and the public service (Dampsey & Hashemi, 1999). For example, the authors found that manual materials handling represented the largest source of claims. These results were compared with those reported by some authors who found that manual materials handling accounted for between 24% and 35% of all injuries.

Given the above, it is clear that manual handling operations may be regarded as a major cause of injury and ill-health in the work place. In order to address these issues, some countries have intro

duced regulations aiming at preventing MSD related illness. For example, the Manual Handling Operations Regulations 1992 (MHOR) were introduced from 1 January 1993 in the UK (HSE, 1998). Some similar steps have been implemented in the USA. In view of the individual distress, occupational limitations, and economic costs associated with MSD, the topic has attracted much research attention in the fields of epidemiology, medicine, physiology, and psychology. However, there is no evidence of studies associated with MSD being conducted in Mexico.

This paper presents the results of a study con

Measurement of safety social norms at organizations: Construct validation of a safety social norms survey

C.S. Fugas & S.A. Silva

Lisbon University Institute, Portugal

J.L. Meliá

University of Valencia, Spain

ABSTRACT

Attempts to minimize errors and reduce accidents have been predominantly purely reactive, after the occurrence of accidents. The measurement and analysis of safety social norms can be a way to manage safety on a proactive basis in order to improve

the safety of individuals in the workplace.

Extending recent findings that social proc
esses underlying safety at work are multidimen
sional and can impact safety behaviors differently
(Fugas, Meliá & Silva, 2009), the present study
was designed to test the reliability and construct
validity of a questionnaire devoted to the meas
urement of social influences on safety behavior.
This instrument can be useful as a diagnostic tool
for intervention aimed at improving safety of the
organizations in different industrial sectors.

Following Cialdini and Trost (1998) assump
tions, in this paper, safety group norms are con
sidered as informal safety internalized rules
emanating from relevant group figures that work
groups adopt to regulate group member's behav
ior and that are used to infer acceptable behavior.
Norms include not only a prescriptive element, but
also a descriptive element. Descriptive norms refer
to perceptions of others' safety behavior, based on
observations of how supervisors and coworkers
participate in and comply with safety practices and
injunctive norms refer to the perceived approval of
proactive and compliance safety practices (Fugas,
Meliá & Silva, 2011). In contrast to the descrip

tive norms, which specify what is done, injunctive norms specify what should be done.

The results of this study confirmed the reliability and validity of constructs of the Safety Social Norms Survey. The CFA has played an important role in assessing the dimensionality of the constructs proposed in this study. Results showed the factor structure proposed for 4-factors related to safety social norms. Supervisors and coworkers' descriptive and injunctive norms are not isomorphic constructs, but refer to dif

Organizing for quality and safety in health care—the Norwegian case

S. Wiig

University of Stavanger, Norway

J. Quartz

Erasmus University, Rotterdam, The Netherlands

C.v. Plessen

University of Stavanger, Norway & Hillerød Hospital, Denmark

S. Harthug

Haukeland University Hospital & University of Bergen, Norway

ABSTRACT

Quality and patient safety can be considered as complex processes in socio-technical systems depending on structures, process and information

flow between different institutions, organizations and stakeholders. In order to map vital institutions and their relationships and activities to improve quality and patient safety one should approach them from a multi-level perspective (e.g., Wiig, 2008; Rasmussen, 1997) incorporating the macro (national health care system), meso (hospital) and micro (frontline clinical teams) levels. Despite growing awareness of quality and patient safety risks, and significant effort to improve, progress is hard to measure (Goeschel et al., 2010).

In the Norwegian context the patient safety research and efforts related to organizing for patient safety in external and local governance sys tems is in its infancy. The aim of this paper is to describe the organization of the Norwegian system for patient safety and quality improvement.

The paper reports results from a pilot study of the Norwegian health care system (van de Bovenkamp et al., 2011). Data collection has been conducted through a triangulation of semi-structured interviews and document analysis. We have performed 20 interviews with informants representing organizations and institutions on macro, meso, and micro level.

Organizing for quality and safety in the

Norwegian context strongly relies on state insti

tutions and self-regulation as part of the exter

nal governance system. In the local governance

system internal control is the main mechanism in

organizing for quality and safety. At the macro

level a national health plan and a national strat

egy for quality improvement has played a vital role in increasing attention to quality improvement at different system levels. At the meso and micro level effort is still needed to increase the status of the quality and patient safety initiatives. The informants at the meso and micro level argue for the importance of bottom-up approaches in the Norwegian context. Informants at the micro level rely on their professional international communities and argue for a higher trust in guides and guidelines developed by the professional communities compared to guides and guidelines established and distributed by Norwegian state organizations. The specialized health care sector has been exposed to major structural changes such as hospital mergers and health care reforms the past years. Presently, changes in the legal framework are on public hearing. Several of the suggested changes are related to organizing for quality and patient safety such as the organizing of the error reporting system; the role of the regulator; and new legal requirements related to quality improvement and patient safety. The effort to improve organization of quality and safety is increasing at different system levels in the Norwegian case. However the meso and micro level still lack resources resulting in improvement efforts prone to priority issues and lack of enthusiasm.

ACKNOWLEDGEMENTS The study is part of the EU-project Quality and Safety in European Union Hospitals. A researchbased guide for implementing best practices and a framework for assessing performance (QUASER). The authors wish to thank the European Commission for funding this research.

Goeschel, C.A., Wachter, R.M. & Pronovost, P.J. (2010).

Responsibility for Quality Improvement and Patient

Safety. CHEST, Vol. 138, No. 1, pp. 171–179.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, Vol. 27, No. (2-3), pp. 183-213. van de Bovenkamp, H., Quartz, J., WeggelaarJansen, A.M. & Bal, R. On behalf of the QUASER research team (2011). Guiding quality work in European hospitals. (Paper F). Wiig, S. (2008). Contributions to Risk Management in the Public Sector. PhD Thesis UiS no. 48- February 2008. University of Stavanger.

Safety design of high consequence systems based on first principles

S. Li, J. Li, B. Suo & L.Y. Xiao

Institute of Electronic Engineering, CAEP, Sichuan, China

ABSTRACT

High Consequence Systems (HCSs) are those which would bring on some potential catastrophes when accidents occur. For example, nuclear weapons, manned spaceships, nuclear power stations fall into this category. It is crucial but extremely difficult to design assured and quantified safety consequence systems to avoid political storm, social instability or economic loss. Fortunately, lots of problems are solved by safety design approach based on first principles, which makes use of the fundamental characteristics inherent in the physics and/or chem istry of a material in order to provide a predictable response of a component when subjected to spe cific environmental stimuli. An example of a first principles design approach is the use of a material

having a well-defined melting point in the design of a component that is required to fail safe if a certain undesired threshold temperature is exceeded. Rather than utilizing an active heat sensor in order to detect and then send a signal to some safing circuit, the material will instead inherently melt and fail safe. In this paper, the authors present their work on safety design of HCSs based on first principles about how to analyze system precondition and get the safety critical component. The detailed design approach of safety critical components, which utilizes the intrinsical physical/chemical characteristic of material to eliminate the hazard after identification, is proposed to guide the safety design of other HCSs. Then the most successful use of first principles technology, which induce the invention of ENDS (Enhanced Nuclear Detonation Safety) presented in Arming & Fuzing (A&F) system of nuclear weapons, is particularly specified in this paper about how to achieve its safety design goal. A&F system, the primary function of which is outputting detonating signal to detona

The contribution of balanced scorecards to the management of occupational health and safety

F. Juglaret

Preventeo and Mines-ParisTech, Sophia-Antipolis, France

J.M. Rallo

Preventeo, Le Cannet, France

R. Textoris

L'Oreal, Aulnay sous bois, France

F. Guarnieri & E. Garbolino

Mines-ParisTech, Sophia-Antipolis, France

ABSTRACT

While it has been established for many years that the management of Occupational Safety and Health (OSH) is carried out by means of Management Systems, the question of how to measure the performance and the control of these systems is still current. This article addresses this problem, and discusses the contribution of the use of Balanced Scorecards.

Management Systems are the combination of many interacting processes, which are usually the result of standards implementation (OHSAS 18001, ILO, etc.). These processes are generally organized along the same lines; the logic being one of continuous improvement. Traditionally, performance indicators have been used to measure the performance of Management Systems: the frequency and severity of absences due to sickness,

and work-related diseases. These traditional, ret

rospective indicators have several constraints and

limitations. First, they are based on historical

results and cannot be used to handle anomalous

situations that have not arisen before. In addition,

benchmarking is made difficult because the

indicators, by their very nature, are heterogeneous.

If the primary purpose of a Management Sys

tem is considered to be the reduction of absences

due to sickness and work-related illness (in terms

of severity and frequency), its functioning can be

evaluated and assessed in detail, by looking at the

constituent interacting processes.

Balanced Scorecards are a tool designed to fill

some of the gaps identified when traditional OHS

indicators are used. They bring together synthetic

indicators. This enables both the measurement

of the outcome of actions (lagging indicators), and also the correct functioning of internal sub-processes (leading indicators) (Figure 1). This article is in three parts. The first part addresses the issue of the traditional indicators identified in the literature. Once defined, their contribution and limitations are discussed. Next, Figure 1. Regulatory and risk activities integrated into an OHS management model. Figure 2. Regulatory compliance and risk control indicators.

the general concept of Balanced Scorecards is

described, along with a survey of the work that has

been carried out in the OHS domain. Finally, an

example from the aeronautic and aerospace indus
try is used to illustrate the prospective Balanced
Scorecards model. It integrates leading manage
ment indicators for two particularly interesting
sub-processes of a Management System; namely,
the supervision of regulatory compliance and risk

The impact of framework conditions on HSE in subcontracting/ outsourcing

K. Skarholt, U. Forseth, M. Hermundsgård & R. Rosness
SINTEF Technology and Society, Trondheim, Norway

ABSTRACT

The purpose of this paper is to investigate how
various framework conditions affect issues related
to Health Safety and Environment (HSE) in a
contractor hierarchy within the Norwegian petro
leum industry, both positively and negatively. By
framework conditions for HSE work, we refer
to conditions that influence the opportunities an
organisation, organisational unit, group or individ
ual has to ensure good HSE conditions (Rosness
et al., 2009, Rosness et al., 2010). The term thus
covers a broad range of conditions, such as mar
ket conditions (e.g., oil prices), terms of contract,
physical layout of installations, management style
and ideology.

In recent years it has become increasingly com
mon to outsource tasks which were previously seen
as core activities (Marchington et al., 2005). The
petroleum industry was one of the first industries
to make use of extensive outsourcing and is prob
ably among the most specialized industries in the
Norwegian economy. This sector is organised in
contractor hierarchies, where operators buy serv
ices from several contractors which in turn hire
subcontractors. In this setting, actors at one level
(e.g., operators) may have a strong impact on the
framework conditions facing other actors (e.g.
contractors).

In this paper we investigate how HSE is nego
tiated between different actors in a contractor
hierarchy. Using different power perspectives, we
analyze two stories/examples identifying strategies
and tactics employed by the actors involved in the
contractor hierarchy, and how collaborations and
networks are mobilized to improve HSE.

According to our interviewees, there has been
a positive development towards more integration
of personnel from contractors and subcontractors
offshore. Operators and subcontractors alike con
sider it a goal to promote collaboration and shared

The impact of human and organisational factors on risk perception

on Danish production platforms

H.B. Rasmussen

Centre of Maritime Health and Safety, University of Southern Denmark, Esbjerg, Denmark

ABSTRACT

The study explores the impact of human and organizational factors on subjective risk perception of personal injuries and process accidents on Danish production platforms. The present study applies models used in several studies conducted in the UK and Norwegian offshore industry (Fleming et al., 1998; Mearns et al., 2001; Rundmo, 1995; Rundmo, 1996). These studies have shown that organisational factors like priority of production versus safety and satisfaction with safety measures had an influence on risk perceptions among offshore employees in the UK and Norwegian sectors.

The definition of risk perception varies dependent on the research area and who is defining. There are two general ways of looking at risk perception: an objective and a subjective. The objective risk has been defined by experts as the probability of the unwanted dangerous event that can happen and its

consequences (Rundmo, 1996). The subjective risk perception is the way the individuals perceive risk and behave in response to it (Fleming et al., 1998). The subjective risk perception is socially con structed and depends on the social context (Bye & Lamvik, 2007).

Danish data were collected through a question naire survey sent to all productions platform in the Danish sector in 2010. Principal component analysis (with Varimax rotation) was used to iden tify underlying dimensions. All dimensions were tested in both SPSS and in the LISREL program. LISREL analysis of structural relationships by the method of maximum likelihood was used. Sta tistical significance of the goodness of fit of the model was tested with Root Mean Square Error of Approximation (RMSEA), Comparative Fit Index (CFI) Goodness of Fit Index (GFI). The reliability

A BBN risk model of maintenance work on major process equipment

on offshore petroleum installations

B.A. Gran, O.M. Nyheim & J. Seljelid

Safetec Nordic AS, Trondheim, Norway

J.E. Vinnem

University of Stavanger, Norway

ABSTRACT

Operational safety is receiving more and more attention in the Norwegian offshore industry. Almost 2/3 of all hydrocarbon leaks on offshore installations in the period 2001–2005 according to the Risk Level Project by Petroleum Safety Authority in Norway (Vinnem et al., 2006), resulted from manual operations and interventions, as well as shut-down and start-up, confirming what is considered common knowledge; that incidents and accidents often are caused by failure of opera tional barriers. Investigations of major accidents show that technical, human, operational, as well as organizational factors influence the leakages. In spite of these facts, quantitative risk analyses of offshore oil and gas production platforms have focused on technical safety systems.

The intention with the Risk OMT (Risk Modelling—Integration of Organisational, Human and Technical factors) program was to develop more representative models for calculation of leak frequencies as a function of the volume of manual operations and interventions. The Risk OMT program represents a further development of the work in the Barrier and Operational Risk Analysis

(BORA, Vinnem et al., 2003) and Operational Condition Safety (OTS, Sklet et al., 2010) projects. The basic approach is the same, but the emphasis is on a more comprehensive modeling of Risk Influencing Factors (RIFs) and how these affect the performance of operational barriers. In the Risk OMT project a generic risk model has been developed and is adapted to use for specific failure scenarios (Nyheim et al., 2010; Vinnem et al., 2010). The model considers the operational barriers in event trees and fault trees, as well as RIFs that determine the basic event probabilities in the fault trees. The generic risk model applies Bayesian Belief Networks (BBNs) in its modeling. The model has been evaluated through case studies and has been applied to evaluate the effect of different proposed strategies to reduce the leakage rates (Gran et al., 2011).

This paper presents the BBN model step by step

A methodology to quantitative ecological risk assessment for industrial accidents

O.H. Duarte & E.A. Droguett

Federal University of Pernambuco (UFPE), Recife, Pernambuco, Brazil

ABSTRACT

Recent industrial accidents such as toxic spills have caused catastrophic damage to the ecologi

cal environment and consequently great economic losses to the responsible company, as the British Petroleum painfully learned after the oil spill in the Gulf of Mexico, causing one of the most severe ecological disasters in history and a loss to the company estimated at U$37 billion to be spent with cleanup, fines, damages and repairs. However, this leak could have been avoided with the purchase of an equipment of U$500,000, able to seal the well in case of accident. The savings were there fore miscalculated under the risk-taking, which means that risk estimates were inaccurate. Such accidents as well as the high number of smaller accidents that happen every year has demanded an effective method to assess ecological risks. In fact, establishments with very hazardous installations or activities require quantitative values to the risks related to accidents with potential to cause human injury, ecological damage or economic loss, in order to objectively decide the necessary amount of resources to be invested in preventive measures, and this is the greatest contribution of Quantitative Risk Assessment (QRA). On the one hand, most studies in QRA for industrial accidents only consider risks to human health,

disregarding the quantification of ecological risks.

On the other hand, in the context of ecological

QRA (i.e., QERA), although some methodolo

gies have been able of quantifying ecological risks,

they focus on risks caused by almost surely events

(e.g., chronic pollution) of an industrial establish

ment, i.e., events that happen with probability one;

because they do not include the event frequency in

the composition of the risk, they are not capable

of contemplating accidents, i.e., (rare) events with

low probability of occurrence but that may cause

catastrophic damage. Therefore, this work aims

at proposing a methodology capable of quantify

A predicting method of system safety risk state transition time

based on Markov process

H.T. Li, X.M. Liu, J.L. Zhou & G. Jin

System Engineering Department, College of Information System and Management,

National University of Defense Technology, PR China

ABSTRACT

Safety risk which can be described by the

probability and severity level of consequence is an

important measure of system safety. Nowadays,

most of the classical methods used to evaluate the

safety risk are probability safety assessment meth

ods, which rely on the system safety model includ
ing event tree and fault tree to assess the probability
and severity level of various consequences based
on the analysis of the reliability of component.
Marseguerra gives a Monte Carlo approach to
PSA for dynamic process systems (Marseguerra,
M. et al., 1996). Aneziris presents a method for
evaluating the probability of catastrophic failures
in process systems (Aneziris, O.N. et al., 2004.) and
another for calculating the dynamic reliability of
safety systems and its application to a refrigerated
liquid cryogenic ammonia storage tank (Aneziris,
O.N. et al., 2000). Dynamic safety assessment:
Scenario identification via a probability clustering
approach is researched by Podofillini (Podofillini,
L. et al., 2010). Zhu gives a framework to integrate
software behavior into dynamic probabilistic risk
assessment (Zhu, D.F. et al., 2007). To ensure the
safety of a process system, Kalantarnia puts up
Dynamic risk assessment using failure assessment
and Bayesian theory (Kalantarnia, M. et al., 2009).
Probability risk assessment methods listed above are
only some typical examples, and the similar meth
ods are so many that we cannot enumerate all.
These methods are very effective for the safety

assessment of certain system and have solved a lot of safety assessment problems including static system and dynamic system. However, they also have some limitations. In these classical methods, the safety risk is only represented by probability and no system state evolving process of the safety is presented. So, it can't clearly describe the safety using the method of dynamic evolvement of the system state. Actually, most catastrophic accidents of complex system occur as a result of a series evolvement of system states over a time interval after the abnormal event has happened. Therefore, a problem that how do we model the evolving process of the accident through the system state evolvement

A research on simulation methods for system risk assessment

X.M. Liu, H.T. Li, J.L. Zhou & P.C. Luo

College of Information System and Management, National University of Defense Technology, Changsha, China

ABSTRACT

In the areas of system safety, it is difficult but important to perform safety risk assessment. The accurate assessment is significant to risk management and control. Many of researches have promoted the safety risk assessment. Nevertheless, few papers are devoted to simulation methods of

system risk assessment. The aim of this work is just to make researches on the simulation methods.

Safety risk is a characteristic for measuring safety level, which is the combination of the probability of occurrence of accident and the severity of that accident. Risk can be divided into low medium-high risk sets. Suppose that system state risk is the risk when the system in the state X(t), denotes R(X(t)). And we can partition the system state space into low risk state set E_{LR}, medium risk state set E_{MR} and high risk state set E_{HR}. It's known that the probability of system state X(t) at time t belonging to E_{LR}, E_{MR} and E_{HR} is $P_1(t)$, $P_2(t)$, $P_3(t)$ respectively.

The simulation methods for safety risk assessment based on system initial perfect state can be carried out as follows:

Step 1 Determine the time t for risk analysis;

Step 2 Calculate the probability of picking state from state sets for the component i at time t, and sample a state $x_i(t)$ randomly with the probability. Sequentially, the system state $X_1(t)$ can be obtained by sampling of all the components;

Step 3 Repeat step 2 by N times, and get N system states $X_1(t)$, $X_2(t)$, … , $X_N(t)$ at time t;

Step 4 Classify these N system states by risk as

E LR , E MR , E HR , then compute P 1 (t), P 2 (t), P 3 (t).

Let the time t increases gradually from zero, the

system safety risk in the future period beginning

from initial perfect state can be gained.

The simulation methods based on system cur

rent state are similar to above steps, but we must

get failure rate λ(t) firstly.

According to the proposed methods, the risk

change from system initial and current states

(including known runtime and unknown runtime)

Assessment of common cause failures and defensive measures

for the representation of I&C in probabilistic models

G. Deleuze, N. Thuy, R. Quatrain & F. Jouanet

EDF R&D, France

ABSTRACT

Digital equipment and systems have an important

role in the operation and control of Nuclear Power

Plants (NPP) and their main components. Dig

ital equipment and systems may have beneficial

effects, for example due to advanced capabilities

or improved hardware reliability. They may also

have detrimental effects. In particular, although

digital equipment is usually more reliable than

analog equipment it replaces, its use raises specific

technical and modeling issues, especially on digital Common Cause Failures (CCF) due to design or software faults.

As many products are available, and many architectures are possible for a given project, it is important for designers to be able to assess without excessive conservatism the impacts of the proposed solutions on plant safety, in new builds or through upgrades. Even if software related failures are systematic, it is important to note that many sys tematic failures are non-software related. A recent analysis (EPRI, 2008) has highlighted the domi nance of non-software failure mechanisms such as pre-accidental human factors. For example, human errors due to difficulty in the analysis of compli cated logic, whatever the I&C technology (relays, FPGA, microprocessor), may be significant.

This article presents an approach to improve the representation of digital I&C, while keep ing the models simple and usable in probabilistic models of an installation, the so called SPINOSA approach. It relies on the combined use of a partic ular representation of I&C effects, the “Compact Model”, and a sensitivity analysis based on “Beta Factors” representing potential dependencies due

to hardware, software, human actions or interac

tions. It considers random mechanisms and sys

tematic mechanisms, assessed by a combination

of probabilistic and deterministic approaches. The

framework used to assess the systematic failures

due to hardware, software and human actions is

partly presented here, i.e. the taxonomy of soft

ware related failure mechanisms and associated

defence measures necessary to assess associated

NUREG, 2009. NUREG/CR-7007 ORNL/TM-2009/

302, “Diversity Strategies for Nuclear Power Plants

and Instrumentation and Control Systems”.

Thuy, N. 2010. EPRI Report Estimating Failure Rates

in Highly Reliable Digital Systems, Draft November

2010.

Thuy, N. & Deleuze, G. 2009. A Mixed Approach to

Assess the Impact of I&C in PSA. Sixth American

Nuclear Society International Topical Meeting on

Nuclear Plant Instrumentation, Control, and Human

Machine Interface Technologies, NPIC &HMIT 2009,

Knoxville, Tennessee. Torok, R. & Thuy, N. 2010. EPRI Report 1019182 Protecting Against Digital Common-Cause Failure - Combining Defensive Measures and Diversity Attributes, December 2010.

R. Guillerm & H. Demmou

CNRS; LAAS—University of Toulouse, Toulouse, France

N. Sadou

SUPELEC / IETR, Cesson-Sevigne, France

ABSTRACT

Modern systems are increasingly complex. Indeed, they integrate more and more different technolo gies, offering more functions, but with a complex components in interaction. The process and the design methods must evolve to reflect this grow ing complexity. In particular, for our purposes, the dealing with properties such as security and reliability must evolve accordingly, to ensure and enable the necessary level of confidence. For an effective consideration of safety in the design process, it is necessary to consider safety in over all studies by the engineering system process. For this purpose it is necessary to define safety system (global) requirements and then to decline then into sub-systems requirements. Indeed, safety is defined as a non functional requirement and is related to emergent system properties. These non-functional properties cannot be attributed to single system components, they emerge as a result of integrating system components. So safety requirements must

be formulated in the large (system level) and then

declined in the small (sub-system level).

Avizienis, A., Laprie, J.-C., Randell, B. & Landwehr, C.

Basic Concepts and Taxonomy of Dependable and

Secure Computing. IEEE Transactions on Depend

able and Secure Computing, vol. 1, pp. 11–33, 2004.

Buzzatto, J.L. Failure mode, effects and criticality analysis

(FMECA) use in the Federal Aviation Administration

(FAA) reusable launch vehicle (RLV) licensing process.

Digital Avionics Systems Conference, 1999. Proceed

ings 18th. vol. 2 10/24-29/1999. Location: St Louis,

MO, USA.

CEI 60812: Techniques d’analyse de la fiabilité des sys

tèmes, 1995.

Chavalarias, D., Bourgine, P., Perrier, E., Amblard, F.,

Arlabosse, F., Auger, P., Baillon, J.-B., Barreteau, O.,

Baudot, P. & Bouchaud, E. et al, French Roadmap

for complex Systems 2008–2009, French National

Network for Complex Systems (RNSC), Paris Ile-de-France Complex Systems Institute (ISC-PIF) and IXXI, “Entretiens de Cargèse 2008”, 2008. ED-79/ARP 4754: Certification considerations for Highly-Integrated or Complex Aircrafts Systems, SAE 1996–11, 1996. EIA-632: Processes for engineering systems, Electronic Industries Alliance standard, January 7, 1999. Goguen, J. & Linde, C. Techniques for requirements elicitation. In 1st IEEE International Symposium on Requirements Engineering, pages 152–164, San Diego, 4–6th January 1993. Gotel. O.C.Z. & Finkelstein, C.W. “An analysis of the requirements traceability problem,” in International Conference on Requirements Engineering, 1994, pp. 94–101. Guillerm, R.,

Demmou, H. & Sadou, N. System engineering approach for safety management of complex systems. Proceedings of European Modeling and simulation (ESM'2009). October 26-28, 2009, Leicester, United Kingdom. Juristo, N., Moreno, A.M. & Silva, A. "Is the European Industry Moving Toward Solving Requirements Engineering Problems?" IEEE Software, vol. 19, no. 6, pp. 70-77, 2002. Komi-Sirvio, S. & Tihinen, M. "Great Challenges and Opportunities of Distributed Software Development - An Industrial Survey." in Proceedings of the Fifteenth International Conference on Software Engineering & Knowledge Engineering (SEKE'2003), 2003, pp. 489-496. Rasmussen, J. Risk Management in a Dynamic Society: A Modelling Problem. Safety Science, vol. 27, No. 2/3, Elsevier Science Ltd., 1997, pp. 183213. Sahraoui, A.-E.-K. "Requirements Traceability Issues: Generic Model, Methodology and Formal Basis." International Journal of Information Technology and Decision Making, vol. 4, no. 1, pp. 59-80, 2005. Sahraoui, A.-E.-K., Buede, D. & Sage, A. "issues in systems engineering research," INCOSE congress, Toulouse, 2004. Sommerville, I. Software Engineering: (Update) (8th Edition) (International Computer Science). Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 2006. Lee, W.S., Grosh, D.L., Tillman, F.A. & Lie, C.H. "Fault tree analysis, methods, and applications - A review", IEEE Transactions on Reliability, August 1, 1985; ISSN 0018-9529; r-34, page 194-203.

Discussion of a mathematical model to simulate a fire ball

from gaseous explosion (BLEVE)

A.N. Haddad

Universidade Federal do Rio de Janeiro, Rio de Janeiro, Brazil

E.B.F. Galante

Exército Brasileiro, Brazil

ABSTRACT

This work presents (mathematically) the phenome

non of explosion of a cylinder of LPG—Liquefied

Petroleum Gas, mixing with air and the subsequent

fireball.

Currently, the mathematical tools used to model this kind of events relies upon the equations of state. Furthermore, it relies upon the Navier Stokes equations to model the flow, the energy equation for the temperature. Usually this kind of models are calculated by the use of finite elements technique, having the continuity equation (density variation equal to zero) as convergence criteria. Using a computational platform some algo rithms can be implemented to calculate expected the effects a Bleve (having gas as fuel). These algo rithims used different hypothesis, wich allowed comparison. Among the hypothesis list, it ought to be enumerated:

- Absence of external influences on the flow (wind and topography)
- Linear correlation between enthalpy and specific heat source for the term of the energy equation
- Incompressible Fluid
- The cylinder of LPG will be reduced to a point

The importance of this work is justified by the need to quantify the risk of such event by the used of computational tools that can be simple, fast and accurate. These three qualities are a trade off. Increase one imposed a loss on another. Even

more, the tools a designer has to deal to chance

these qualities are the hypothesis used at imple

mentation stage, The same hypothesis discussed

Enabling quantitative risk assessment of the real world

transport system

M. Kowalski & J. Magott

Wrocław University of Technology, Wybrzeże Wyspiańskiego,
Wrocław, Poland

ABSTRACT

Fault Trees do not have great power of expressing

the real systems. Factors that increased applicability

of Fault Trees were the following papers: (Dugan

et al., 1992), where dynamic fault trees have been

introduced and (Bobbio & Codetta 2004), where

repair boxes have been defined. However, descrip

tive power of the above extensions when such time

dependencies like a sequence of time consuming

activities or time redundancy have to be expressed

is strictly limited.

These extensions failed when challenged with

timing dependencies of a tram-based public

transport system (Werbińska-Wojciechowska, S.

2008). In this system a failed tram is replaced in

some time by a spare one. When the failed tram is

repaired and delivered, it is put into action releas

ing the spare one. However, the failed tram has to be either replaced or delivered after repair within a time resource. If not, an undesirable event called hazard starts occurring.

Although we finally managed to express the tram system using a stochastic Petri net (Kowalski et al., 2011), the model was deemed obscure by domain experts. Hence, driven by the necessity to increase modeling power of fault trees and their applicability we blend them with Petri nets, thereby coming up with Fault Graphs with Time Depend encies (FGTDs) (Kowalski & Magott 2011), which are capable of expressing not only the system in question, but also a number of formerly devised fault tree extensions. In (Kowalski & Magott 2011), three repair policies applied to computer system failure/repair process have been analyzed. FGTDs contain probabilistic fault tree with time dependencies (Babczyński et al., 2010) based ele ments and Petri net based elements. In the research we strive to retain the genuine intuitiveness of fault trees, which is the main reason for their popularity and acceptance among safety engineers.

The hazard probability of the tram system and simulation time metrics are examined using a dedi

cated simulator. The values are computed depending on a number of redundant trams. Additionally, analytical estimations of these values are found

Fault tree analysis of substations

M. Čepin

Faculty of Electrical Engineering, Ljubljana, Slovenia

ABSTRACT

Substation reliability is defined as the inability of the substation to support the delivery of electrical power supply to any of its related loads.

The objective of this paper is to investigate the ways how to assess reliability of substations in order to avoid complex dynamic methods and at the same time include in the analysis the features of different system configurations and conditions.

The goal is to develop a method, which would enable preparation of substation models, which are useful for their integration into the models of power system reliability. The integration of substation models and model of the power sys tem is important for realistic assessment of power systems.

The method consists of the following steps:

- definition of the conditions of the systems under investigation,

- the model of the substation structure,

- transformation of the model of substation structure into the model, which is suitable for the fault tree analysis,

- the fault tree analysis,

- the interpretation of the results and direction of possible improvements.

Different conditions can represent the system in a different configuration or in different operating conditions. Each set of conditions related to spe cific configuration or operating conditions can in theory require changed models in the other steps of the method. The model of substation structure is defined with the help of the matrix of connec tions. Substation structure is transformed into the model, which is suitable for the fault tree analysis. The results of the fault tree analysis give system reliability. Several fault trees are developed for one system.

The method upgrades the static reliability calculation of the systems by introduction of several configurations and conditions of the sys tem, which are evaluated separately under different

Formalization of a quantitative risk analysis methodology for static explosive events

R.G. Salhab, I. Häring & F.K.F. Radtke

Fraunhofer Ernst-Mach-Institute (EMI), Efringen-Kirchen, Germany

ABSTRACT

The paper presents the methodology of a quanti

tative risk analysis implemented in an interactive

3D expert software-tool for high explosive events

of static sources, e.g. terrorist bombing threats

in urban environments, which is being developed

since more than 10 years (Dörr & Gürke 2006).

The methodology is described in a formal way cov

ering the following steps: analysis of scenario, haz

ard, damage, event frequency, exposure and finally

risk assessment.

For each step we give the input and output,

the engineering and physical models as well as

the algorithms. The effects of fragment and blast

are considered. We show that the formalization

describes the methodology in a short and concise

way and discuss possible generalizations and fur

ther improvements of the methodology and the

formalization.

Risk assessment tools have been developed,

amongst others, in the US (SAFER (Tatom 2008))

or the Netherlands (Dongen 2000). A formaliza

tion of a quantitative risk analysis for fragments

of high-explosive shells in air has been presented in (Häring & Schönherr 2009).

The presented risk analysis follows the scheme illustrated in Figure 1. In the scenario analysis step the geographical conditions, properties of hazard sources, exposed sites and counter meas ures are defined by the user. Implicitly standard conditions for the atmospheric conditions are assumed. Physical consequences of the detona tion are computed in the hazard analysis step, like specific impulse and peak overpressure of the blast and fragment densities on the ground. The expo sure of the personnel is defined by the user. The event frequency is predefined in a probability of event table that has been adapted to German con ditions. In the damage analysis step the damage due to fragments, blast and a combination of both are calculated using probit distributions and prob abilistic considerations. In the final risk analysis

High-pressure pipeline break risk assessment

T. Saska, J. Novak & F. Kratochvil
Technical University of Liberec, Liberec, Czech Republic
R. Sousek
University of Pardubice, Pardubice, Czech Republic

ABSTRACT

The risk quantification represents complex multidisciplinary problem, requiring pipeline disturbance probability evaluation, escaping gas quantity assessment, physical effects of caused fire or explosion under different technical and meteorological conditions, individual risk evaluation and vulnerability assessment of exposed people or objects.

This work represents trying to criteria formulation for development licence with the usage of individual and social risk assessment. It is affected by estimation uncertainty of probability of major pipeline break. In the worldwide scale it is concerned about unique cases, so it is not possible to consider available statistic data as adequately reliable for accident frequency determination.

The physical effect calculations are more accurate. Here the uncertainties arise from large number of available conditions, from which it is possible to take into account only limited number. It is necessary to notify, that the reach of negative effects (in case of major accident, such as e.g. pipeline total rupture) may affect to the distance which several fold exceeds the bandwidth.

Vulnerability assessment of objects and people

results both from methodics recommended by

Ministry of the Environment of the Czech Republic

and from recherche to principles of landscape

planning and to risk acceptability in foreign coun

tries. The social risk calculation is not aimed at

concrete existing objects, but at typical objects cat

egory, which are under consideration in the term

of acceptability assessment of their localization

inside safety zone.

Risk is defined as a product of unwanted event

rise probability and its consequences. The event

probability is contingent both on equipment tech

nical parameters (gas pressure, pipeline diameter,

material, number of components), their reliability

and random outside effects resistance. The con

sequences may be related to detriment of people

health and lives, also economic losses and environ

mental damages. We know two different risk types: – individual, – social. Individual risk represents probability of specific quantified consequence for person or object which inheres in given location against potential risk source (eventually more risk sources). Individual risk for one person in specific place near the accident source (e.g. individual fatality, individual risk of injury) depends not on population density round about the source, generally not even on the fact, whether in the area some people are. Similarly the individual risk for object is possible to determine no matter if some object is situated in the given point. Individual risk value sinks with the distance from the accident source. According to its area distribution it is possible to specify areas of enhanced risk. Social risk is relevant to

the number of threatened people, to the number, value and significance of objects, eventually also to the quality of threatened environment. So, it depends on population density (also on its distribution in area and time) and on concrete objects existence in threatened area. Social risk is defined as a product of number of threatened people or value of affected resources and relevant individual risk. That is why the social risk value may be (and often is) higher in farther points from the accident source, than in near points. According its level the risk acceptability for industry objects is evaluated. The continuous economic growth, country industrialization and the development area expanding is connected with finding an acceptable balance between risk from energetic infrastructure and its need for every people because of power supply. In our case we will concern with VTL pipelines. Present legislature in the Czech Republic and the technical regulations and rules solve these problems. We have to claim, that the concrete conditions specification is different in most of European countries. We could say that it is less strict and simpler than in the Czech Republic. For finding acceptable level for above mentioned balance we can successfully use risk assessment methods.

Integrated risk assessment for LNG terminals

O.N. Aneziris, I.A. Papazoglou & Myrto Konstantinidou

National Centre for Scientific Research “DEMOKRITOS”, Terma Patriarchou Grigoriou,

Aghia Paraskevi, Greece

ABSTRACT

This paper presents the methodological and

procedural steps for quantified risk assessment of

LNG and its application to two LNG terminals an

onshore and an offshore. The onshore consists of

two storage tanks with total capacity 100000 m 3

and the offshore of four double containment

spherical tanks, each with capacity 34672 m 3 . This

analysis was performed in the framework of the

iNTeg-RISK project, coordinated by Jovanovic (2010).

Over the last years risk assessment methodology has been widely used for estimating risk of chemical plants storing flammable and toxic substances, such as ammonia, LPG and fuels, by Papazoglou et al. (1992) and Taveau (2010). Nevertheless quantified risk assessment of LNG installations appears in few cases in the literature.

Extensive research has been performed in the area of consequence analysis. The behaviour of LNG has been extensively studied if released in the atmosphere, on ground or on water. Results of experiments and modelling concerning LNG outflow, dispersion, pool fires and vapour explosions have been presented by Cleaver et al. (2007), Hanlin (2006) and the Sandia report (2004) presents methods of LNG spills on water.

The basic steps for risk assessment followed in both cases are the following: a) Hazard Identification, where the main sources of LNG release are identified and the initiating events that can cause accidents are determined b) Accident Sequence Modeling, where logic models for the installations are developed. c) Data Acquisition

and Parameter Estimation; parameters which were estimated with generic values include the frequencies of the initiating events, component unavailability and probabilities of human actions. d) Accident Sequence Quantification; the frequency of occurrence of all accident sequences identified in the second step is assessed by using the laws of Boolean algebra and required data e) Consequence Assessment; calculation of release and evapora tion rate, radiation levels and overpressure owing to immediate or delayed ignition of LNG is per

ITRA: GUST—The Guttman scaling tool for supporting IT risk assessment audits

R. Mock & Ph. Aeschlimann
University of Technology Zurich, Zurich, Switzerland

ABSTRACT

There is not a chance for something like Fault Tree Analyses of IT at Small and Medium Enterprises (SME): At any rate, practitioners regard a check list approach as a resource-conserving method of choice. However, the seemingly simplicity of check list compilation and application often leave aside its heuristic procedures and biased results. Optimising the way of questioning in check lists offers great potential to improve the quality

of risk assessment surveys of IT infrastructures at enterprises. For this, staggered lists of IT security measurements are constructed (Guttman scales) whereas the Code of Practice ISO/IEC 27002 [1] provides the objectives and recommendations relating to information security management in this regard. The FMEA approach finally structures the overall risk analysis process. A questionnaire/ survey design using this “Best Practice FMEA” enables the analyst to represent the results in the form of matrices of measurements with regard to the Code’s Objectives improving statistical analy sis and validity. The respondents’ answers are dis played as rectangular array X of j; j = 1, 2, …, n rows and k = 1, 2, …, 5 columns. The statistical evaluation of X mainly sorts Objectives, e.g. in ascending order from total non-implementation O j;non = {0 0 0 0 0} to full implementation of meas urements O j;full = {1 1 1 1 1}.

Three types of scales are developed: Pure and near Guttman scaling as well as an FMEA scaling of frequencies of expected interferences or failures. However, the drift from pure Guttman to other scales requires sophisticated statistics to group the Objectives.

The statistical evaluation process uses k-means

which is a nonhierachical clustering method.

Hierarchical clustering methods are only outlined

as already presented at the previous ESREL con

ference. Both clustering methods are equivalent as

they group the Objectives in the same way. With

regard to applicability, the k-means approach is

found easier to implement at (small and medium

sized) enterprises. The interpretation of k-means

results is eased by the usage of shilhouette plots. The results of a literature research show the placement of Best Practice FMEA among other IT risk assessment approaches, e.g. CRAMM and OCTAVES. It becomes apparent that Best Practice FMEA is most applicable at small-scale enterprises which are not fully covered by the other approaches. The paper also shows the transfer of the previous paper-based approach into the web based tool ITRA: GUST. The concepts of tool design and software architecture are presented. The closing remarks summarise and reason the method development of Best Practice FMEA and ITRA: GUST. REFERENCE [1] ISO/IEC, 2005. Information Technology – Security Techniques – Code of Practice for Information Security Management (ISO/IEC 27002:2005). 0 0.2 0.4 0.6 0.8 1 1 2 3 4 5 6 7 8 Silhouette Value C l u s t e r Figure 1. Silhouette plot of clusters according to case study data (Value ≥ 0.6: Objective is well located in its cluster).

Literate PSA modeling for a modular PSA

M. Hibti

Departement Management des Risques industriels, EDF R&D
Clamart, France

The very act of communicating one’s work clearly to

other people will improve the work itself. D.E. Knuth

ABSTRACT

Now that PSAs are widely used to check and improve the design of many complex industrial systems, and as a key tool for maintenance planning and many Risk Informed Decision processes, it is time to take a look at the complexity of the tool and have a discussion on the way models are built and documented.

For Nuclear Power Plants, for example, many PSA models were developed and are used for maintenance and operational tasks. These models have been extended in many directions to meet licensees needs and safety authority requirements. The models nowadays deal not only with internal events, for shut-down and power states, but also with fire, flooding, and all external events in addition to other considerations with respect to different PSA applications.

These developments depend on the softwares that are used to develop the models. Moreover, the modeling was mostly performed regarding a set of needs, requirements, extensions that may not have necessarily been planned initially. This generally leads to huge models with the following characteristics:

- The models are developed by many PSA devel

opers, with different methodologies, and with different objectives (e.g. a model for internal events is not developed in the same way as one dedicated to technical specifications needs),

• Different tricky modeling (due the lack of expressiveness of the Boolean Algebra) may be used without necessarily being documented since it seems “at least for the moment” obvious

Managing the risks to personnel within occupied buildings

N.J. Cavanagh

DNV, London, UK

ABSTRACT

Accidents like Buncefield and Texas City have put the risk to people in occupied buildings high on the agenda of both regulators and operators. Regula tory regimes for assessing the safety of those in occupied buildings are becoming more demand ing and the need for accuracy and transparency has increased. For example, regulatory guidelines like API RP752 and RP 753 provide guidance on the design and location of permanent and port able buildings to minimise risks to occupants. This paper focuses on advances in software models for assessing risks to people in buildings from releases of flammable materials.

When deciding on the location and construction of occupied buildings in the vicinity of hazardous installations, a number of factors must be considered during the design and operational phases. Key to the process of deciding where to locate buildings and what level of protection they should offer their occupants are the level of risk to which it is acceptable to expose those occupants. Traditional QRA tends to use “generic” vulnerability for people indoors where their probability of death when particular levels of different types of hazardous effects are exceeded, such as explosion overpressure, radiation from fires, flame impingement or toxicity, is treated as being independent of the type of building within which they reside, This is obviously a significant limitation to using the results of traditional QRA in selecting appropriate building types in different situations or to locate buildings in the safest place from the standpoint of risk to occupants.

Risk to building occupants is a function of both building location and construction. In order

UMR STMR—CNRS, Institut Charles Delaunay, Université de Technologie de Troyes, Troyes, France

ABSTRACT

In the field of risks analysis, the domino effect or chain of accidents has been documented in technical literature since 1947. The accidents caused by the domino effect are those that cause the most catastrophic damage. The consequences of the damage caused are at various levels and may not only affect the industrial sites (activities, importance …), but also people, environment and economy. The probability of the domino effect is increasingly high due to the development in indus trial plants, their proximity to such establishments, and their inventory of dangerous substances, the transportation networks and the population growth.

The potential risk of the domino effect is widely recognized in legislation since the first “Seveso-I” Directive (82/501/EEC), which required the assess ment of domino effects in the safety analysis of industrial sites whose activities are subject to this directive. Furthermore, the “Seveso-II” (Directive 96/82/EC 1997) extended these requirements to the assessment of domino effects not only within

the site under consideration, but also to nearby plants.

Recently, in an inventory of the past domino accidents (Abdolhamidzadeh, Abbasi, Rashtchian & Abbasi 2010), authors have recorded 224 domino accidents occurred over the period 1917 to 2009 with 30% of these domino accidents recorded between (2000 to 2009). This study reveals that explosion are the most frequent cause of domino effect (57%), followed by fires (43%).

An industrial site and/or storage areas contains many storage equipments that may be subjected to an external and/or internal incident like over pressure. The escalation vectors or physical affects (overpressure, heat radiation, and toxic release) generated after a vessel rupture (explosion), may affect the surrounding equipment / facilities. If the affected targets are damaged, these latter, may

Organizational interface failures: A historical perspective and risk analysis framework

T.T. Pires & A. Mosleh

University of Maryland at College Park, MD, US

ABSTRACT

This article argues that it is crucial to extend our understanding on how weaknesses in Organiza

tional Interfaces (OI) can contribute to significant losses. The bases of the argument are detailed analysis of various accidents and incidents that have occurred in the past, with an emphasis on identifying evidence that organization interface flaws played important role in such accidents and incidents. The analysis presents accidents and incidents in assorted fields including commercial nuclear power generation, air and rail transporta tion, health care, defense, space exploration, and the entertainment industry. The objective of the analysis is to provide building blocks for a generic OI failure classification scheme and an approach to quantify OI failure probability based on a model of organizational interface. The accidents and incidents analysis has revealed that poor com munication channels, lack or weak collaboration mechanisms and poor coordination were impor tant factors in the initiation, development, and/ or mitigation/prevention of the accidents and inci dents analyzed. Therefore, communication, coor dination and collaboration interface failure are defined as top level OI failure categories. Communication Interfaces (CmI) are impor tant because it is through them that information is

exchanged between the elements at the ends of the

interface. Some CmI failures identified in the acci

dent/incident analysis include wrong information content being transmitted, information transmitted or received at the wrong time or location, etc. Coordination Interfaces (CrI) are important because it is though them that the information that is communicated is used for a purpose. Some CrI failures identified include poor organizational rules and common grounding, causing the inability to identify one's intent, comprehension of the situation, and poor feedback. Collaboration Interfaces (CoI) are important because it applies to the interactions among the elements at the interfaces, which must have trust, has to be beneficial, and lead to joint value creation. Some CrI failures identified include lack of confidence or predictability in one's expectation and lack of confidence in the other's goodwill. The paper will summarize these insights and provide the evidence gathered to support the classicization of interface failures. Having identified these three OI failure categories, the paper outlines an approach to incorporate OI failures in risk models of complex socio-technical systems. The risk model can then be used in aiding organizations identifying and eliminating interface weaknesses, and comparing different interface design alternatives. The quantification approach proposed is a Bayesian belief network model that accounts for a set of factors assumed to influence communication, coordination and collaboration interfaces failure probability. An illustrative example is presented, using one of the accidents analyzed as subject.

Probabilistic risk analysis procedure for aircraft overruns

M.G. Gratton, M. De Ambroggi & P. Trucco

Department of Management, Economics and Industrial Engineering, Politecnico di Milano—Milan, Italy

ABSTRACT

According to the World Aircraft Accident Sum

mary, during the 14-year period from 1995 through

2008, commercial transport aircrafts were involved

in a total of 1,429 accidents resulting in major or

substantial damage. Considering the 431 runway related accidents (30% of the total), the 97% (or 417 accidents) were runway excursions (FSF, 2009). Mitigations approaches for these kinds of accident mainly consist in the enlargement of the runway safety area up to standards set by inter national or national agencies. This procedure is however very expensive and in many cases of no easy accomplishment. There is therefore the need for a probabilistic risk-based approach to analyze the portion of space lying beyond the runway end to understand if case-specific solutions, alternative to standard requirements, are available.

Based on a literature review of available models, we assumed the ACRP hazard probability model (Hall et al., 2008) as a basis for the development of a Probabilistic Risk Analysis procedure specific for aircraft overruns. Input variables (e.g. aircraft characteristics, runway characteristics, weather conditions) were described by way of statistical distributions derived from historical data of the airport under analysis. The resulting probability distribution of accident probability was then cal culated by means of Monte Carlo simulation and used, along with longitudinal and lateral location

models, to generate a two-dimensional grid report

ing the probability of each area to be the end

location of an overrun accident. This result is par

ticularly original and useful as it can be reported

superimposed to an airport map to provide imme

diate visual information on the probability of

interactions between overrunning aircrafts and

infrastructures beyond the runway end.

Further a stocastic indication of the kinetic

energy was also introduced on the location models,

Probabilistic Safety Assessment of a UF 6 production process

Behrooz Ebrahimi

Department of Energy Engineering of Sharif University of Technology, Tehran, Iran

ABSTRACT

Application of Probabilistic Safety Assessment

(PSA) to a Uranium Hexafluoride (UF 6) produc

tion process in this paper is presented. The process

is constituted from three main units, UF 4 conver

sion to UF 6 , condensation of produced UF 6 gas

and tail gas treatment. UF 4 powder reacts with F 2

and N 2 gas mixture in a vertical fluorination reac

tor. Produced gas goes to condensation unit and is

condensed in two stages. Gaseous waste from con

densation process goes to tail gas treatment unit

for F 2 and HF removal. Radioactive gas is present in all parts of the process and occurrence of high pressure or temperature in process equipments may lead to radioactive release to workplace and envi ronment. The work is mainly based on PSA experi ence in nuclear power plants. Accordingly for the process, major Initiating Events (IE) leading to UF 6 gas release have been identified using HAZOP study. Eight different groups of IEs after HAZOP study have been identified. These IEs are events leading to high pressure or temperature in Fluori nation Furnace or two condensers, which eventu ally will lead to UF 6 gas release. For each IE, based on related safety systems and functions, accident sequence analysis is performed with Event Tree Analysis (ETA). First step in ETA is identification of safety systems and functions which act against IEs. After identification of safety systems, they are entered as top events of event trees and based on engineering judgments final states of different accident sequences in ETA has been defined.
For frequency estimation of IEs which require failure of more than one component to occur FTA is used, for other IEs since data from simi lar plants are unavailable simply expert judg

ment has been applied. Due to greater reliance placed on operator in nuclear fuel cycle facilities compared to NPPs, special consideration is taken into account for Human Reliability Analysis (HRA). HRA is performed according to Swain and Guttman method (THERP) described in

Safety factors in fire safety engineering

H. Bjelland & O. Njå
University of Stavanger, Stavanger, Norway

ABSTRACT

During the 1980s and 1990s there was a major regulation regime shift in many countries, going from a regulation based on prescriptive solutions to performance-based design. Many authors were involved in the process of developing appropri ate performance goals and engineering tools (Hadjisophocleous, Benichou et al., 1998).

In this paper we discuss the current practice of fire safety design, i.e. a prescriptive approach with deviations and a deterministic approach. We also take a look at the probabilistic approach. Based on our experience with the fire safety engineering industry we claim that a probabilistic approach introduces serious fundamental challenges. These challenges are related to a) a lack of holistic

understanding of the sociotechnical relationships between buildings, fires and occupants and b) the lack of relevant probabilistic data.

Consequently, we argue that a development of the current practice based on determinis tic approaches and the use of safety factors is more promising. Our perspective is the abilities of buildings to provide life safety for occupants during a fire. This leads to a discussion of safety factors related to Required Safe Egress Time (RSET) versus Available Safe Egress Time (ASET) (Babrauskas, Fleming et al., 2010).

The concept of safety margin between load and capacity is challenging in engineering of occupant fire safety. If the safety margin is related to an extreme event, an even more extreme event could always be specified. The concept of safety margin appears to be important to regulators; hence there is a need to address its contents. In structural engi neering the safety margin reflects variability with respect to loads deviating from “normal condi tions” and variability in material characteristics

Setting rational safety goals for human spaceflight

Joseph R. Fragola

Vice President M&S / Risk Analysis at Valador, Inc.,

Rockville Center, US

Elisabeth L. Morse

Systems Engineer at Valador, Inc., Broadlands, US

ABSTRACT

NASA is embarking on a new era of human spaceflight, one in which commercial service providers will sell astronaut transportation services to NASA. Thus NASA will have limited insight into the design and manufacturing processes of space transportation vehicles. In this new paradigm, setting appropriate safety requirements and goals, for the service providers to meet, and a standard process for evaluating the safety of commercial rides, will be of paramount importance to ensuring the safety of the astronauts.

Good systems engineering practice emphasizes the importance of having valid and verifiable requirements (NASA 2007). While challenging requirements can serve as incentive for the industry to innovate, requirements that are too high could be ignored altogether. In the case of safety, carrying an unrealistically high, and thus unverifiable requirement can actually reduce the safety of vehicles under development because it can lead to focus on quantification of known failure modes

rather than on a search for the unknowns, focus on process rather than experience, false sense of security, and tendency to game the analysis to meet the requirement (Gleick 1993, Jenkins 1992).

A probability of Loss Of Crew (LOC) requirement cannot be strictly verified, as there will be too few flights for statistics and probability forecasts are only “opinions” of the forecaster. But the reliability and safety that were actually achieved by previous vehicles, with reasonable expectations of growth, inform the range of LOC probabilities that can be credibly achieved by new systems. This paper shows how this process can inform the development of rational requirements with the example of launch vehicle safety.

Flight history shows that launch risk has been driven by the unknowns and the under-estimated, meaning that the actual safety risk faced by astro

A discussion on expert judgments in national risk analyses

K. Russell Vastveit & O. Njå

University of Stavanger, Norway

G.S. Braut

Stord/Haugesund University College, Norway

M. Ruge Holte

Directorate for Civil Protection and Emergency Planning, Norway

ABSTRACT

Risk and vulnerability analyses are widely used by national, regional and municipal authorities as well as many business sectors in Norway. In 2009 the Ministry of Justice and the Police asked the Directorate for Civil Protection and Emergency Planning (DSB) to develop a National Risk Picture (NRP) by conducting a National Risk Assessment. The end goal of the NRP was support of policy making. The project was conducted in three phases; methodology development; hazard iden tification; and scenario development and analysis. The analysis of ten scenarios was completed by the end of 2010 and the first National Risk Picture report was published in March 2011.The aim of the directorate is to continue the project by adding new scenarios to the National Risk Picture every year.

The work described in this paper deals with the core of risk analysis—the interpretation and understanding of risk, uncertainties and perform ance. It examines the use of experts in the context of the scenario development and analysis phase of the National Risk Assessment. It discusses the structure of expert judgment with regard to knowl

edge contributions to the analysis, the elicitation techniques that were used and associations with different types of judgment biases. Experts took part in the process by developing scenarios, pro viding consequence judgments and assigning prob abilities to events described in the scenarios. They represented core organizations with responsibilities related to the specific scenarios. In addition they also held expert knowledge related to risk areas and the expected outcomes of events. We found that there were several challenges associated with the expert opinion elicitation process during the scenario meetings. Among there were a lack of scientific and professional knowledge; lack of and variation (local, regional, national or international) in personal experience; personal agendas (politics) and variation in preparations for the meetings. We observed the use of several heuristics, such as availability, anchoring and representativeness during the expert scenario analysis. We conclude that the risk analysis process provided spin-off effects beyond policy making support, such as multidisciplinary learning and collabo ration across institutional borders. The national risk analysis processes can therefore become the starting point for a significant shift in the national major hazard and accident prevention and emergency management concept. It is clear that experts are important participants when discussing consequences and uncertainties related to major disasters and incidents with serious impacts on society. We did however find that the scenario analysis meetings showed substantial weaknesses in the methodology used for expert judgment in National Risk Assessments. There is a lack of standardized and evaluated methods for expert participation in complex risk analyses at the societal level. Such methods would ensure that inputs from expert participation were made explicit and thereby open to criticism.

A simple polynomial regression to estimate the parameters of the Weibull distribution with $\gamma > 0$

I.B. Sidibé

Université Paul Verlaine, Laboratoire de génie industriel et de production de Metz, Metz, France

K.H. Adjallah

Ecole nationale d'ingénieur de Metz, Laboratoire de génie industriel et de production de Metz, Metz, France

ABSTRACT

The life of industrial mechanical equipment is in general a continuous random variable, difficult to be accurately predicted, in spite of progresses in reliability engineering. These random variables have statistical distributions that can be modelled using probabilistic distribution function such as exponential, gamma, Weibull, lognormal, etc. These laws must accurately describe the equipment degradation behaviour in operation.

The Weibull model is an important distribution widely used in mechanical reliability under those properties to describe the equipment behaviour (degradation process) throughout their lifespan (youth, maturity, old age). This distribution is defined by three positive parameters characteriz ing explicitly the model: β models the shape of the distribution, η models the scale and γ models the time origin of the failure events.

Field experience data should allow estimating

these parameters but in practice this is difficult due to the complexity of the calculations requirements.

There are three approaches for the parameters estimation: 1) the Allen Plait technique based on functional paper graphic; 2) analytical identification based on statistical inferences; 3) combines the two above techniques to estimating the coefficients of a regression line by the least square method.

In this paper, without any hypothesis, we introduce an approach for identifying the 3-parameters based Weibull distribution function, conversely to the practice. We propose to implement a simpler, practical, robust and effective approach for estimating the Weibull 3-parameters distributions.

Our method is based on polynomial regression whose purpose is to build an explicit expression of the parameters without recurrent use of optimization tools.

The approach uses analytical and graphical methods for estimating the parameters of

Accelerated test model in fatigue life reliability evaluation of stub axle

E.A. Azrulhisham

Malaysia France Institute, Universiti Kuala Lumpur, Malaysia

Y.M. Asri

Universiti Teknikal Malaysia Melaka, Malaysia

A.W. Dzuraidah

Universiti Kebangsaan Malaysia, Malaysia

A.H. Hairul Fahmi

Engineering Division, Perusahaan Otomobil Nasional (PROTON), Malaysia

ABSTRACT

In view of increasing pressures of shortened development cycles and desire to save costs, accel erated life testing method has been devised to force products to fail quickly. In case where the scatter in fatigue life was neglected it is sufficient to know the relationship between load and the acceler ated life using typical stress-life (SN) relationship. However, in terms of mass production, fatigue properties of material used in the fabrication of components cannot be exactly consistent in qual ity due to uncertainties associated with the size effect, machining and manufacturing conditions (Schijve 2005). These uncertainties factors should be considered as random variables that results in variation of the fatigue life curves (Azrulhisham et al., 2010).

In this study, fatigue life of an automotive stub axle was calculated by the linear damage

rule stress-life method using stress range inter

cept and slope of a Probabilistic SN (PSN)

curve along with Belgian pave load patterns. In

this approach, the PSN curve was illustrated

by the reliability function of Inverse Power

Law-lognormal (IPL-lognormal) parametric

model of accelerated cyclic load test. The IPL

lognormal parametric model was derived from

incorporation of IPL stress-life model with log

normal life distribution. The parameters of the

model were then estimated using Maximum Like

lihood Estimation (MLE).

In view of the fact that that the material property

represented by the PSN plot has been obtained by

a set of accelerated cyclic tension test, the experi

mental data have the standard deviation and it is

difficult to ensure that the actual material used in

the fabrication is closely matched to the known mean value. In this study, the degree of reliability of the estimated fatigue life of the component was evaluated by developing a Pearson statistical model considering stress range intercept and slope of the PSN curve as random variables. Based on the first through fourth statistical moments, the type of the Pearson system was determined as Type I. Probability Density Function (PDF) of the fatigue life estimates shown in Figure 1 was obtained using Pearson curve of Type I relationship and the fatigue life reliability is then evaluated from the PDF. Considering normal distribution of fatigue strength, it is found that the fatigue life of the stub axle to have the highest reliability between 4000- 5000 cycles. Taking into account the variation of material properties associated with the size effect, machining and manufacturing conditions, the

method described in this study can be effectively 1000 2000 3000 4000 5000 6000 7000 8000 0 1 2 3 4 5 6 Fatigue Life (cycle-to-failure), N f (N) Figure 1. PDF of the fatigue life estimates.

applied in determination of probability of failure

of mass-produced parts.

Azrulhisham, E.A., Asri, Y.M., Dzuraidah, A.W.,

Nik Abdullah, N.M., Shahrum, A. & Che

Hassan, C.H. 2010. Evaluation of Fatigue Life Reli

ability of Steering Knuckle Using Pearson Parametric

Distribution Model. International Journal of Quality,

Statistics and Reliability. vol. 2010, Article ID 816407,

doi:10.1155/2010/816407. Schijve, J. 2005. Statistical distribution functions and fatigue of structures. International Journal of Fatigue 9(7): 1031–1039.

Analysis of wave energy parameters based on copula functions

C. Ejoh & S. Sriramula

School of Engineering, University of Aberdeen, Aberdeen, UK

ABSTRACT

The amount of available wave energy at a particular

location is one of the most significant variables

influencing the installation choice of these turbine

facilities. It is widely accepted that the available

wave energy is highly uncertain and depends on

the significant wave height and the zero-crossing

period variations, which in turn are randomly

varying. Probabilistic methods provide a rational

framework to represent the randomness in reliable

system performance. By simulating the variations in significant wave height and the zero-crossing period in terms of appropriate probability distribution models with accurate dependency considerations, it is possible to study the randomness in the corresponding wave energy output. This requires the formulation of the corresponding multivariate distribution model. Conventional approaches of simulation with multivariate probability distribution models require the univariate marginals to be from the same class or impose a restriction on the statistical dependence by the distribution parameters. The widely used Pearson's correlation coefficient for dependence modelling cannot capture the dependence structure accurately and may be misleading in case of non-elliptical distributions and is sensitive to outliers.

The desire to get the best and most reliable method for modelling data led to the research on copula functions. Although rather new to the engineering world, copula functions have been widely used in the financial and actuarial risk management strategies. These functions work by separating the dependence structure of the marginal distributions from the multivariate model. One very important fact about copula functions is that the marginal distributions can be chosen arbitrarily. This paper will show why copula based simulation is a better alternative than the traditional linear correlation based simulation by analysing wave

energy parameters. Environmental field data on the significant wave height and the zero-crossing period is obtained from a potential turbine location and the dependency of these data is being utilised. Copula functions are then used to simulate the parameters and the dependence structure of the simulated data is compared to that of the actual data. The scatter plots for the elliptical copulas and for the traditional linear correlation method are shown in Figure 1. It can be seen that there exists a tail dependency in the observed data; both the Gaussian and the t-student copula simulate this tail dependency well but this is not the case for the traditional linear correlation method of simulation. All three Archimedean copulas are also found to be better representations of the observed data. By doing this, it is seen that the copula based simulation provides a better model than the traditional linear correlation method which is generally an acceptable engineering method. Its unique advantages and the flexibility could make it a preferred simulation option than the traditional linear correlation method.

Figure 1. Scatter plots for the elliptical copulas and for the traditional linear correlation method.

Database concept in early stage of operation

I. Dziaduch & M. Mlynczak

Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Evaluation and management of new established

systems is difficult and loaded with uncertainty

because of lack of information concerning its

behavior and possible disturbances. If common

operation process is properly designed due to

usage and maintenance, then expected effect and

profit should be achieved. But usually random dis

turbances influence negatively process efficiency

(human error, failures, environmental hazards).

The role of operator and staff responsible for the operation process is carrying on the process and meets the threat preferably with sufficient advance. Operating manager usually expects positive feed back from the operation system to be informed how efficiency indexes vary due to undertaken actions.

It is described in the paper assumptions and for mal model of database supporting the regional rail transportation system operating new rail-buses. The operational system is at present in build-up phase i.e., new rail vehicles are to be bought, new railway connections are opened and operat ing staff is growing. New elements of the system and expanding offer of services introduce much information and unexpected events. It is almost obvious that informative database and operation aid system have to be designed and introduced to real system. The computer aided system is directed on managing current operation and maintenance, especially preventive maintenance and scheduled preventive maintenance of single object in the group of objects. Proposed database, based on similar idea shown in Computerized Maintenance Management System (CMMS) has been improved

by segment of cost analysis helpful in LCC

methodology especially important for the owner

of regional transportation system.

The crucial point underlies in selecting, collect

ing and processing operating data. Data acquisi

tion is a spread computerized and based on formal

written forms system. Database collecting segment

involves operators, maintenance staff and dis

Estimation of an aging failure process taking into account change

in trend and local perturbation

E. Idée, P. Briand & C. Labart

University of Savoie, LAMA—UMR 5127 CNRS, Le Bourget-du-Lac, France

V. Verrier & P. Bertrand

EDF R&D—Industrial Risk Management Department, Chatou, France

ABSTRACT

Power companies have entered a far more com

petitive market and industrial assets management

is now a major issue. That is why EDF, the major

French utility, must find strategies to detect ageing

phenomenon, have robust estimation of compo

nent reliability or maintenance efficiency in order

to reduce damages and to control costs.

When historical data are collected to model fail

ure process of a component, different trends can

sometimes be observed: at first, constant failure

rate with a law intensity and then an increase in the

number of failures. When change in trends occurs,

classical non homogeneous Poisson process are not

well adapted to describe these different periods.

The purpose of this paper is to propose a general

threshold loglinear process adapted to describe:

• a break in the failure process (for example change

in trend, which are usually observed when failure

come from fatigue mechanism),

• some locally sudden increase in the number of

failures.

This model is based on a classical loglinear proc

ess. The intensity of the threshold loginear process

we studied is given by:

λ( )

( ) ( ) ( ) e

z a bt c z c z = + { } ( )N > { } ( ) t t s N − ≤ 1 2

1 1 1 1 with

z { } t t { } N > { } t t s N − ≤ { } t t≤ < = 2 1 1 1 and

( )t t t

with t ≥ 0, s > 0 and a, b, c 1 , c 2 real.

The observation time is divided in 2 periods

[0,t 1] and [t 1 ,τ], where c 1 describes the first trend

Gamma process classification according to relevant variables: Problem statement and first study

Xuan Zhou Wang, Edith Grall-Maës & Pierre Beauseroy

Institut Charles Delaunay-LM2S, UMR STMR CNRS Université de Technologie de Troyes, Troyes, France

ABSTRACT

With the rapid development of engineering industry, the importance of system reliability and maintenance management has grown (Dekker & Scarf 1998). In order to analyze the reliability or to make a maintenance decision of the system, we could look into a number of sample data that characterize the deterioration level. However, the sample data often come from different system classes, and for each class the deterioration level is supposed to be modeled by a statistical process that depends on certain parameters. It is also assumed that the deterioration model depends on some covariates. Take the corrosion of pipeline for example, we could probably measure the thickness in certain parts of the pipeline as sample data that represent the deterioration level. Besides, as the deterioration process might be changing in different positions of the pipeline, we could refer to the positions as covariates. Since the values of thickness might be

described by some mathematical process, we need to know which process they fit best and make a proper decision to carry out the maintenance based on such kind of information. In a word, the aim is to design a decision rule depending on the covariates to determine the deterioration model that applies to the observed system. For achieving that aim, a partition of the covariate space needs to be learned and the parameters of the stochastic process have to be estimated simultaneously using the data.

In this paper, we consider the deterioration processes as the homogeneous Gamma processes. According to (Van Noortwijk 2009), the Gamma process is appropriate for stochastic modeling of monotonic and gradual deterioration, as it can be well adapted to data in a lot of cases such as creep of concrete, fatigue crack growth and corroded steel gates etc. The property of ‘homogeneity’ rep resents that the transition probability between two given state values at any two times depends only on the difference between those times. A brief summary of Gamma process is given including its definition and several important statistical and

and risers

Pavel Praks

VŠB-Technical University of Ostrava, Ostrava, Czech Republic

Sava Medonos

Petrellus Engineering Ltd, UK

ABSTRACT

Statistical failure frequencies of offshore pipelines and risers are relatively low, which would indicate good reliability. However, if a gas or oil leak occurs and it is ignited, the resulting consequences in the form of explosions and fires, harm to personnel, environmental damage, impairment of assets and financial losses may be very severe due to the high volume of leaking fluid. The relatively low number of observed failures causes uncertainties in statisti cal estimations of failure frequencies. This Paper deals with a probabilistic approach for analyzing data based on counts of events (failures) during the fixed time period of monitoring (pipelines-years and risers-years). There is a problem with uncer tainties of data resulting from observed failures because of i) limited number of observed failures and ii) restricted time-monitoring limitations. As point estimations of failure rates for pipelines and risers can underestimate or overestimate the

computed risk, this Paper gives probabilistic estimates of lower and upper bounds of failure characteristics. Advantages of using these probabilistic estimations for practical risk analyses in the offshore oil & gas production are also discussed.

In this Paper we present typical leak scenarios of hydrocarbons from pipelines and risers on a piled offshore production and risers platform, and analyze uncertainties in failure rates of selected components from the offshore industry. The Poisson model is used for computing confidence limits of the failure rates. Our test case indicates that especially the short exposure times of flexible pipelines risers and steel wells risers cause substantial uncertainties of failure rates, i.e., large confidence intervals. Direct computations and the simulation approach show how these input uncertainties influence a risk model. For example, with 90% confidence, direct computations indicate that IRPA (Individual Risk Per Annum) is somewhere between 3.32E-05 and 7.51E-04. The ratio between these numbers is

Links between reliability Cox model for MV electrical component and the reliability target defined for the global MV electrical network

P. Carer, R. Lattes, L. Guerineau & B. Puluhen

EDF R&D (« Clamart » and « Les Renardières ») France

L. Pierrat

L.&P Consulting Grenoble, University of Grenoble, France

ABSTRACT

In the context of the deregulation of the electric
ity market in Europe, the French regulator defines
reliability and availability target for the electrical
power supply. For example one of the target is:

• 95% of the customer at less than 6 outages
per year (“outage”: long power cut more than
3 minutes)

In order to estimate the reliability indices of the
MV (medium voltage: 20 kV) distribution network,
ERDF (the DSO Distribution System Operator in
France) has:

• to estimate the failure rate of the different MV
electrical component,

• and to compute at the level of the distribution
network the reliability and availability indices.

A first approach (2004-2007) was to obtain for
each component the Weibull law associated to the
failure rate of the electrical component [Spelleman
2007]. Since 2006, in a second approach, more
precise reliability model was developed to take
into account the seasonal variation of the failure

rate due to external weather constrains. Reliabil

ity model for the component taking into account

weather parameter, such as the temperature, the

humidity or the intensity of the lightning, was

developed.

Reliability model elaborated for the electronic

device such as the reliability “Peck” model

[Peck 1986], [Blischke 2000] (Temperature, humid

ity) had been adapted for the MV electrical com

ponent. In the following model for one type on

electrical equipment, the diffusion of the humidity

represents the aging phenomena with the year of

operating of the component, and the temperature

is varying with the seasons of each year:

λ λ D t h o o n e p ( ) , + ( ) ⎡ ⎣ ⎤ ⎦ ( ) T T o ⎡ ⎣ ⎤ ⎦ 1

t: age of the component

On a goodness of fit test for gamma process: Comparison

of an observed process with a reference

Edith Grall-Maës

Institut Charles Delaunay—CNRS UMR STMR—Université de
Technologie de Troyes, Troyes, France

ABSTRACT

The applications of maintenance optimisation

models are numerous. The modeling of deteriora

tion is the basis of most of the maintenance mod

els. Usually, the rate of deterioration is modeled in terms of a time-dependent stochastic process and generally assumed to be a Markov process. Gamma processes have been satisfactorily fitted to various data such as creep of concrete, fatigue crack growth, and thinning due to corrosion. The gamma deterioration process has been applied to model time-based preventive maintenance as well as condition-based maintenance [3].

Statistical goodness of fit tests characterize the discrepancy between observed values and the values expected under a model. For example, they can be used to test if an observation sample follows a spec ified distribution. Since their introduction [2] they have been widely studied in respect to general or specific distribution but rarely studied for proc esses. As far as the author knows, no study deals with goodness-of-fit test for the gamma process. Such test would be of real interest to decide if an observed process is fitted to a reference process in the aim of concluding if an optimal maintenance decision rule is valid for the observed process.

This paper presents a study of a statistical test based on the Kolmogorov-Smirnov test for com paring an observed gamma process with a refer

ence gamma process, in the case of periodic or aperiodic inspection. The null hypothesis is defined as “the observed gamma process sample follows the reference gamma process”. The test is built for satisfying a given first order error.

The well known Kolmogorov-Smirnov test allows to decide if a sample of independent and identically distributed observations is drawn from a reference distribution for a given first order error.

Reliability prediction model of a multi-state system subject to general repair and maintenance with limited failure data

Masdi Muhammad, Ainul Akmar Mokhtar & Mohd Amin Abdul Majid

Universiti Teknologi PETRONAS, Malaysia

ABSTRACT

Effective maintenance management is essential to reduce the adverse effect of equipment failure to operation. This can be accomplished by accu rately predicting the equipment failure such that appropriate actions can be planned and taken in order to minimize the impact of equipment fail ure to operation as well as optimizing maintenance resources. However, accurate failure prediction is often bounded by the scarcity of time to failure data as mentioned by several researchers.

The current study focuses on the develop

ment of reliability assessment model for repair able equipment subjected to degradation by utilizing equipment performance data instead of the normally used time to failure data. The system performance data is gathered and then clustered into several discrete states using a combination of k-means data clustering method and silhouette plots. The theory of multi state repairable system is then used to determine the system reliability based on the state definitions and different repair assumptions.

A repairable system is defined as a system which can be restored to satisfactory working condition by repairing or replacing the damaged components that caused the failure to occur rather than replac ing the whole system. In other words, the system performance degrades into several discrete states prior to total system failure. The degradation process, if left unattended, will often lead to degradation failure that can be attributed to a myriad of factors including variable operating environment, fatigue, failures of non-essential components and random shocks on the system. In addition, the system can experience random failure from any state at anytime upon which a general repair will be performed bringing the system back to the state between new and old. A general preventive maintenance is performed when the system reaches the last unacceptable state, again, bringing the system back to state between old and new. This paper presents a development of model based on discrete time Markov process for a degraded multi-state system subject to both general repair and maintenance to assess the system reliability. The system degradation was quantified by discrete level of system’s performance from

perfect functioning state to complete failure. An actual case study is presented to illustrate the applicability of the model. The results indeed prove the relevancy of discrete time Markov in assessing the reliability of multi-state systems using the system performance data when there is very limited time to failure data. This is shown by the statistical comparison of reliability predictions results from traditional binary assumption using time to failure data.

Reliability prediction of oil wells by support vector machine

with particle swarm optimization for variable selection

and hyperparameter tuning

I.D. Lins, M.C. Moura & E.L. Droguett

Departamento de Engenharia de Produção, Centro de Estudos e Ensaios em Risco e Modelagem Ambiental

Universidade Federal de Pernambuco, Recife, Pernambuco, Brazil

E. Zio

Laboratoire Génie Industriel, Ecole Centrale Paris-Supelec, Paris, France

Dipartimento di Energia, Politecnico di Milano, Milan, Italy

C.M. Jacinto

CENPES, PETROBRAS, Rio de Janeiro, Brazil

ABSTRACT

In oil industry, sudden failures of wells are not

desirable since they bring non-planned costs,

e.g., loss of assets, costumer dissatisfaction, envi

ronmental damages, among others. In order to

prevent these situations, reliability prediction can

be performed so as to enable proper maintenance

planning. Different factors, such as operational and aging conditions, impact the reliability behavior of production systems and a comprehensive analytical treatment may be prohibitive due to the increased complexity of the problem.

Alternatively, an empirical modeling based on observations such as regression via Support Vector Machine (SVM) may be effective as a reliability prediction tool. One of the main advantages of using SVM are: (i) the training step involve a quadratic optimization problem for which the Karush-Kuhn-Tucker conditions for a global optimum are necessary and sufficient, thus SVMs are not trapped in local optimum; (ii) the training objective function trade-offs the machine generalization capacity with training errors. Nevertheless, the performance of SVM depends on a set of hyperparameters required by the training optimization problem.

Besides, in regression problems, the available data set may contain numerous explanatory variables that may be redundant or even irrelevant to enlighten the variability of the response variable.

Situations like this may arise mainly when there is lack of knowledge about the functional relation between the target and the other variables, which is common when Support Vector Regression (SVR) is chosen as learning

approach. Common methods for variable selection, such as the backward elimination strategy, do not allow for the concurrent adjustment of hyperparameters. However, during this incremental procedure, optimal values of the SVR hyperparameters may change, given that the training data set is progressively modified. In spite of that, a new search for the SVR hyperparameters is often skipped due to the additional computational effort. Therefore, this paper presents a Particle Swarm Optimization (PSO) algorithm, which is a probabilistic optimization technique based on the group motion of organisms, for the simultaneous variable selection and SVR hyperparameter tuning. The resulting PSO+SVR methodology is used for the prediction of times between failures of onshore oil wells located in the Northeast of Brazil. Although being related to mature wells of low productivity, onshore activities are responsible for a non-negligible part of the national oil production. The obtained results show that the variable selection procedure, combined with hyperpa-rameter adjustment, enhances the predictive ability of SVR. The outcomes also indicate that PSO+SVR is a promising tool for reliability prediction and it could be part of maintenance framework so as to support decisions concerning preventive actions.

Reliability prognosis for mobile phones: A case study

A. Braasch, F. Plinke, D. Althaus & A. Meyna

University of Wuppertal, Germany

ABSTRACT

Nowadays, technical devices are expected to

operate faultlessly and reliable. Failures espe

cially when occurring during the warranty period

result in extensive costs for the manufacturer and

displease the customer. As there are no absolute

reliable products, measures have to be taken by

the manufacturer to deal with occurring failures

quickly and customer-friendly.

As shown in Pauli (1998) Reliability prognosis

models have been proved to be suitable in practice in the automotive industries since the 1990s to answer quality and reliability issues and to provide an opportunity of predicting the future field failure behaviour. Using this information facilitates a more accurate prediction of required repair capacities or replacements like presented in Braasch et al. (2007). In this paper modified reliability prognosis models concerning the needs of the mobile industry are developed for the first time to provide assistance when predicting serial or end of life replacements. The reliability prognosis model, which is based on the well known prognosis model of the automotive industry, uses field failure data being available dur ing the warranty period. This assures the consid eration of the real field stress in the further steps of the reliability prognosis model. Based on methods like the Weibull-Analysis or parameter estimation a model is presented that analyses the occurring field failures in connection with additional information such as the influence of registration or report ing delays. Furthermore, an approach has been developed concerning the influence of failure can didates (or failure aspirants) due to the censored warranty data (e.g., two years for electronic devices

in Germany). By giving an example of a mobile

phone which was sold in the Mediterranean region

the steps of the reliability prognosis model will be

Risk of postoperative complications after surgeries: Laparoscopic

versus open surgery

P. Jahoda & R. Briš

Department of Applied Mathematics, Technical University of Ostrava, Ostrava, Czech Republic

L. Martínek

Clinic of Surgery, University Hospital Ostrava, Ostrava, Czech Republic

ABSTRACT

Gross numbers presenting morbidity and mortality

are often misguided and distorted because they do

not consider the whole range of factors. For exam

ple the variability of health conditions of the evalu

ated sample of patients, conditions in the moment

of surgery, the process of surgery, health condi

tions of the population and many more. Hence,

they do not allow an objective comparison of the

results achieved and the evaluation of recently

implemented methods is problematic as well.

Therefore, in the beginning of the nineties the

scoring system POSSUM was developed by Cope

land et al. (Copeland et al., (1991)). Using logistic

regression it allows to estimate the risk of compli

cation for individual patients or groups of patients.

The explanatory variables are the physiological

score, P, (characterising the patient’s health condi

tions) and the operational score, O, (characterising

the surgical performance). In this model, the prob

ability of postoperative complications is estimated

by the relation

π (,) (,) , (,) O e e O O = + φ φ 1 (1)

where

φ (P,O) = -5,91 + 0,16P + 0,19O, (2)

The numbers of postoperative complica

tions estimated by the original Copeland’s model

POSSUM were compared with the actual numbers

collected by colorectal surgeries operated in years

2001-2006 in the University Hospital Ostrava.

It was learnt that this model does not simulate the

mentioned data sufficiently.

Considering the failure of above mentioned

model to predict postoperative complications

in our group of patients, we have created mod

els of postoperative complications based on new explanatory variables. We have focused on the group of patients with diagnosis C20. The values of statistical variables Leucocytes (L), and the Operative Severity (S) were proven statistically significant by laparoscopic surgeries. The values of statistical variables Cardiac Signs (C), and the Operative Severity (S) were proven statistically significant by open surgeries. Focusing only

on these variables, we gained simple, nevertheless very accurate models Os – POSSUM 2 (l) for laparoscopic surgeries and Os – POSSUM 2 (O) for open surgeries. Os – POSSUM 2 (l): φ (L,S) = -9,57078 + 3,04722L + 0,892555S, (3) Os – POSSUM 2 (o): φ (C,S) = -2,07602 + 0,467884C + 0,175036S. Using the models Os- POSSUM 2 (l) and Os- POSSUM 2 (o), it is possible to choose an optimal operational technique for a particular patient, to minimize the risk of postoperative complications. Our recommendation is to use laparoscopic method if and only if the unequation 7,49476 + 0,467884C – 3,04722L – 0,715519S > 0. (4) holds. We estimate, that choosing the right operational method, the number of postoperative complications can be reduced by 47,56% (but not more) in comparison with the worst scenario possible (all the patients operated with the unsuitable operational technique) and by 31,75% compared to the possibility, where the operational technique is chosen randomly in proportion 1:1. REFERENCE Copeland, G.P., Jones, D. & Wakters, M. (1991). POSSUM: a scoring system for surgical audit. Br. J. Surg. 78, 356-360.

The RAW concept: Early identification and analysis of product failure

behaviour in the use phase

S. Bracke & S. Haller

University of Wuppertal, Department of Safety Engineering and Risk Management, Germany

ABSTRACT

The increasing complexity of product functionality

and manufacturing process parameters often leads

to complex product damage symptoms during

the product life cycle. The damage causes must

be detected at an early stage after product market

launch to avoid further risk effects of the field fail

ure modes. The very early identification of the dam

age causes requires new risk analysis approaches:

The analysis of field data based on a small amount of field data is one excellent possibility. Regarding to the outlined requirements the Chair of Safety Engineering and Risk Manage ment at the University of Wuppertal developed the ‘reliability analysis based on warranty databases (RAW)’ concept for the early, economical and detailed statistical reliability analysis of guaranty and warranty databases. The application of the RAW concept has the following goals:

- Comprehensive mapping and analysis of compo nent failure behaviour. Furthermore analysis of conducted product optimisations, climatic and regional influences (through customer usage) based on different production months/batches or different points of use.
- Detection of damage causes based on few field damage cases (small sampling sizes) at an early stage after market launch.
- Support the selection of appropriate actions for product improvement at an early stage is feasible.
- Technical analysis of damaged components based on a reduced amount of requested field components.

The elementary phases of the presented RAW

concept are field data acquisition, graphical analysis as well as analysis with nonparametric and parametric statistics. Performing field data analysis at an early stage of the field monitoring phase leads to a small amount of data with respect to the damaged field components. For realising an early field data analysis, the RAW concept contains a combined application of nonparametric statistics. Nonparametric distribution-independent statistics allows significance analysis based on a small amount of data. More extensive data at a later time period enable the usage of parametric statistics. The analysing results based on nonparametric analysis are now verified and supplemented with the appendant parameter interpretation. This paper outlines the effectiveness and use of the RAW concept in a close to reality case study of the automotive industry. The focus of the case study is the analysis of an electronic control unit including different failure modes and software updates. The results of the RAW concept application show significant identifications with respect to changes of the control unit failure causes, the failure rates, frequencies and trends. Therefore, a comprehensive evaluation of the control unit and software optimisations is feasible. THEMATIC AREAS Reliability and Safety Data Collection and Analysis, System Reliability Analysis, Automotive Engineering

Trialling the use of safety performance indicators within Great Britain’s

railway industry

K. Thompson, J. Heavisides, G. Bearfield & D. Griffin

RSSB, London, UK

ABSTRACT

Safety critical industries traditionally rely heavily

on failure and incident data to monitor performance

and this is certainly true of the railway industry,

with the key monitoring database, the Safety Man

agement Information System (SMIS), primarily

reporting safety related incidents. Such measures are referred to as ‘lagging’, ‘reactive’ or ‘outcome’ related. The consequence of this approach is that improvements or changes are only determined after something has gone wrong. However emerging practice in safety management asserts that effec tive management of hazards requires a proactive approach. Information to confirm critical systems (such as competency management, inspections and responding to audit findings etc.) are operating is also needed. These measures are referred to as ‘leading’, ‘active’ or ‘activity-related’). Both types of measures need to be effectively integrated into an organisation’s safety management system—a practice known as ‘dual assurance’.

There is much emerging practice in the area of the application of safety indicators across a range of safety critical industries internationally. Progress in the practical application of the theo retical concepts has advanced as a result of the rec ommendations of the Baker Report (Baker et al., 2007) into the Texas City oil refinery accident which was published in 2007. In the United King dom (UK) the Health & Safety Executive (HSE) has published guidance (HSE 2006) on the develop

ment of process safety indicators for major hazard

industries and this guidance has been successfully

Warranty data analysis for service demand forecasting: A case study

in household appliances

O. Borgia, F. De Carlo & M. Tucci

“S. Stecco” Energetics Department of Florence University, Florence, Italy

EXTENDED ABSTRACT

The prediction of warranty claims is a major

interest for the after-sales department of a manu

facturing company, since all the goods produced

are subjected to a warranty of varying duration.

Indeed, the costs that the producer has to pay for

the failures occurred during the warranty period,

are one of the items that contribute to form the

goods retail price.

This article presents a methodology to predict

the number of technical assistance interventions

during the warranty period. The study was devel

oped relying the expertise gained by analyzing

a product in the household appliances.

We carried out a case study to assess the qual

ity of the approach. Starting from field data of

technical support for products manufactured in

a given year and using a simulation approach, we

predicted the number of technical assistance inter
ventions for the products of the following year.
The ability to predict the cost-related technical
assistance during warranty enables to appropri
ately size the necessary resources and, therefore,
to optimize costs. The advantages are twofold: on
the one hand, you can reduce the selling price and,
on the other, you can increase the contribution
margin.
The study shows that it is possible to predict the
demand for technical assistance during the war
ranty period for products manufactured during
a given year, relying on knowledge of the technical
data of the products made in the previous year.
The main difficulty in this type of analysis
lays in the fact that, during its life cycle, a prod
uct exhibits a varying reliability that changes over
time. Indeed, if we consider a generic product, we
observe that, during the launch, it has a certain
service request. With the passing of time, we can
appreciate that reliability tends to increase by means
of re-engineering and manufacturing refinements.
This improvement is not obvious because other
causes may, however, generate a deterioration of
quality such as, for example, changing a supplier,

or changing a component of the product. As a result of what has been said, we can say that the characteristic parameters of the reliability function of the product (like the shape factor and characteristic life of the Weibull function), may vary over time. The goal of this study is the prediction of service demand related to the warranty claims of a population of products. It was decided to proceed with a simulation approach by developing a model to simulate the service calls of a products population, known its production profile. The main information used were the field data from the warranty calls. The major strengths of the adopted approach are twofold. First of all, the simulation model considers the latency period of the products. This is the time that elapses from the date of product manufacturing and the first use by the costumer. This analysis was the key to determine the correct time to the first failure. The second distinctive feature of the study is the use of a variable failure distribution depending on the manufacturing date of the products. This type of approach was necessary since we had clearly identified the phenomenon of product maturity. In general, the maturity of the product is due to a dynamic management of the product life which aims to a continuous improvement. It also translates into a dynamic behavior of the product service demand. It is obvious that this approach has required a thorough study of the field data aggregation criteria to determine the product groups with a homogeneous reliability behavior. Specific business needs, which have arisen in the course of the study, and research interests will be developed in following studies with the goal of maintaining the current model performance in terms of predictive capabilities, despite of a strong reduction of the historically database. This requirement is justified in the light of the continuous reduction of the products life cycle. So in the future works we are going to face a fast reliability prediction and not more the simply reliability prediction. Risk and hazard analysis This page intentionally left blank

A modelling framework for model based risk analysis

Jean-Marie Flaus

G-SCOP, Laboratoire des Sciences pour la Conception, l’Optimisation et la Production de Grenoble—

UMR5272, Grenoble Cedex 1, France

ABSTRACT

Traditionally, risk analysis projects use a document based approach: the description of the system and the result of the analysis are expressed in a textual way or in drawings without an explicit semantics. The consistency and the relationships between documents are difficult to assess and it is rather difficult to extract and manipulate needed infor mation for validation or for another purposes, or to capitalize knowledge.

An approach to overcome these limitations is to use a model based approach for risk analysis. This would allow to represent knowledge in a consistent manner, easy to manipulate and to transform.

In this work, we present an approach for model based risk analysis, which can be used with any classical methods such as PHA, HAZOP and FMEA.

The idea is to describe the physical system according to three views:

- the first one describes the structure (physical and functional),
- a second one, optional, with information about the behaviour when this is useful,
- and a third one to express the risk analysis result.

The first view, called SysFis, has three kinds of

models blocks: systems, functions and resources:

a system may be seen as an entity whose goal is

defined by a set of functions which requires and/or

consumes physical elements, called resources, to

produce and/or acts on others resources. From a system engineering model point of view, the SysFis modelling view uses function and resources that may be seen as two types of components used to describe two complementary aspects of the system: the physical and functional ones. This view may be optionally completed by the behaviour view, called SimFis, which allows for the addition of variables and constraints in order to provide more details about some parts of the system. As the goal is to avoid modelling overhead to the risk analyst, this model view is optional and may be partial. The result of the analysis is then expressed using the last view, called DysFis, which allows the representation of the abnormal behaviour of the system at a level of abstraction which is relevant for risk analysis. This view is based on model blocks defining abnormal events and rules for connecting them. A small set of abnormal events types has been defined. This model is related to the structuro-functional model and to the behaviour model. It allows to automatically generate tables for various risk analysis and various representations such as fault tree, consequence tree, bow tie diagram and to compute probability or severity. A software tool, XRisk, has been developed to implement and to test this modelling approach. This tool allows to perform model based risk analysis and is able to generate, from a common representation, various risk analysis views such as PHA, FMEA, HAZOP, or MOSAR.

A linear programming approach to risk prioritization in FMEA

Pauli A.A. Garcia, Ilton C. Leal Jr. & M.A. Oliveira

Fluminense Federal University, Volta Redonda—RJ, Brazil

ABSTRACT

Risk analysis is an activity which is commonly

done by reliability engineers and/or risk analysts

from any industry. The results of a Probabilistic Safety Analysis (PSA) provides much information to make decisions about maintenance policies or about care to be taken over some critical points of a system (Fullwood, 2000). The purpose of a Failure Mode and Effect Analysis (FMEA), in a PSA, is to find and supply semi-quantified information about the different ways that the system can fail, and constitute relevant inputs to the system modeling (IAEA, 1992).

The data gathered through a FMEA should be considered in a decision making process concerning risk. The data which should have influence over the decision maker are associated with occurrence probability (O), severity of the respective effect (S) and with the potential to detect that something is going wrong. This potential is called detectability (D). (Bowles, 1998, Bowles & Bonnell, 1998).

Up to now, different approaches have been considered in turn to reduce the erroneous interpretation occasioned by the traditional Risk Priority Number (RPN) (Bowles & Bonnell, 1998, Bowles, 2003).

The traditional RPN consist of the product of the three criteria, i.e., RPN = O.S.D. These criteria

are considered in an ordinal range, commonly, from 1 to 10, where greater the order worsts the case. The main problem was the one associated impor tance of the severity criteria. For example, a failure mode with the following criteria, O = 1, S = 10 and D = 1 is considered less important than another one with O = 4, S = 4 and D = 4. The former have an RPN = 10 and the last one have a RPN = 64, which will be prioritized.

In the present work one proposes the use of the traditional constant return to scale DEA model (Charnes et al., 1978), considering an output approach. In this approach, the efficiency frontier identifies the improvements for each critical fail ure mode, enveloped by the frontier. To make the prioritization proposed by DEA more realistic, we will consider the effect of weight restriction, i.e.,

Ageing and life extension for safety systems on offshore facilities

S. Håbrekke & P. Hokstad

SINTEF Technology and Society, Safety Research, Trondheim, Norway

ABSTRACT

A large number of facilities on the Norwegian Continental Shelf are approaching or have exceeded their design life. Many fields, however, have remain

ing recoverable oil and gas reserves, so that life extension can be profitable. But in order to extend operation beyond the design life of the facility it must be assured that the safety integrity is maintained throughout a life extension period. This means that it is required to investigate the condition of structure, equipment, procedures and organisation, and also the compliance with requirements etc. for the entire facility.

So far, studies on ageing of offshore facilities have focused on main systems, such as structures and pipelines. The present paper in particular addresses ageing issues related to offshore safety systems, including Safety Instrumented Systems (SIS), during a potential life extension period.

It is a main objective to prevent that Life Extension (LE) will increase the probability of major hazards, such as for instance blowout, fire, explosion, ship collisions or structural collapse. To avoid major hazards, it is important to have control with the safety systems, the barriers, their state, and the risk factors influencing each barrier. Thus, to ensure the integrity of the entire facility throughout a possible life extension period, the main focus is on such systems and barriers. Each system

should therefore be broken down into subsystems

or components, following a barrier line of think

ing. The focus is on physical barriers related to the

actual equipment and barrier systems. In a com

plete analysis of ageing, the level of breakdown

should proceed until we arrive at units with unique

degradation mechanisms or to maintainable items.

Typical barrier elements for offshore safety systems

are power supply, logic, detectors and valves.

When LE is considered the main question is how

to perform the process for deciding whether LE can be performed without compromising safety. The length of a possible LE period depends on the facility's ability to maintain the technical, operational and organisational integrity. The first task is to identify all (possible) challenges related to ageing and future operation; incorporating the whole facility and all safety related systems and equipment on the facility. For instance, will there be any changes during a future operational period, resulting in challenges? Secondly, the risk related to these challenges should be analysed (for the entire LE period). Finally, a maintenance and modification plan to reduce the risk contribution from all equipment and systems must be prepared and implemented in order to maintain (or, if required, improve) the safety integrity and to comply with the current requirements. Lack of knowledge about ageing and degradation mechanisms for certain equipment types, is relevant for safety systems, in particular ageing of electronic systems may be a challenge. Besides increasing failure rates due to e.g. material degradation, increasing demand frequency is important to be aware of during LE. Tripping the safety systems (either due to real demands or spurious trips) can increase as the entire facility ages. Also, Common Cause Failures (CCFs) are important for the life extension evaluations, in particular for redundant equipment. There are various types of dependencies, e.g. physical-, functional, location-/environmental-, plant configuration—or human dependencies. In general a CCF

analysis should consider failures due to common causes/ stresses. Common ageing of various components and equipment on a facility during the LE period can possibly result in a common (sudden) increase in the failure rate. This means that the contribution from CCF, which often is the largest contributor to the total PFD compared to independent failures, may increase.

Applying a systemic model of accident within a system for treatment

of contaminated materials

K. Hardy & F. Guarnieri

A.A. Center for Research on Risk and Crisis, Mines ParisTech, France

ABSTRACT

Contaminated sediments are a source of hazards

to people and ecosystems because of the presence

of toxic substances that can cause major natural

disturbances. The situation of some contaminated

sites is not without consequences on health, eco

nomics, politics or law.

Therefore, any approach to treatment of contam

inated sediments must be accompanied by a hazard

analysis approach in order to avoid any collateral

damage on the entire system. Indeed, any manipu

lation of sediments contaminated always causes

a release of contaminants into the environment.

Furthermore, this manipulation exposes operators

to numerous risks, mostly chemicals.

Thus, treatment of contaminated sediments

requires a comprehensive approach taking into

account the safety assessment and maintenance of

a set of constraints in order to avoid accidents.

In this context, a solution is provided through the

systemic accident model called STAMP (System

Theoretic Accident Modeling and Processes). This model was developed by Professor Nancy Leveson, Massachusetts Institute of Technology (MIT), within the framework of socio-technical system to address a safety need for non-linear behavior. This model does not consider an accident as a chain of events but as a problem of control within its structure. It allows the analysis of a system for reducing pollution by modeling its structure and its dynamic behavior. STAMP model is a systemic model based on Bertalanffy's general theory of systems. This theory is not without limits to consider complex systems. This article is organized into three sections: - A presentation concerning the system of treatment of contaminated sediments - A presentation of STAMP model and technology STPA - An implementation of STPA on the processing system and a discussion of results. - A presentation of limits of STAMP model.

Assessment of loss results by means of multi–criteria analysis

P. Suchardova, A. Bernatik & O. Sucharda

VŠB–Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

This paper discusses the results from the long-term

research that focused on the assessment of major

accident consequences using the MDCA approach.

The research has been carried out in cooperation

with industrial companies and includes modeling

of potential extraordinary events affecting tech

nological parts. Within previous research parts of

the infrastructure that transport metallurgical and technical gases, gas–holder with coking gas and storage of the hazardous benzole were modeled and evaluated. This article presents these techno logical parts in detail.

The goal of this article is to demonstrate the usage of MDCA in a risk management area. This task is supported by a real case study which has been carried out in a metallurgical international industrial company situated in Moravian–Silesian region of the Czech Republic in the middle of Europe. This paper also discusses contribution of this analysis to the risk management area.

The proposed MDCA approach determines the consequences of major accidents where the goal is to evaluate particular serious accidents, to deter mine their order and their significance such as gas-holder, vessels, infrastructure and others.

The Figure presents the ranking value for five

Figure 1. Multi–criteria decision analysis. Figure 2. Range of rankings.

Evaluation of regional risk analyses in Norway

O. Njå

University of Stavanger, Stavanger, Norway

G.S. Braut

Stord/Haugesund University College, Norway

K. Russell Vastveit

University of Stavanger, Stavanger, Norway

ABSTRACT

The regional, public system of governance in Norway is traditionally divided into 19 counties (including the capital Oslo which is a municipality as well as a county) and 430 municipalities. The highest ranking governmental representatives at the county level, the county governors, are tasked with carrying out county risk and vulnerability analyses. The purpose of conducting the assessments is the development of county risk pictures. Though the county risk and vulnerability analyses are mandatory the content, nature and process of the task have not been rigidly defined, thus the different county governors have solved the task in quite different ways. An aim of this project is to suggest topics that should be considered when describing the expectations and clarifying the formal requirements to such analyses.

This paper presents an evaluation of these regional risk and vulnerability analyses based on data collection done through a project for students at a master degree course in risk governance. The

overall goals, organization of the risk analysis process, hazard identifications, risk modeling, data collection, risk presentations and the anticipated subsequent use of the CRAVAs have been the focus of the evaluation. There are many different ways to interpret the role of risk analyses in risk management. In this evaluation we have adopted Stephen R. Watsons 20 year old view on risk and risk analysis which we find should be the perspec tive that guides regional public risk governance. Watson says: “Probabilistic safety analysis should be interpreted as reasonable argument, rather than an objective representation of truth.” This view may be seen as a request for dialogue and reflec tion about risk analyses.

At present we find that the risk analyses under taken by the counties show a large degree of vari ation in terms of contents and comprehensiveness. They range from being analyses that show signs of being mandatory bureaucratic exercises, focusing on services provided by public bodies to analyses that are designed to influence and guide activities in entire counties. Despite the current large differences we find that such analyses can be important tools for county governors in their work to provide and implement strategies for developing county risk pictures. Based on our evaluation of the different risk analyses we suggest that a new approach to uncertainty assessment in the analyses is needed. This approach must encompass an openness to comprehending changes, a willingness to search for a better understanding of critical systems in the counties, and an understanding of the functionality of the systems, the

intersections between them and the related vulnerabilities. Only making more specific requirements related to the format of the analyses and proposing questions to be answered will probably not be sufficient to ensure a more uniform approach to this task by the county governors. In addition we find that clarification of the role CRAVAs should play in county wide and municipal planning as well as the work done by the county governor is necessary. The data that has been gathered and the broad discussions that have often taken place during the analyses offer good opportunities for continued learning. This learning should not only be seen as a process for increasing knowledge and competence, but also as a fundament for continuous updating of the analyses so that valid risk pictures can be presented to the different actors in the societal planning processes. If this is to become a reality a core requirement will be that the county governors should strive to establish a sound knowledge base for the CRAVA-process. This knowledge base must contain general scientifically based information in addition to knowledge about local conditions. Systems for gathering information and knowledge from the municipalities should be a part of this as the CRAVAs must not only present a top-down perspective.

Fragment launching conditions for risk analysis of explosion and impact scenarios

R.G. Salhab, I. Häring & F.K.F. Radtke

Fraunhofer Ernst-Mach-Institute, Efringen-Kirchen, Germany

ABSTRACT

Explosives and impact are an often used tactic in terrorist events. For a quantitative risk analysis of such security threatening scenarios in particular the fragment hazard sources must be described. Examples for the generation of fragments are homemade bombs, vehicle born improvised explo sive devices, contact detonations and building structures penetrated or perforated for example by

fragments, bullets or rockets.

We present distributions that describe the initial launching conditions of the generated fragments or debris. Within risk analyses these distributions determine initial positions, velocities, directions and masses. They can be used to represent experi mental, empirical-analytical and computational simulation data. We discuss the restrictions of the often used point source approximation, various normalization conditions and effects of discreti zations of distributions. We also use multiple and higher dimensional distributions going beyond the standard point source approximation. The advan tages of the distribution types are discussed for typical applications.

First of all a fundamental set of sizes needed for describing hazard sources as well as ammuni tion storage depots are introduced, which give an insight to the complexity of the problem of determining launching conditions of fragments or debris.

To simplify descriptions approximations and simplifying assumptions are presented. Often only based on these, analytical or numerical calculations are possible. Their advantages and their disadvan

tages as well as limitations are presented.

To specify launching conditions, the rotational

symmetric fragment matrix is introduced, which is

the most used structure in this field. Possible gen

eralization and simplifications are discussed, which

can also be used for determining debris launching

conditions.

Analytical-empirical as well as experimental

Improving reliability allocation in a complex repairable system

using STRR allocation technique

W. Baun

UTC Power, South Windsor, CT, US

ABSTRACT

The task of allocating failure rates to components

within a complex repairable system is executed

early in a product development process in order to

set reliability targets for those components. This

allocation process is often accomplished versus

more than one constraint, for instance to achieve

an overall system-level failure rate target, λ_{sys}, and

to achieve an overall system Life Cycle Unplanned

Maintenance Cost target (LCUMC).

Traditional allocation methods leave it to the

judgment of the analyst to decide how to allocate

failure rate amongst the components. Presumably, there exists an optimum component allocation solution that would most effectively meet those goals. Because there are an infinite number of com binations of component failure rate allocations which could achieve the system-level targets, these approaches are somewhat unsatisfactory in that they leave the analyst to question if their particular allocation solution is a good one.

This paper demonstrates the application of an alternative allocation technique which employs genetic algorithms to find better allocation solutions—solutions which meet product reliabil ity goals while attempting to minimize a metric called System Total Reliability Risk (STRR). STRR is a measure of the aggregate risk inherent in the allocation solution, where risk is defined from the perspective of eventual product reliability and maintenance costs. It is the prob ability that the actual λ sys is ultimately found to be higher than its allocation, and the consequences of that higher failure rate in the form of higher-than expected LCUMC and λ sys . It is also a measure of the degree of difficulty to achieving the proposed component failure rate allocations, given that dif

ferent types of components generally have a limit

to the best failure rate that can be achieved in

Managing inconsistency in safety analysis: An initial exploration

L. Sun & T. Kelly

Department of Computer Science, University of York, York, UK

ABSTRACT

It is typical for any system safety justification to

rely upon multiple forms of safety analysis. It is

unacceptable to have (unexplained) inconsistency

between these models. However, inconsistency will

commonly arise in safety analysis. Safety analy

sis is often conducted iteratively throughout the

engineering lifecycle, using a variety of different

techniques, and according to different viewpoints,

boundaries and assumptions. Although engineer

ing practice shows that it is difficult to eliminate

these inconsistencies completely, it is necessary

to understand how analyses can be inconsistent

and what we can do to rationalize and justify the

inconsistencies.

The usage of the term of consistency is very

different according to its context. In this paper,

we clarify and frame the working meaning of

consistency in safety analysis in this study as the

description of logic and data in safety analysis is

in agreement with each other or hold some prede
fined relationships.
Then, a small-scale case study is introduced and
the initial observations from a set of safety analysis
results from different analysis groups are presented.
The major findings from the case study include the
inconsistent analysis structural data, the inconsist
ent language expressions, and the inconsistent con
tent of the results. In addition, the limitations and
features of the cases under study are analyzed.
On the basis of the clarification of the mean
ing of consistency and our direct observations
obtained from the case study results, the follow
ing five possible organizing principles are explored
to support the classification of the inconsistency
in safety analysis: data elements required by the
safety analysis methods; the location of inconsist
ency in safety analysis; the causes of inconsistency,
the consequences of inconsistency; and the types
of consistency checking rules.
Considering the variability and features of the
organizing principles described, taxonomy for
describing inconsistency in safety analysis is pro
posed. The primary perspective is from the location

petroleum industry—operational categorization of events

J. Seljelid, S.A. Kvalheim & O.M. Nyheim

Safetec Nordic AS, Trondheim, Norway

J.E. Vinnem

Preventor AS/University of Stavanger, Stavanger, Norway

ABSTRACT

The Trends in Risk Level project initiated in 2000 by the Norwegian Petroleum Safety Authority (PSA) aims to monitor the risk level development on the Norwegian continental shelf. An extensive database containing 1300 descriptions of inci dents of falling objects in the petroleum industry between 2006 and 2010 have been analysed based on the initiating event categories developed in the BORA (Barrier and Operational Risk Analysis) project. The BORA categories were modified to fit events of falling objects, using a sample of 100 event descriptions from the database. The remain ing 1200 events were categorized using the new cat egories. The aim of the project is to identify and validate operational categories that are suited to inform the industry of specific hazards connected to common offshore work processes. The complete procedure of category development, testing and

results are presented and discussed in the paper.

The Risk level project has established a large

database of incidents with falling objects from

cranes, in the derrick and on the drill floor, from

movements of equipment in the process areas as

well as from various scenarios where objects may

fall, such as during erection of scaffolding. The

paper gives an overview of causes of falling objects

in the work processes related to:

- B_: Drilling and well activities.

- K_: Crane related work processes.

- P_: Processing related work operations.

- G_: Work processes not related to drilling, well, crane or process operations.

Based on the generic main categories in BORA

(Vinnem et al., 2007), a set of sub-categories was

developed through an exploratory review of inci

dents. The categories were clarified through discus

sion and then validated in a new sample through

a blinded peer review. Inter rater agreement of

26 initiating causes of 29 reviewed was judged to

be satisfying, and the categories were applied to

On software interoperability in accident consequence assessment

S. Contini, L. Fabbri & V. Matuzas

European Commission, Joint Research Centre, Ispra, Italy

M. Binda

THS Informatica, Besozzo, Italy

ABSTRACT

The Interoperability of different risk analysis software tools is a very important aspect that would strongly and effectively support the work of safety authorities in their reviewing activity of safety reports for Seveso-type installations. This reviewing activity could indeed be not very straightforward if the models and software tools used by the authority are different from those used by the operator of the industrial facility under scrutiny.

Software interoperability has recently been addressed in many application fields and it consists of the definition and the recognition of a common data format for data exchange amongst different software, which are intended to perform similar tasks and functions. This would clearly allow the use of the same set of input data and facilitate a lot the comparison of the software output and the associated results. In the case of risk analysis, software interoperability would facilitate the dialogue and accelerate the consensus building between the manufacturer and the licensing

authority. Moreover, it would be of great benefit also to model developers and software developers.

Some initiatives in this direction have already been launched in the nuclear sector. The “Open Initiative of Next Generation PSA Software” is an important activity to advance the state of the art in methodologies and tools for the probabilistic analysis of nuclear installations. A “Model Representation Format for Probabilistic Safety Assessment”—based on Fault Trees and Event Trees—was developed. A major task of this initiative was the definition of a common format for data exchange and the execution of a series of experimental tests on a number of software tools for PSA. A first attempt to study the interoperability among accident-consequence tools (fire explosions, dispersion of toxic substances into the environment), used in the chemical sector, was performed by the authors. The consequence assessment represents a very critical phase in the risk analysis process of Seveso-type installations. A first prototype of a common data exchange format was developed and tested on a number of commercially available software tools. Even if this preliminary study did not touch all aspects of the problem, it allowed addressing some of the main issues associated with the definition of a common data format. The paper will describe the reasons for the need of a standard format in risk analysis, the results of the project and possible future extensions.

Risk assessment of dropped and dragged anchors to offshore pipelines

Luiz Fernando Oliveira & Darío Gusovsky

DNV, Paris, France

ABSTRACT

Dropped and dragged anchors are among the dominant causes of potential external damage to subsea pipelines in general. There are records of several accidental events of anchor damage to off shore pipelines in the North Sea area reported in

the UK-HSE PARLOC database (UKOOA 2003).

The pipeline damage caused by such events varies from simple scratching of the external coating to complete rupture of the pipeline. The associated consequences may vary from large expenditures with stoppage and repair of the pipeline to sig nificant loss of lives in case of rupture of a gas pipeline near a populated offshore installation and severe environmental problems in case of rupture of a large oil pipeline.

This problem has already been studied in some papers in the open literature (Kim, B.M. 2005, Rességuier, S. et al., 2009). In this paper a com prehensive methodology for the quantitative risk assessment of dropped and dragged anchors to offshore pipelines is presented which makes use of existing AIS ship tracking data for defining trajec tory and crossing frequency, distribution of ship and anchor types, emergency anchoring condi tions, anchor impact energy, damage mechanisms, pipeline mechanical characteristics, soil properties and conditional probability of damage levels.

An application is presented for the case of a 24” oil pipeline from an offshore platform to an onshore terminal. The pipeline runs through an

area of intense and varied ship traffic. Results are presented per pipeline kilometer (kp) and com pared to typical risk tolerance criteria used by international pipeline operators. the pipeline. The anchor damage to the subsea pipelines are divided in two types of interaction mecha nisms: 1) damage caused by dropped anchors, and 2) damage caused by dragged anchors. Damage caused by dropped anchors occurs

Safety assessment methodology for a UAV development program

Celik Sirma

TAI—Turkish Aerospace Industries, Inc, Ankara, Turkey

ABSTRACT

Risky missions and pilots' physiological limits render Unmanned Aerial Vehicles (UAV) advanta geous in both civil and military operations. With the rise in their usage, UAVs started to share the civilian airspace with manned aircrafts. Result antly, people on other aircrafts and populated areas started to be endangered. Even though there are some rules for UAVs flying in the civilian airspace, they are still considered as a potential for mid-air collisions and uncontrolled crashes. In either case, catastrophic conditions are possible. This is the main reason of why safety issues of UAVs are pop

ular and important.

Safety analyses of the UAVs are more serious

than those of manned aircrafts, since these intel

ligent systems comprise highly complex systems

such as autopilot, sensors, airframes, and embed

ded computing platforms. Ground systems, con

trolling software(s) and data links make system

safety analyses more challenging when compared

with conventional aircrafts' analyses. Furthermore,

failures of UAVs are harder to identify due to lack

of pilot sensing (such as noise, smell, vibrations

etc.). There are several systems which the pilot is the primary means to sense the failure such as ice, fire etc. For UAVs, failure cases can lead to more critical repercussions since they may not be detected in a timely fashion. Therefore, it is important to define appropriate safety objectives and requirements, and decide on the process. There are several regulations and study groups for UAV safety issues. However these regulations are too general such that they enclose all types of UAVs. Thus, indigenous and innovative approaches need to be carried out during the safety analysis of the UAV design process, according to the operational areas of the UAVs. This paper highlights system safety analysis process implemented during the design phase of a Medium Altitude Long Endurance (MALE) UAV. Since available regulations do not completely meet the needs, additional rules are applied and these supplementary rules are hereby described. Applied standards, participants, system safety process sub-contractor management for safety program, analysis details, and tools are illustrated. Results of the study are explained and main differences in approach are explained. This paper was prepared aiming to be a guide for future UAS safety studies.

Towards an integrated risk model for hydrocarbon industry operation

B.J.M. Ale, D. Hanea, C. van Gulijk, P.-H. Lin, S. Sillem &

P. Hudson

Technical University Delft, Safety Science, The Netherlands

ABSTRACT

The recent blow-out and subsequent environmen
tal disaster in the Gulf of Mexico have highlighted
a number of serious problems in scientific think
ing about safety. One of these is that our current
thinking about how accidents happen, and all the
management systems based on that approach.
This is particularly clear in the case of what can
be described as low-probability high-consequence
accidents which, while quite rare, do not appear to
be reducing in frequency unlike simpler and higher
frequency personal accidents. The suggestion is
that linear and deterministic models of accident
causation are insufficient to catch the residual fac
tors and their interactions.
The current development builds on the earlier
developments in the IRISK, ORM and CATS
projects to connect the descriptions for manage
ment, human behaviour and technology into a sin
gle framework that allows a more in depth analysis
of the interdependencies. Probability distributions,
rather than simple bifurcations, are used to take
account of the wide range of context-dependent

factors that can ultimately result in disaster. This novel approach to probabilistic models, based on Bayesian Belief Networks, has already been successfully applied in civil aviation and developed a rigorous framework capable of being applied to other high-hazard industries.

To develop the human behavior model the overall context has been examined within which risks are taken by organizations given a license to operate by regulatory bodies. Perceptions of risk appear to be misaligned between the top and the bottom of organizations and there is a clear need to develop a common understanding, between executive management and those performing the actual operations. A well motivated theoretical framework has been developed to allow the move from hindsight to foresight in the broad area of risk.

Specific attention is given in the development to the incentive structure of operators, staff and managers, which in the previous models was indicated more generally by motivation and conflict resolution. An incentive structure represents an empirical framework for an organisation which characterises the relationship between specific behaviours of employees and the probabilities of receiving various incentives. The work reported here was aimed at a proof of concept of the approach at two sites of the same company. This paper described the initial preparatory steps towards an integrated model for risk model for the risks of

hydrocarbon industry operation. It feasibility of basing this model on previous work in the WORM project and the Bow-Tie analyses and using the BBN approach developed is CATS is shown. The expectation from defense in depth thinking, that adding an extra barrier will always reduce overall failure rates may not be valid. The failure rate of this extra component is in part influenced by the same managerial mechanisms that influence the probability of failure of the existing safety systems and the addition of extra barriers may increase the isolation of operators from the reality they are controlling and even make failure to detect (one of the necessary defenses) less likely. The initial analysis shows that such common cause failures can be adequately modeled in the BBN system, without the need for artificial non-model correction factors. This does not take away the considerable uncertainties in the numerical evaluation that still exist and need further analyses, especially for the cases in which large investments are under consideration at the one hand, and large negative outcomes could be the unfortunate result on the other. Even though these numerical uncertainties exist, the comparison between different policies can be made on a much sounder basis, recognizing the overarching effect of human behavior, on which the management of the company has a large, but not necessarily determining influence. The work was fully funded by Royal Dutch Shell plc.

Towards CFD fire modelling applied to quantitative risk analysis

S. Vianna, K. Shaba, J. Pujol & A. Garcia-Sagrado

Det Norske Veritas, Energy Solutions, London, UK

L.F. Oliveira

Det Norske Veritas, Energy Solutions, Paris, France

ABSTRACT

Fires on offshore platforms contribute to a sig

nificant part of the overall risk. Nevertheless, the

methodologies that are currently used to estimate

fire risks, impairment of safety functions and

design of fire protection and mitigation means

may be coarse and based on subjective opinions and standard solutions. Prediction of fires and radiation impact could be performed using free field models. These models are based on fires in open terrain, and work fine for the far-field which is a typical situation of interest for most onshore installations. However, in an offshore module, the fire is constrained by walls and decks and confine ment which will completely change the location and impact of the fire. The free field models usu ally apply constant surface emitting powers from the flame surface. This radiation flux is largely varying dependent on the flame thickness and temperature, causing the free field model to have a considerable uncertainty compared with a more detailed CFD (Computational Fluid Dynamic) model. Figure 1 shows the fire dynamics com parison with experimental data for two different numerical approaches. It can be noted a good agreement with experimental data.

After Piper Alpha accident in particular, the uti lisation of CFD has become reality. An example of CFD combined with risk analysis techniques can be found in Vianna (2005). CFD (Computational Fluid Dynamics) has been combined with risk

analysis techniques in order to provided a better understanding of the risk and help on its management. Gas dispersion, gas detector optimisation, explosion modelling, toxic release are some of the analysis which have been performed with CFD combined with risk analysis approach (Oliveira & Vianna (2005), Vianna & Cant (2010)). The fire modelling is also an important aspect of the risk.

An evaluation of the risk governance of civil aviation during the 2010 volcanic ash cloud

H. Veland & T. Aven

University of Stavanger, Stavanger, Norway

ABSTRACT

In this paper we evaluate the European authorities' handling of the 2010 volcanic ash cloud originating from the eruption of the Icelandic volcano Eyjafjallajökull. The evaluation is based on a comparison of the actual risk management against established principles and criteria for risk governance (management) as well as a set of risk governance deficits developed recently by the International Risk Governance Council (IRGC). Risk governance deficits are defined as deficiencies (where elements are lacking) or failures (where actions are not taken or prove unsuccessful) in risk

governance structures and processes. These princi
ples, criteria and deficits relate to the assessment
and understanding of risks, including the collec
tion and development of knowledge, and to the
acceptance of responsibility and the taking of
action in order to manage risk. In the paper we
specifically address the assessment and treatment
of uncertainties, and the use of the cautionary and
precautionary principles.

Our initial hypothesis was that the actual risk
governance was, to a large extent, in compliance
with defined principles and criteria of good risk
governance. In the evaluation, we focused espe
cially on the handling of uncertainty, and on three
aspects of risk governance relevant for this case:
available factual knowledge about risks, the design
ing of effective risk management strategies, and
how dispersed responsibilities were dealt with.

A recognized lack of scientific knowledge
existed prior to this volcanic eruption: namely, on
the ash concentration levels for safe flying. We have
argued that in a wider decision-making perspec
tive, the available knowledge and related uncer
tainties should be seen in relation to the actual risk
management strategies implemented at that time.

In the period prior to the Eyjafjallajökull erup

tion, a strict cautionary/precautionary approach

was maintained as a strategy to handle the uncertainties/risks. When new knowledge became available during the volcanic eruption, the policies were revised to allow aircraft operations under specific, well-defined conditions. We argue that there was a deficit of risk governance in the dealing with dispersed responsibilities in the time period prior to the volcanic eruption. This became apparent in the first period of the 2010 volcano eruption, when national authorities were paralysed, i.e. unable to respond effectively because it could lead to diversion from the internationally established guidelines that recommended avoiding all flying in airspace potentially contaminated with volcanic ash. During the eight days of the first intense phase of the eruption, the European Commission took an initiative to coordinate the national authorities' response to the crisis, resulting in a new set of harmonized and differentiated guidelines for risk assessment and risk management. The first priority of civil aviation policy is to ensure safety. Going back to the first reported encounter in 1982, no fatal accidents have been registered from flying in airspace contaminated with volcanic ash. This could be seen as a testimony of the authorities' successful handling of the specific risks for civil aviation during the 2010 Icelandic volcano ash cloud, and for the handling of historical volcanic ash cloud incidents in general. However, there have been several close calls, and the international civil aviation community still has several major issues to resolve in order to further improve the response of future volcanic ash cloud incidents. Nevertheless, the overall conclusion of our evaluation remains that the actual risk governance (management) in this case was, to a large extent, in compliance with the defined principles and criteria, and few severe deficits were identified. We cannot see that the massive level of criticism directed at the authorities was justified.

Regulatory response to hazards. Case studies from the Norwegian

petroleum industry

P.H. Lindøe, O.A. Engen & Anita Moen

Faculty of Social Science, University of Stavanger, Norway

ABSTRACT

For some years new principles of risk regulation has been introduced as alternatives to detailed prescriptive regulations. Enforced self-regulation, where part of the regulatory process is delegated to the industry was introduced in the 1980s. This regulatory regime implies a process of negotia tion and interpretation among the regulator and regulated regarding risk assessment, norms and safety practice. The purpose of this paper is to give a better understanding of what factors that may influence the outcomes of this process. An ana lytical framework including risk images and haz ardous identification, arenas of negotiations and discursive practice is introduced. This framework is tested against three case studies (1) Hazardous workload, (2) Chemical Hazards and (3) Techni cal assessment of platform. The findings from the three cases are summed up in figure below.

The cases illustrate how diverse risk problems require different solutions, procedures and implies different amount of stakeholder involvement.

The more complexity and ambiguity, the more involvement is seemingly required to manage risks. Ordinary and traditional risk problems are usually best handled using an instrumental discourse among agency staff, directly affected organization and enforcement personnel. When

uncertainty and complexity increases and disputes about values or consequences arise, a discursive practice concerning risk is required. The model promotes “discursive aspects” of risk regulation. A discursive practice concerning risk may confront sloppy and ignorant attitudes at local levels and challenge the actors’ attitude towards responsibility. Trust and legitimacy is embedded in the organizational structure and in the relationship that characterizes by the affected agents. Decision making is a result of negotiation, and new regulations are prepared and implemented according to consensus between the regulators, organizations and stakeholders. The organizations’ reactions to the decision making processes depend on whether the choices meet the institutional identity. All involved actors will try to have influence on priorities, and the decisions are judged according to whether they are recognized as rational, effective Hazardous work-loads Chemicals hazards Acknowledgement of compliance

Socio-economic

factors Minor groups of workers with low status. Industry argues on that high cost and disputable benefit Minor group of workers belonging to low status service providers. Limited cost of improvement. Regulatory issue to be solved by coordination of actor with unlike power basis

Risk images

and hazard

identification Working hours offshore go far beyond reasonable and safe limits. Lack of research Assessment of exposure hampered by lack of information, measurement and long term effect of health problems Assessment according to well defined technical standards

Discursive

practices Controversies between industry and regulator concerning cost and benefits. Unlike alliances between unions, research communities and regulators. A process of muddellingthrough and continuous discussion between regulators, unions and industry. Several arenas for co-operation and discussion between governmental and industry actors across national borders

Outcomes Unsolved dispute. Possible solution is more prescriptive rules and reduced flexibility in the regime.

Hazards has gradually been reduced by a combination of enforced regulation, technical design and effort among the stakeholders Pragmatic solution where AoC represents an exception from the main principles of the offshore regime.

and fair. However, this form of regulative practice,

accounting for social and cultural values when

designing and implementing new routines and pro

cedures, may lead to less responsibility aversion by

the actors involved. Accordingly, rules and proce

dures with local involvement gain greater legiti

macy among the participants but also demand a higher willingness to take responsibility for the working conditions. The article proposes a process of regulatory practice to a larger extend is adjusted to the character of the risk and hazard of the working conditions.

The effect of the Deepwater Horizon accident on the Norwegian debate

concerning future oil and gas development in Lofoten and Vesterålen

I.L. Johansen

Department of Production and Quality Engineering, Norwegian University of Science and Technology,

Trondheim, Norway

ABSTRACT

In April 2010, the blowout of the oil rig Deepwater

Horizon in the Gulf of Mexico caused the loss of

11 lives and the largest quantity of oil spill ever

experienced. The objective of this paper is to

address how the accident has affected the ongo

ing debate concerning whether to open up for oil

and gas development in the vulnerable areas of Lofoten and Vesterålen (LoVe) in the North of Norway, and the implications for risk assessment to inform the decision process.

For almost ten years, the debate on LoVe has engaged a wide range of stakeholders from minis tries and oil companies to environmental groups. The Deepwater Horizon accident has made visible the opposing stakeholders, who have used the event to argue against development and the adequacy of risk assessment to inform decision making. Proponents, on the other hand, have accentuated the differences which limit its relevancy to North Norwegian conditions. Those who have wavered inbetween have generally maintained their ambiva lence in quest for more knowledge. The perceived relevancy of Deep-water Horizon to LoVe is thus shown to correlate with the stakeholders' funda mental reasons of interest in the decision, which can be intuitively arranged on a value spectrum from environmental preservation to value crea tion as shown in Figure 1. A clear connection is indicated between stakeholder values and the con ception of risk; while the opposition emphasizes consequences, proponents accentuate probability,

and the political midst highlights uncertainty.

Even though the Deepwater Horizon accident

has served to confirm rather than alter the prior

positions, it has definitely affected the arguments,

momentum, and dynamics of the debate. Through

the mechanisms of social amplification of risk, an

information gulf has arisen as stakeholders use

values as pervading benchmarks for selecting and

interpreting risk information to strengthen their

positions. Ultimately, this has brought the parties

farther way from a shared understanding of both the quality and quantity of major accident risk in LoVe. The Deepwater Horizon accident has also seemed to alter the views on what makes a suitable strategy to risk evaluation and the role of risk assessment in the decision process. Apparently, the accident has masked what this author considers to be the two defining challenges of the situation; complexity and ambiguity. Instead, the debate has been reframed as a problem of uncertainty, at the risk of reducing value conflicts to a mere factual level of risk debate while leaving analytical disagreements still unresolved. The study concludes that the Deepwater Horizon accident has jeopardized the extent to which risk assessment is to be accepted as decision support, by increasing skepticism, pragmatism, and the gulf of knowledge and understanding. In order to regain analytical integrity in a debate which is necessarily politically laden, this calls for explicit attention to problem framing and establishment of scientific conventions through broad deliberation prior to risk assessment. Value creation Environment Relevance of Deepwater horizon Environmental groups Leftwing parties Right wing parties Oil companies and directorates Low High The government, detached experts and commentators, townspeople Figure 1. Principle drawing of the correlation between values and the perceived relevance of Deepwater Horizon. Risk management This page intentionally left blank

Benchmark study on international functional safety standards

F. Massé

Ineris, Verneuil-en-Halatte, France

R. Tiennot

Ligeron, Saint-Aubin, France

J.P. Signoret

Total, Pau, France

P. Blancart

PSA Peugeot Citroën, La Garenne-Colombes, France

G. Dupin

RATP, Paris, France

L. Marle

IMdR, Gentilly, France

ABSTRACT

The practice in use for the development and the evaluation of safety related systems is to follow the requirements of international functional safety standards. Thus, the quality of these standards and the way they are applied are particularly critical. That is why several partners (Total, PSA, RATP, INERIS) decided to realize a study on this subject in the framework of the IMdR (French Risk Management Institute). This study was realized by Ligeron. The motivations and the main results IMdR Project P08-2 are given in this paper.

In order to develop and evaluate their safety related systems, various industrial sectors have developed their own standards. These standards were defined by taking into account sector-based practices and constraints and without reference to a common state of the art. Consequently, there are strong disparities between the standards and often important inconsistencies with the state of the art in safety and reliability engineering.

Each standard defines its own multiple degree qualification scale like SIL for the IEC 61508, ASIL for the ISO 26262, DAL for DO 178, Category for machines. Each one introduces its specificities and leans on different hypotheses. The Different semantics and definitions are in use and similar terms have different meanings depending of the standard in which they are used. Furthermore the principles, the underlying hypotheses or the simplifications introduced are sometimes ambiguous or scientifically questionable. In front of those difficulties of interpretation and use, it appears necessary to list the standards, make a critical analysis and compare them in order to identify the convergences, the main differences and the possible weaknesses. The following issues have been studied: Identification of existing safety standards Feedback on standards application Standards comparison and critical review Vocabulary status The results of the identification and analyze of functional safety standards of main industrial sectors provided: A vocabulary comparison and analysis The qualification criteria The conditions for standards applicability The benefits and limitations of each standard The relevance of each standard with regards on technologies and operation

philosophy. In this paper, the safety lifecycles and the main requirements of the IEC 61508 and three standards derived from IEC 61508 are presented. Then, a few vocabularies issues are summarized. Finally, the main qualities and weaknesses of these standards are discussed.

Brissaud, F., Barros, A., Bérenguer, C. & Charpentier, D.

2010. Design of complex safety-related systems in

accordance with IEC 61508 In: R. Bris, C. Guedes

Soares, S. Martorell (eds), Reliability, risk and safety:

theory and applications, proc of the European Safety

and Reliability Conference, Prague, 7-10 September

2009.

Gentile, M. & Summers, A.E. 2008. Cookbook versus

performance SIS practices. Process Safety Progress,

27: 260-264. IMdR Project P08-2, 2011. Benchmark study on safety instrumented systems safety approaches. Langeron, Y., Barros, A., Grall, A. & Bérenguer, C. 2008. Combination of safety integrity levels (SILs): a study of IEC61508 merging rules, J Loss Prevent Process Ind 21, pp. 437-449. Lundteigen, M.A. & Rausand, M. 2010. Reliability of safety instrumented systems: Where to direct future research?. Process Safety Progress, 29: 372-379.

Correlating risk and innovation management in projects

F. Marle, M. Jankovic & G. Turré

Ecole Centrale Paris, France

ABSTRACT

Innovation management is inherent to many

projects. Namely, the competitiveness of a com

pany is partially given by its capacity to innovate,

on both its products (services or systems) and on

its internal performance (organization, methods,

process). But constraints are increasing and include more and more dimensions. Today health, society, safety, security, environment should be considered as objectives in addition to the classical cost, time and quality. Finally, increasing project complexity induces new challenges for innovation management.

Innovation may have a direct positive impact, but as well indirect negative or positive impacts which in our opinion are not properly considered today. Moreover, innovation integration timeline is not certain in the project. Most of the times it is planned at the very beginning; but it can also be required during the project because of the occur rence of an undesired event, like a change in the laws context, or a change in the budget or a change in the customer requirements. This means that already identified risks have to be updated due to this change.

In the first place, this paper aims at identifying the portion of the project which contains innova tion (distinguishing the desired innovation and the novelty or change of a parameter). Secondly, it aims at anticipating the potential propagation of innovation to the rest of the project in order to

analyze related risks, including positive and nega

tive ones.

The methodology consists of four steps. Firstly,

we propose to identify the novelty degree and the

link with innovation, if it is a desired innovation or

an obligation (not flexible constraint) or a novelty

(a new version/a change in a parameter). As uncer

tainty is inherent to innovation, the expected

direct benefit may be balanced by indirect negative

Drilling consortia—new ways of organising exploration drilling

in the oil and gas industry and the consequences for safety

L. Hansson & G.M. Lamvik

SINTEF, Trondheim, Norway

S. Antonsen

NTNU Social Research, Trondheim, Norway

ABSTRACT

Drilling for oil and gas is a high risk activity. This

has recently been illustrated by the Deepwater

Horizon disaster, which caused the deaths of 11

people as well as the worst environmental disaster

ever to occur in the Gulf of Mexico. Traditionally,

the exploration drilling activities in the oil and gas

industry have been carried out by a single operator

and a drilling contractor. The drilling rig is usually

owned by this contractor and the drilling opera

tions are done according to the specifications and

requirements from the oil company.

Recently, a new model for organizing explo

ration drilling has emerged, especially on the

Norwegian Continental Shelf. Smaller oil compa

nies are now joining forces by creating a temporary

organisation called drilling consortia. Several oil

companies contract a drilling rig while outsourc

ing several planning and operational functions to a

well management company. In this way, the drilling

activities are becoming more and more organized

as networks than traditional hierarchical organiza

tion models. This is an organization form which is

rarely addressed in the literature on safety man

agement, which usually presupposes that risky

activities can be governed within the boundaries of single organizations (e.g., Petersen 1978). How safety is to be managed in more transient organization forms is thus a largely unanswered question in safety research. This paper presents the preliminary results of a study of the safety consequences for this way of organising exploration drilling. It is based on a study where two minor oil companies and two well management companies are involved in a project funded partly by the Norwegian research council. One of the study's focus areas is the split between the HSE responsibility and the execution of the HSE related activities. We find that this split involves both strengths and challenges with regards to safety. One possible challenge is found in an increased need for coordination when such a large number of separate companies are to cooperate in high risk activities. On the positive side, and somewhat counterintuitive, we found that the new model can actually lead to greater continuity

in the execution of many HSE-related activities. REFERENCE
Petersen, D. (1978). Techniques of safety management, New York, McGraw-Hill.

Effectively mitigating and managing the risk to public assets

D. Prochazkova

Institute of Security Technologies and Engineering, Faculty of Transport Sciences,

Czech Technical University, Praha, Czech Republic

ABSTRACT

The paper presents the overview of results of systematic research of negotiation with disasters in the Czech Republic that was realised in the frame of four national projects in 2004-2008. The research itself was based on basic data sets on disasters from last millennium and it was performed by 17 high educated experts, 23 technical workers and by 11 PhD students with use more than 5000 professional sources and 12 special investigations; all sources are given in original research documents (Prochazkova, 2006, 2007 a, b, 2008). The territory including the human society is considered as the human system with assets: human lives and health; property and public welfare; environment; infrastructures and technologies; mainly the critical ones. The all human aim is to ensure the safe territory and the leading role belongs to public

administration that is responsible for risk govern
ance in the territory. Because the risk management
is very challenging to knowledge, experiences, data,
data processing method, quality of result interpre
tation, decision-making and of implementation
capability, there is necessary to separate tasks for
strategic, proactive territory safety management
between research institutes and public administra
tion itself. The integral territory safety manage
ment is new task for public administration, and
therefore, it needs correct tools and they have been
prepared under the research mentioned above.
Principles used coincide with those in (EMA, 1996,
FEMA, 1997, etc.).
The paper summarizes results obtained from
representative data sets from the mathematical
statistics viewpoint, i.e.: list of disaster types that
might be considered at application of the All
Hazard Approach (FEMA, 1996); basic terms
for discipline which deals with integral territory
safety; concept of tool for public administration
that ensures its capability to separate expected dis
asters into categories (relevant, specific, critical)
and to apply correctly and effectively preventive,
mitigation, response and renovation measures and

activities; set of 12 methods that help to public

administration correctly and effectively to fulfil

its responsibilities connected with territory risk

Prochazkova, D. 2007c. Metodology for Estimation of

Costs for Property Renovation in Territories Affected

by Disasters. Ostrava: SPBI SPEKTRUM, ISBN 978

80-86634-98-2, p. 251. Prochazkova, D. 2008. Professional Reports to Project MZe 1R56002 “AuxiliaryMulti Criteria System for Decision-Making Supporting the Sustainable Development of Landscape and Settlemens” (in Czech). Praha: Ministry of Agriculture, p. 1020.

Empowered agents or empowered agencies? Assessing the risk

regulatory regimes in the Norwegian and US offshore

oil and gas industry

P.H. Lindøe

University of Stavanger, Norway

M. Baram

University of Boston, MA, US

G.S. Braut

Norwegian Board of Health Supervision, Norway

ABSTRACT

This paper deals with the contrasting regula

tory approaches taken by Norway and the US

towards the prevention of major accidents in the

exploitation of offshore oil and gas resources.

Our purpose is to assess the two regimes as mod

els or prototypes of different control paradigms

which define the relationship between the regula
tor and the regulated. In one model, companies
serve as the instruments of risk control and are
empowered agents exercising “internal control”
(self-regulation). In the other model, agencies are
the empowered agents and control risk by impos
ing external controls (detailed prescriptive require
ments) on companies.

In the 1970’s and 80’s, major accidents at drill
ing platforms on the Norwegian continental shelf
(Bravo 1977, Alexander Kielland 1980) and the
UK shelf (Piper Alpha 1988) led the Norwegian
government to replace its prescriptive regula
tion of offshore safety with a system of enforced
self-regulation. As a result, Norwegian regulators
established broad functional requirements in the
form of performance-based rules, and transferred
responsibilities for implementation to companies.

In contrast, the US regulatory approach has
remained essentially unchanged with a prescriptive
regime. It involves technically-detailed regulatory
programs, adoption of industrial standards and
practices when these are available, inspecting com
pany activities, and penalizing companies found to
violate the regulations. The US approach, which has been
applied to drilling in the Gulf of Mexico (GOM) and other

parts of the US continental shelf, involves several federal agencies which are directed by law to carry out a prescriptive program. Another feature is that companies are subject to significant liability of two types: liability to government for oil spill clean-up costs and damages to resources, and liability to individuals and private entities for negligentlycaused damage to private property and personal injury. However, the BP Deepwater Horizon disaster in 2010 is causing a major re-evaluation of the regulatory regime. Multiple sources of information provide the empirical basis for the analysis. First, a portfolio of research projects on the Norwegian and US approaches related to technological change, safety management and regulation. Secondly, we have assessed legal documentation from both countries, and thirdly, we have reviewed the rapidly increasing body of documentation and reports following the BP Deepwater Horizon disaster. The two regimes are assessed and compared by using an analytical framework with five dimensions; basic regulatory approach, goal setting and measurability, stakeholder participation, learning processes, and how the control dilemma is being addressed. Finally, the strengths and weaknesses of the different approaches and the interchangeability of elements in the two regulatory systems are discussed.

Experience from chemical industry for controlling patient safety

C. van Gulijk & B.J.M. Ale

Technical University Delft, Safety Science, Delft, The Netherlands

D. Dongelmans & M. Vroom

Academic Medical Centre of Amsterdam, Amsterdam, The Netherlands

ABSTRACT

Controlling medical errors is just as difficult as

controlling any other error. Unfortunately, these

errors can lead to deadly victims all too easy. It was

estimated that the number of unintended deaths

in hospitals in the Netherlands may be anywhere

between 1700 and 6000 on a yearly basis on a pop
ulation of 16 million people (Wagner & de Bruijne
2007). Ever since that information became public
in 2007, hospitals in the Netherlands are urged
to design systems that can reduce the number of
victims. A safety management system is obligatory
since the beginning of 2010.

Hospitals have limited experience with complex
safety management systems, so they turned to an
industry with an abundant experience. A report by
a former director of Shell shared the experience
in the petrochemical industry to Dutch hospitals
(Willems, 2004). However, the rigid technical
approach was difficult to handle by the medical
and nursing staff. The experience from chemi
cal industry had to be adapted before it could be
applied in hospitals. Therefore, the aim of this
work was to design and test a safety management
system based on experiences from chemical indus
try that fits into the normal way of working in the
hospital. The development of that system was per
formed for the Intensive Care department at the
Amsterdam Medical Center

Prior to the design and implementation of
the safety management system the intensive care

department was analyzed and an ethnographic

study took place. These analyses resulted in impor

tant implications for the design of the safety man

agement system for patient safety. The implications

were incorporated into the safety management sys

tem proposed by Willems (2004) so that it could be

used in the hospital.

An important part of the analysis were interviews

with the staff to assess their opinion about patient

safety. The investigation shows that they perceive

their own efforts and the efforts within their imme

diate working environment as the most important

Integrated safety management based on organizational resilience

T.O. Grøtan

Norwegian University of Science and Technology (NTNU), Department of Production and Quality Engineering, Trondheim, Norway

SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

F. Størseth

SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

ABSTRACT

Resilience (Engineering) is about to become

a significant part of safety thinking and practice.

Although not fully developed and mature, increas

ing evidence of its relevance raises a forthcoming challenge, namely how to combine resilience with other (traditional) safety approaches into a coher ent sociotechnical and organizational scheme of protection. The prime issue of this paper is how measures of resilience (engineering) can be added to the existing portfolio of principles and prac tices of safety management. Resilience is not just advances in applied methodology, but another approach based on different assumptions (e.g., on normal variability) and a radically different system model. Hence, the integration of resilience into the safety management portfolio will have implications for existing principles.

A complexity perspective, related to social emer gence (Sawyer, 2005) acknowledging that complexity is (also) endogenous to the practice of any risk/safety management, is employed to explore how the “new” emerging safety through resilience and the “old” resultant safety through compliancerelate to each other. Moreover, resilience as a theme reinforces with urgency an already pressing, but rather unat tended distinction between a) the abilities/properties that we want the systems to comply with (e.g., “the ability to anticipate”), and b) the situated MTO

(Man-Technology-Organization) measures that have to be employed in order to accomplish these objectives in a composite organizational context. The notion of Organizational Resilience (OR) signifies the full MTO premise of its implementa tion, and the organizational intent of its achieve ments. Incorporating a full MTO perspective ultimately demands that safety management is willing to look behind the organizational facades (e.g., questioning unified actors, homogeneous environments and long lines of uninterrupted action), relax its traditional stronghold on a “real ist” position stemming from a distinct focus on

Principles for setting risk acceptance criteria for safety critical activities

E. Vanem

Department of Mathematics, University of Oslo, Norway

ABSTRACT

Nearly all activities in life involve risk in some way or another, and there is no universally agreed crite ria for what levels of risk are acceptable. Identified and unidentified risks are always sought to be con trolled and minimized. The most commonly used strategy for managing risk in the public interest is through legislation and regulation, although eve

ryone is constantly voluntarily managing personal risk in daily life on an individual level, both consciously as well as unconsciously.

Risk reduction will come at a price and there will be a trade-off between the level of risk one accepts and the cost one is willing to spend to mitigate it. For decision-makers responsible for public safety, at the expense of the public wealth, this trade-off needs to be considered carefully and thoroughly. The overall objective is to best allocate the society's scarce resources for risk reduction, by supporting the implementation of efficient risk reduction measures and to avoid wasting efforts on inefficient ones.

Risks introduced to the society from a given activity may be of different types. Fatality risks or health risks are the risk of depriving members of the community of their lives or their good health. Other types are property risk, economic risk and environmental risks. When decisions about safety are made, all risks should be considered, and appropriate acceptance criteria for fatality, health, environmental, economic and property risks should all be met before an activity can be declared safe enough. However, this paper focuses

on safety risk.

Safety is surely an important objective in soci

ety, but it is not the only one and allocation of resources on safety must be balanced with that of other societal needs. In the literature, different fundamental principles for appropriate risk acceptance criteria have been proposed and extensive research is continuously going on; new principles for establishing and evaluating criteria are continually being introduced. Having adopted a set of fundamental principles to govern the establishment of risk acceptance criteria, specific risk acceptance criteria can be formulated. In the full paper, some important principles for establishing risk acceptance criteria are presented and discussed. At first sight, some of these may seem exclusive but it will be demonstrated how the different principles can be employed to complement each other in one and the same regulatory regime. Brief considerations on the ethical foundations of the various principles will also be given. Some examples will be given from the maritime industries, but the principles and discussions are believed be general enough to apply to all areas of technical risk. Some of the principles that will be discussed in the full paper are – Absolute risk criteria – The ALARP principle – The principle of equivalency – The utilitarian principle of maximum benefit to all – No mandatory risk reduction measures – The accountability principle – The holistic principle – The precautionary principle – The principle of parsimony.

Quality aspects in planning of maintenance and modification

on offshore oil and gas installations

S. Sarshar, A.B. Skjerve & G. Rindahl

Institute for Energy Technology (IFE), Halden, Norway

T. Sand & B. Hermansen

Den Norske Veritas (DNV), Høvik, Norway

ABSTRACT

The process of planning maintenance and modifi

cations activities on offshore installations is com

plex. The planning process is traditionally carried

out in sequences by different departments in the organization, depending on the time frame and level of granularity of the plan: from 5-year plans to daily plans. It involves highly skilled persons representing different professions, which are located at different physical sites (onshore/offshore). Planning is performed using various software tools such as SAP, SAFRAN or Microsoft Project.

People involved in the planning process are under constant pressure for ensuring that the plans will have a minimum negative impact on production, i.e., in terms of time, cost and resource constraints. The specific attributes that characterize a high quality plan are, however, not readily defined. The robustness of plans, i.e. the inherent ability to keep as much as possible of the original structure as time moves forward, is furthermore, considered as a key concern. The reason is that robustness will reduce the amount of re-planning between each level of planning and it will enable more accurate cost estimates and better basis for material/logistics planning earlier on in the process.

This paper explores aspects in planning of maintenance and modifications of offshore oil and gas installations: What are the characteristics or aspects

of a high quality plan?

To answer this question, insights are needed

about how plans are developed. This paper

describes how the different planning levels from

annual plans down to work preparations for activi

ties to be undertaken the following day are handled.

Risk assessment is performed in each of the plan

ning phases, but with different means and purposes.

It is of high importance that risk detected in early

phases of the planning are communicated through

each step of the planning activity to maintain

a high level of safety. The personnel involved,

Reducing the risks faced by small businesses: The lifecycle concept

S. Clusel

AFNOR Group / Crisis and Risk Research Centre, Mines Paris-Tech, La Plaine Saint Denis, France

F. Guarnieri

Crisis and Risk Research Centre, Mines Paris-Tech, Sophia-Antipolis, France

C. Martin

ESAIP / Crisis and Risk Research Centre, Mines Paris-Tech, Grasse, France

D. Lagarde

AFNOR Group—Marketing and Innovation Department, La Plaine Saint Denis, France

ABSTRACT

In France, more than 99% of failed businesses are Small or Medium-sized Enterprises (SMEs) (Altares, 2010).

Failure is considered here in practical terms as a state of insolvency, i.e., the company is unable to meet its liabilities from its available assets. This final and extreme demonstration of the difficulties that a company can experience (De la Bruslerie, 2006) is the result of deeper causes, which are for the most part predictable, and for which the most frequently cited problems are financial and mana gerial, related to demand and/or a crisis within the organization.

One of the solutions classically envisaged is glo bal risk management that allows analysis of the major risks for the business (loss of a significant debtor, significant increase in production costs, loss of a key worker etc.) using a methodical, sys tematic and iterative process. The idea is attractive, however, the implementation of such approaches within SMEs, and specifically within micro— and small businesses (defined by EU regulation 2003/361/EC as having less than 10 or 50 employ ees respectively) is far from obvious. In fact, on the one hand there is a little interest in the implemen

tation of such procedures from business owners,

who look at the ratio of the time and complexity

of implementation with respect to the relevance of

the results for strategic orientation of the organi

zation, and on the other hand, the inadequacy of

tools which are really only ‘lite’ versions of systems

under the control of big business.

The aim of this current work is to rethink cur

rent commercial approaches which do not take

into account the metamorphosis of the SME

and its changing needs at different stages of its

Risk assessment method for shopping centres

S. Nenonen

Tampere University of Technology, Department of Industrial Management,

Center for Safety Management and Engineering, Tampere, Finland

K. Tytykoski

Inspecta Tarkastus Oy, Tampere, Finland

ABSTRACT

The unique features of shopping centres (e.g., large

numbers of visitors and design of premises) cre

ate specific risks for the management of safety and

security (European Agency for Safety and Health

at Work, 2011). Shopping centre hazards, if real

ized, may endanger the safety of both visitors and

people working and doing business in shopping centres (Finnish Council of Shopping Centres, 2005). Therefore, the management of safety needs to cover both the customers who visit the shopping centres and the personnel working in the premises. However, even though the prevention of safety and security risks plays a critical role in shopping centres, safety and security issues have not received much attention in scientific literature to date. This paper discusses risk assessment in shop ping centres and presents an assessment method developed particularly for shopping centres. The aim was to construct a comprehensive risk assess ment method on shopping centre safety and secu rity by considering significant factors regarding shopping centre property and premises, as well as the activities of those working and doing busi ness in the premises. The development of the risk assessment method was started by reviewing the special features of safety and security in shopping centres by a literature review, interviews directed to the personnel of two Finnish shopping centres and a questionnaire carried out among a group of Finnish shopping centre operators. Based on the gathered information, a new shopping centre spe

cific risk assessment method was compiled.

According to the results of the interviews and the questionnaire, shopping centres are perceived as safe and serious incidents seem to be rare. The main risk that was brought out related to undesir able behaviour of visitors. Other potential risk fac tors were considered to relate, if poorly managed,

Security risk management in Norwegian aviation meets nordic traditions of risk management

O.A. Engen

University of Stavanger, Norway

ABSTRACT

Both the aviation sector and the petroleum sector are technologically based organisational systems and both aspire to be associated with best practises of high reliability. Traditionally the safety regime on the Norwegian Continental Shelf has been developed and governed by a sophisticated body of laws and regulations coined as the “Nordic model” of Occupational Health and Safety and based on a three-part pillar with the regulator, the employer and the employees/unions as legitimate. It is rea sonable to claim that the Nordic Model and the safety system that has developed in the Norwegian oil industry are closely connected. The traditional

Norwegian safety system is found in the system oriented approach where socio-technical design and organizational factors adjusted to how humans act are seen as the dominant factors.

The terrorist attacks that took place September 9/11, 2001, demonstrated that the security system, comprising legislation, regulation, and implemen tation were not adequate to handle an intentional event of this magnitude. The 9/11 attacks caused a major reshuffling in the regulatory system and made it mandatory for all member countries.

The convention formed the basis for EU's new frame regulation 2320/2002 which evolved into a detailed, deterministic system The risk manage ment systems in the Norwegian aviation sector in the aftermath of 9/11 have system that aimed at securing civil aviation through a detailed and uniform system for all of the European countries.

From the more goal-based way of regulating, the new security regime essentially followed a 'pre scriptive' regulatory approach which is based upon mandated compliance.

This paper discusses how the security regime in aviation deviates from traditional "Nordic" practises of technological risk management in the

petroleum sector. The paper highlights differences

and similarities between the two systems and ques

tions whether local participation and stakeholder

involvement are necessary prerequisites for suc

cessful safety/security management.

The safety regimes in aviation and the Norwegian

The collective risk, the individual risk and their dependence on exposition time

J. Braband

Siemens AG, Braunschweig, Germany

H. Schäbe

TÜV Rheinland, Köln, Germany

ABSTRACT

he exposition of an individual or a group of per

sons to a hazard is important, when a risk analysis

is carried out to derive a safety integrity level. The

same holds true, when the achieved risk of a system

is computed, e.g., for a safety case. The exposition

time is mentioned in several standards when the

safety integrity level is derived. There, the exposi

tion is used as a parameter, e.g., in IEC 61508 as

“exposure in the hazardous zone”. Risks are some

times given per calendar year, sometimes per hour

of use. In other cases, risk is presented per person

kilometers for a traffic system. The values of risk

might differ, depending on the time unit which is used for indication of the risk. In section two, we give an introduction and show, which standards use hazard exposition as a parameter.

In section three, we describe collective risk, F-N., curves and individual risk and their interrela tionship. We show, which important role is played here by exposure time of an individual and cumu lated exposure of a group of persons when relating individual and collective risks to each other.

In the fourth section, we provide application examples. Different sources provide different risk values with different time units and, consequently, different absolute values. We discuss examples, where the risk figure is so vague, that it becomes useless, because exposition to the hazard is com pletely undefined.

We show that a risk is presented best for a gen eral unit of exposition time, e.g., per hour. This holds true, if exposition time cannot be neglected as e.g., for Bungee jumping. If risk is given per cal endar time, the assumptions about exposition need to be considered in the form of exposition time per event and the number of events or the cumulative exposition time in order to avoid misunderstand

ing. When talking about transport systems, also

the risk per unit of transport capacity, i.e., person

kilometer. This makes sense for collective risks.

If exposition time is incorrectly taken into account,

one might easily have differences of one order of

Development of a safety management system for Small and Medium

Enterprises (SME’s)

Edgar McGuinness

College of Engineering and Informatics, National University of Ireland Galway (NUIG), Galway, Ireland

Department of Marine Technology, Norwegian University of Science and Technology (NTNU),

Trondheim, Norway

Ingrid B. Utne

Department of Marine Technology, Norwegian University of Science and Technology (NTNU),

Trondheim, Norway

Martina Kelly

College of Engineering and Informatics, National University of Ireland Galway (NUIG), Galway, Ireland

ABSTRACT

It is widely reported in the literature that

employers in the Small and Medium sized Enter

prises (SME’s) sector consider the available safety

management standards to be costly and bureau

cratic, paper-driven exercises, of no materialistic

value to the organization (Duijim et al., 2008). This paper presents a generic guideline for devel opment of a simple Safety Management System (SMS) to be implemented by (SME's). The out lined guideline possesses the strengths covered by existing commercial standards but without their inherent limitations, such as cost, man hours, excessive documentation and record keeping. The generic format of the proposed guideline is based on the simplification and adaptation of available standards, and specifically designed for non-health and safety professionals, working with limited resources. The guideline needs to be introduced in manner that is easily understood, implement able and maintainable, combining simplicity and a strong self-help element. In addition, the SMS guideline aims at keeping financial and manpower costs low while delivering ownership and interest in continuous improvement in to an organization. Since, health and safety legislation has placed the emphasis on risk assessment and risk management (Vassie et al., 2000), the guideline proposes the development of a SMS based on a simple risk assessment. The guideline is divided into three steps, consisting of 1) risk assessment, 2) system

management and 3) performance evaluation. The

elements determined as essential in the construct

of the SME SMS guidance document were

hence divided into each of these steps based on

their influence on safety. An extensive literature

Fernandez-Muñiz, B., Montes-Peón, J.M. & Váz

Quez-Ordás, C.J. (2007a). Safety culture: Analysis of

the causal relationships between its key dimensions.

Journal of Safety Research 38: 627–641. Vassie, L., Tomas, J.M. & Oliver, A. (2000). Health and Safety Management in UK and Spanish SMEs: A Comparative Study. Journal of Safety Research 31:35–43.

Relation between organizational culture styles and safety culture

M.A. Mariscal Saldaña & S. García Herrero

University of Burgos, Spain

A. Toca Otero

Sta. Mª de Garoña Nuclear Power Plant, Spain

J.M. Gutierrez Llorente

University of Cantabria, Spain

ABSTRACT

An analysis of the main accidents that have taken

place throughout history shows that these events

cannot be explained by random equipment failures

alone, but also by a combination of human and

organizational factors. In the nuclear industry,

the IAEA’s International Nuclear Safety Advisory

Group introduced the term of “safety culture” to highlight this fact.

However, Safety Culture (SC) may not capture all the management and organizational factors which are important for the safety of the plant operation.

The key problem with most existing SC models is their lack of integration with general models of organization and organizational culture.

In research studies, no attempt has been made to link safety culture with organizational culture.

Therefore, the objective of this study is to show how to improve the Safety Culture in one NPP act ing on organizational culture styles.

In order to establish this relationship, probabi listic Bayesian Network (BN) models have been used. Data was gathered through a survey in June 2007, in a Spanish NPP (Sta. María de Garoña).

The safety culture questionnaire was based on the five characteristics established by the International Atomic Energy Agency (IAEA).

They are: ‘safety is a clearly recognized value’, ‘accountability for safety is clear’, ‘safety is integrated into all the activities in the organiza tion’, ‘leadership for safety is clear’ and ‘safety is learning driven’.

In order to assess organizational culture,

the Organizational Culture Inventory (OCI)

was used. The OCI questionnaire focuses on

the behavioral norms and expectations associ

ated with the values shared by members within

an organization. The OCI proposes 12 types of

organizational cultures. The constructive types are

Risk perception in health care—A study of differences across

organizational interfaces

S. Wiig

Department of Health Studies, University of Stavanger,
Stavanger, Norway

ABSTRACT

This paper examines risk perception among

officials and employees across organizational

interfaces within the health care system as a risk

regulation regime. Officials and employees at

different levels of a given regime may perceive risk

differently (Hood et al., 1999; 2001; Rothstein,

2003), developing divergent attitudes towards the

regulation and demands for risk management

(Kewell, 2006). This paper focuses on institu

tional and instrumental aspects of risk regulation

regimes—namely, the context (type of risk, public

backdrop of regulation—as well as the content

(size, structure, style) involving the objectives

and styles of regulation. The paper explores how these institutional and instrumental aspects shape risk perception among officials and employees across organizational interfaces in the Norwegian specialized health care system. The research question is:

How do contextual and content elements of risk regulation regimes shape risk perception among officials and employees across organizational interfaces in health care?

The study design is an embedded single case study approach covering the specialized health care. Data were collected using a triangulation of qualitative and quantitative methods such as interviews, document analyses, observations, and statistical analyses (Patton, 1999). A total of forty nine tape-recorded interviews were conducted using structured interview guides. Furthermore, a total of 894 written error reports from two hospital divisions were registered and analyzed using an Excel database. Document analyses have been conducted of healthcare legislation, Norwegian White Papers, guidelines and policy documents, inspection reports, and annual reports.

The results showed that risk perception varied

according to officials' and employees' location

within the regime (national or local regulator

or within the hospital hierarchy), responsibility,

profession, and personal experience with

medical errors (Tamuz et al., 2004; Kaplan et al.,

Safety theoretical issues: Scientific please, but keep it brief

Fred Størseth

SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

Tor Olav Grøtan

SINTEF Technology and Society, Department for Safety Research, Trondheim, Norway

Norwegian University of Science and Technology, Department of Production and Quality Engineering,

Trondheim, Norway

ABSTRACT

The current paper seeks to address formal

theoretical issues in contemporary safety research.

Pursuing the thesis that theory is method, the

paper advocates the value of taking the theoretical

'long road'; that is, staying wary for, and actively

trying to match ones theoretical effort against

formal theoretical principles. This does not imply

that 'a' theory-method is suggested. Rather,

it reflects acknowledgement of working with ideas,

the conception that any shortcut in these respects

is an actual short-cutting of reasoning and theo
retical development.

The paper starts by positioning ‘science’
and ‘theory’, within the context of our area of
research interest (i.e., organizational resilience).
By reference to concepts like complexity and emer
gence, resilience can be said to challenge traditional
assumptions of correlation, causation, “laws”, and
system regularities. In a way, resilience challenges
the very rationality of enforcing rule and procedure
compliance in the name of safety. Thus, what we
need is a notion of science and theory that is not
trapped in a notion of ‘science as common sense’.
Inspired by Alvesson and Sköldberg (e.g., 1994),
we emphasize the need to go beyond chasing
ever-increasing exactness of methods to crystallize
‘definitive’ terms and variables; and that (our)
research need to stay sensitive of new (emerging)
relations, perspectives, and world views.

The following set of principles is suggested as
a kind of formal theoretical navigation points
for consideration along the long road: Concept
elaboration, conjecture beyond description,
traceability, and association specification.

It is however well recognized that the long

road is an ideal case, and that today's research practice often is forced or willingly attuned with quick business. Thus, the paper raises issues related to what may be serious obstacles to the ideal long road, e.g., illusions, double edged swords (and standards, e.g., scientific, yes please; but keep

The challenge of system change in aviation: The Masca project

M.C. Leva, N. McDonald & S. Corrigan

Aerospace Psychology Research Group—School of Psychology
Trinity College Dublin, Ireland

P. Ulfvengren

KTH Industriell Teknik Och Management, Stockholm, Sweden

ABSTRACT

The main object of MASCA is to develop and deliver a structure to manage the acquisition and retention of skills and knowledge concerning organisational processes for managing change in the 'whole air transport system'. Different stake holders in a common operational system (airlines, airports, maintenance companies, etc.) joined together in the project to change the shared opera tional system to deliver a better service. An Origi nal Equipment Manufacturer (OEM) and software designer will offer technology solutions which sup port a more effective integrated operation. The

participating companies will develop and maintain new skills and knowledge in change management. MASCA will develop the ‘concepts and techniques’ which can develop, manage, and support the effec tive deployment of these skills and knowledge in the management of change.

The workprogramme takes an action research approach with a primary focus on the transfer of change management capability into the organi sations that are responsible for and involved in change. Thus the workprogramme is organised around two complementary objectives:

- The development of a system to support the development and deployment of an inte grated change management capability (Change Management System—CMS).
- The deployment and evaluation of the CMS in selected change management initiatives, both simulated and actual. Transformation or change of the social system within Masca is seen not just in terms of the ways in which the system “affords” (enables, encourages, directs, mandates) appropriate actions and interactions from its members, but even more, how to influence the common understanding of how the system works, taking into account the background of accumulated collective experience that has formed that cultural expression. It is in fact believed that organizational culture is as much about how things work in the organizational system—“why we do things this way around here” as it is about a simple aggregation of meanings and activities “the way we do things around here” (Deal and

Kennedy 1982). This approach has already influenced the tools and methods used to determine the target case studies for change within the end user organizations. The MASCA consortium covers the range and balance of partners to address the ‘whole air transport system’—an airline includes flight, maintenance and ground operations companies; an airport authority; an original equipment manufacturer— world leader in aircraft technologies; two universities; an aeronautics research organisation, and an SME with a strong profile in technology and human factors services to aviation REFERENCE Deal, T.E. and Kennedy, A.A. (1982). Corporate Cultures: The Rites and Rituals of Corporate Life, Harmondsworth, Penguin Books.

The impact of safety climate on risk perception on Norwegian and Danish production platforms

H.B. Rasmussen

Centre of Maritime Health and Safety, University of Southern Denmark, Esbjerg, Denmark

J.E. Tharaldsen

Petroleum Safety Authority, Stavanger, Norway

ABSTRACT

The study explores the impact of safety climate on subjective risk perception of personal accidents and process accidents on Norwegian and Danish offshore production platforms.

Due to geographical location and history Denmark and Norway always have been closely connected. The same tendency is seen with cooperation in the oil industry. Both the Danish and Norwegian shelves constitute mature oil producing regions. The common view in the Scandinavian countries is that there is some kind

of a common Scandinavian identity? However, in this study we will look for potential differences. Yet, no comparative safety study on Danish and Norwegian offshore employees has been carried out, but one study in the building and construc tion sector has compared Danish and Swedish construction employees. The study found differ ences in their safety performance, where the Danes were found to be more accident prone than the Swedish workers. One of the explanations was better education of the Swedish employees and cultural differences between Swedes and Danes (Spangenberg et al., 2003).

Danish data consists of a survey sent to employ ees on all productions platform on the Danish sec tor in 2010. The Danish survey was translated from the Norwegian questionnaire used the “Trends in risk level” project being performed every second year by the Norwegian Petroleum Authority. Data from these two surveys were thereafter merged together and a five dimensional solution of safety climate were tested on both populations in SPSS and LISREL. The dimensions Safety management and involvement, System perception and Safety Training for compliance and beyond: Enabling high

performance deliveries in the work permit process

H. von Hirsch Eriksen, S. Mjelstad, O.H. Utvik & Helge Smaamo

Operational Training Centre, Development and Production Norway, Statoil ASA, Norway

ABSTRACT

The paper outlines the activities, goals, and results of the Operational Training Centre (OTC) at Development and Production Norway (DPN) at Statoil. Representing a practitioner perspective we underscored that commentary on our practice are very much welcome.

The OTC trains the company workforce on the Norwegian Continental Shelf with the aim to improve risk governed safety behaviour based on compliance. Typically, the training is conducted on-shore over a period of two days. There are two cornerstones in the structure of any program at OTC. Firstly, the focus is oriented towards the process based management system (APOS). Secondly, a company-wide model of Compliance and Leadership contribute as a guide for both par ticipants and facilitators in the ‘way to work’. This model focuses on process in the sense that it directs how tasks are planned, completed, and evaluated

(Figure 1).

In the design of our programs, several phases of

training are addressed. Preparation of participants

prior to the on-shore training, as well as follow-up

(or extension) activities when the workers return

offshore are important criterions for success.

In this paper our point of departure is related

to the legislative requirements for conducting

offshore operations on the Norwegian Conti

nental Shelf. We note that the legislation rests on

Beams on elastic foundation solved via probabilistic approach

(SBRA Method)

K. Frydrýšek

VŠB—Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

The general problem of the beam on elastic

foundation (Winkler’s theory) is described by ordi

nary differential equation. In the most situations,

the influences of normal force, shear force, distrib

uted moment and temperature can be neglected (or

the beam is not exposed to them). Hence

d v

dx K x EJ v EJ

4

4 + ( ) = b q ,

where K(x)/Nm -3 / is modulus of the foundation

which can be expressed as functions of variable

x/m/, b/m/ is width of the beam, v = v(x)/m is

deflection of the beam and EJ is bending stiffness.

Solved beam (Fig. 1) of length L/m/ with free

ends is exposed to one vertical force F/N/ and dis

tributed loading q is zero. Modulus of the founda

tion is given by K(x) = K 0 + K 1 x.

The approximate solution v = v(x) can be found

in the form of polynomial function of 6th order.

Hence, the approximate results (i.e. functions of

displacement v, slope, bending moment and shear

ing force of the beam) can be derived. This example

is solved via probabilistic approach by Simulation

Based Reliability Assessment (SBRA) Method

(i.e., all inputs are given by bounded histograms,

AntHill software, see Fig. 2) which is the modern

and new trend of the solution in mechanics.

Results parameters (i.e. stiffness of the foun

dation k(x), displacement v(x), maximal bend

ing stress σ MAX , factor of safety F S = R e - σ MAX

Deterioration model for large reinforced concrete structures

M. Sykora & M. Holicky

Czech Technical University in Prague, Klokner Institute,
Prague, Czech Republic

1 INTRODUCTION

Durability is becoming an important issue of structural design. General principles on the probabilistic approach to verification of structural durability are provided in ISO 13823 (2008). Limited experience with the use of the document indicates that additional studies focused primarily on models of material deterioration and acceptance criteria are required. For large surfaces, spatial variability of basic variables needs to be considered. A simplified deterioration model is proposed in the study as an operational alternative to random field techniques.

2 SIMPLIFIED MODEL FOR SPATIAL VARIABILITY OF DETERIORATION AND NUMERICAL EXAMPLE

A large surface exposed to deterioration effects should be analysed as an assembly of elementary surfaces rather than a whole structure. Probabilistic characteristics of the variables influencing the deterioration should then include also the spatial variability of the variables among elementary surfaces. In the present study it is assumed that:

- The basic variables can be divided into spatially variable quantities X loc and quantities attaining a

single value for a whole structure X glob ,

– Basic variables X loc form homogeneous random

fields; in an approximation values of X loc in ele

mentary surfaces are considered as independent,

identically distributed variables.

The failure probability at a whole surface

becomes:

P f (t) = E Xglob {P[n deg (t,X loc |x glob) / N ≥ α lim]} (1)

where n deg (·) = number of elementary surfaces for

which the limit state is exceeded; N = total number

of elementary surfaces; and α lim = limiting dete

rioration level. The number n deg is obtained from

the binomial distribution, which decreases com

putational demands compared to random filed

Development of representative seismic fragility function for bridge

group by using results of safety factor

M.K. Kim, I.-K. Choi & D.G. Hahm

Korea Atomic Energy Research Institute, Daejeon, Republic of Korea

ABSTRACT

The purpose of this study is a development of a

seismic fragility function for railway bridge group

based on the results of previous results of seis

mic safety factor analysis. The results of fragility

evaluation of bridge group which developed in this

study can be applied to HAZUS for the evalua
tion of seismic risk. The safety factor is a result of deterministic safety analysis of each bridge system. The safety factors were determined by numerical analysis about failure criteria.

For the evaluation of seismic fragility function for bridge group, safety factors which developed by previous research were used. The safety factors which used in this study were developed consider ing 54 bridges and eight failure parameters. First, a failure status of structural member was defined according to results of safety factor analysis. The failure status was classified as slight damage, inter mediate damage, extensive damage and complete damage like HAZUS. Each damage status was defined as combination of failure of structural member of bridge system.

Second, a fragility function for each of the bridge members was evaluated according to the damage criteria and failure mode. The failure criteria were considered as failure of column, pier and shoe of bridge system and unseating of bridge. The failure was considered a longitudinal and a transverse

Table 1. Element damage status for determination of seismic fragility evaluation for bridge system.

Damage

Status of

whole system Damage status of bridge member Damage of shoe
Deck collapse Damage of pier

Slight

damage Extensive damage Slight damage Slight damage

moderate

damage Complete damage Moderate damage Moderate damage

Extensive

damage X Extensive damage Extensive damage

Complete

damage X Complete damage Complete damage Figure 1. Fault tree for the evaluation of extensive damage and complete damage. Figure 2. Seismic fragility results of bridge group. 0 0.04 0.08 0.12 0.16 0.2 PGA(g) 0 0.2 0.4 0.6 0.8 1 D a m a g e P r o b a b i l i t y Slight Moderate Extensive Complete

Fatigue loading estimation for road bridges using long term WIM monitoring

M. Treacy & E. Brühwiler

Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland

ABSTRACT

Transport networks form a huge part of a countries assets with the highway system usually the dens est component. As bridges form the keystone of these networks, their safe operation with minimal maintenance closures is paramount for efficient operation. Yearly increases in the volume of heavy

traffic means a higher number of fatigue damaging load cycles in road bridges. With recent improvements in durability of materials and proactive maintenance strategies, fatigue requires increased consideration.

To efficiently manage a large bridge stock, knowledge of individual bridge fatigue safety is required. While whole life monitoring of all bridges offers the best solution theoretically; the sheer number of bridges, manpower, energy and data storage requirements make it unsustainable at present. This work develops a methodology for the estimation of fatigue load cycles and hence fatigue safety in short to medium span bridges for today's highway traffic.

Theure study utilises real traffic streams from Weigh-in-Motion (WIM) monitoring within the Swiss highway network performed continuously over a number of years. The concept of a Stand

Table 1. Statistical information on cleaned traffic data set for Mattstetten A1 motorway WIM station.

WIM station	2007	2008	2009
Zurich direction			
GVW > 3.5 t	1,090,330	1,103,443	1,100,071
Mean GVW (t)	17.0	17.1	17.4

Mean Axle load (t) 4.63 4.62 4.71

Max GVW (t) 97.3 99.0 102

Bern direction

GVW > 3.5 t 1,254,036 1,246,402 1,227,014

Mean GVW (t) 17.0 16.9 17.1

Mean Axle load (t) 4.90 4.81 4.87

Max GVW (t) 98.8 97.9 99.0 Figure 1. Comparison of midspan bending moment cycles over 3 years for a simply supported 25 m span bridge using traffic in Zurich direction at Mattstetten A1 WIM station, Switzerland.

Finite difference modeling of formation damage during underbalanced

drilling in a tight gas reservoir

M. Naseri

Chemical Engineering Department, Sahand University of Technology, Tabriz, Iran

S.R. Shadizadeh

Ahwaz Faculty of Petroleum Engineering, Petroleum University of Technology, Ahwaz, Iran

E. Sahraei

Chemical Engineering Department, Sahand University of Technology, Tabriz, Iran

S.S. Ghorashi

Research Institute of Petroleum Industry (RIPI), Tehran, Iran

ABSTRACT

Evaluating near wellbore formation damage is a

vital factor to deal with tight gas reservoirs due

to their low permeability and porosity, high cap

illary pressure and sub-irreducible water satura
tion. Based on these properties, Counter-Current
Spontaneous Imbibition (COUCSI) damage
occurs during underbalanced drilling in the pres
ence of water-based mud systems. Although there
are some analytical and numerical models describe
COUCSI process, to date, nobody has presented
a numerical or analytical model to investigate the
effect of COUCSI in water invasion during UBD
and its resulting influences on formation damage
and hydrocarbon phase permeability reduction.
This paper presents a numerical model to
determine water saturation profile during under
balanced drilling in a tight gas reservoir which is
mainly because of COUCSI. This model provides
significant value by evaluating water invasion and
the resulting drop in gas permeability, resulting in
a better understanding of formation damage and
its consequent effects. Additionally, understanding
the potential damage resulting from temporarily
overbalanced conditions highlights the importance
of completing the well in an underbalanced mode.
During UBD with a drilling fluid alike wetting
phase for the reservoir rock, the capillary pressure
acts as a counter-current force that leads to flow

of drilling fluid towards the reservoir. The dif

ferential form of the governing equations can be

derived from mass balance and Darcy’s equations

for two-phase flow model. Applying the required

initial and boundary conditions and then solving

it using numerical methods, gives water satura

tion profile. Comparing the new water saturation

values with the initial water saturation, can illus

Laboratory simulation technique of non-stationary random vibration

environment

C. Mao, Y. Jiang, J. Tao & X. Chen

College of Mechatronic Engineering and Automation, National University of Defense Technology,

Changsha, Hunan, China

ABSTRACT

While analyzing the structural dynamic response,

random vibration loads are usually assumed to

obey stationary Gaussian distribution. But tech

nically, in severe occasions, such as strong winds,

storms, earthquakes, tsunamis, explosive blast

waves etc, the random excitations that machin

ery and engineering structures undergo feature

non-stationary. Large-scale machinery, such as

aircrafts, high-speed rail transportations, offshore

platforms, etc, also produce random vibration with

a significant characteristic of non-stationary when their operating environment is unstable or faulty. Besides these, non-stationary random vibration might occur during transporting under unstable conditions, for instance, when vehicle accelerates, decelerates or drives on uneven roads. The dam ages caused by stationary and non-stationary random vibration are different due to their very different characteristics in frequency domain. Currently, the requirements of Environmental Testing and Reliability Testing can’t be met that simulating environment accurately due to lacking of simulation methods and experimental equip ments on non-stationary random vibration. Under the circumstances, some primary research was made in this paper on simulating cyclostationary random vibration environment which is a kind of non-stationary stochastic processes: firstly, the characteristics of Cyclic Mean and the periodic properties of Linear Periodic Time-Varying sys tem were discussed; secondly, a Linear Periodic Time-Varying system was established to generate cyclostationary random signals with specified sta tistical parameters, whose structure was built based on trigonometric function and whose coefficients

were determined by Least Mean Square algo

rithm; finally, the signals were loaded to electro

Performance of passive fire protection for liquefied petroleum

gas vessels: An experimental and numerical study

M. Gomez-Mares, S. Larcher, A. Tugnoli & V. Cozzani

Alma Mater Studiorum—Università di Bologna, Dipartimento di Ingegneria Chimica,

Mineraria e delle Tecnologie Ambientali, Bologna, Italy

F. Barontini & G. Landucci

Università degli Studi di Pisa, Dipartimento di Ingegneria Chimica,

Chimica Industriale e Scienza dei Materiali, Pisa, Italy

ABSTRACT

Fire is among the most dangerous accident sce

narios that may affect the process industry. Vessels

containing pressurized liquefied gases are particu

larly vulnerable to external fires, since an increase

in the vessel temperature by a fire scenario may

result in both the rise of the internal pressure and

the weakening of the vessel structure. Vessel fail

ures due to accidental fires may yield a significant

escalation of accident severity, either by the release

of the vessel content or by overpressure generation

in the case of catastrophic failure (BLEVE).

Passive Fire Protection (PFP) is a robust and effec

tive solution to reduce the probability of accident escalation. In particular, fireproofing delays the temperature rise of the protected surfaces retarding vessel heat up and failure (CCPS 2003).

The assessment of the behaviour of the materials exposed to fire is a critical issue for determining the effectiveness of the PFP system. In particular, thermal coatings may undergo degradation (e.g., devolatilization) that causes the variation of key physical properties during prolonged fire exposure. Though the thermal degradation may be an inherent part of the protective action of the coating (e.g., in the case of intumescing coatings), the progressive deterioration of the material may lead to a decrease in the performance of the protection.

Although some large scale tests on vessels have been carried out (Landucci et al., 2009, VanderSteen & Birk, 2003), further studies are required in order evaluate the effectiveness of PFP systems. It has to be considered that this type of tests is expensive and hazardous. Coping with smaller scale tests and modelling is thus advisable to obtain a more effective route to explore this issue. Finite element modelling (FEM) combined with experimental tests at small scale

can be an option which allows to study in depth

these systems in a safe and reliable way.

In the present study, an approach to the

Probabilistic approaches used in the solution of design

for biomechanics and mining

K. Frydrýšek

VŠB—Technical University of Ostrava, Ostrava, Czech Republic

ABSTRACT

Let us consider the Simulation-Based Reliability

Assessment Method (SBRAM), a probabilistic

Monte Carlo approach, in which all inputs are

given by bounded histograms. In SBRAM, the

probability of failure or undesirable situation is

obtained mainly by analyzing the reliability func

tion RF = RV − S, see Fig. 1. Where RV is the ref

erence value and S is the load effect combination.

The probability of failure is P(RF ≤ 0).

This paper focuses on the probabilistic numeri

cal solution of the problems in biomechanics and

mining. Applications of SBRAM are presented in

the solution of designing of the external fixators

applied in traumatology and orthopaedics (these

fixators can be applied for the treatment of open

Figure 1. Reliability function RF (SBRAM).

Figure 2. Design of external fixators a) based on

metals—current design, heavier, expensive etc. b) based on polymers reinforced by carbon nanotubes—new design, lighter, x-ray invisible—leads to shortening the operating time and reducing the radiation exposure of patients and surgeons, with antibacterial protection cheap, more friendly etc.). Figure 3. Typical loading spectrum of an external fixator and numerical modelling for treatment of pelvis and acetabulum. Figure 4. Example of interaction between bits and hard rock and definition of the acceptable probability of overloading.

Probabilistic assessment of an aged highway bridge under traffic load

R.D.J.M. Steenbergen, J. Maljaars, O. Morales Nápoles & L. Abspoel

TNO, Delft, The Netherlands

ABSTRACT

Existing civil infrastructure represents a large economic value. Within the actions applied to the bridges, the traffic load is, in general, the most significant variable action to be considered when the ultimate limit states are under investigation. Consequently, the traffic load models play an important role in the design of new bridges but also in the reliability assessment of existing struc tures. This article evaluates the safety of an exist ing highway bridge in the Netherlands. In order to determine whether the structure can be safely used up to the moment of renovation, a proba

bilistic assessment of the bridge was performed. Important part of that study was a measurement program in order to determine the distribution of the stresses in the main load bearing structure due to the traffic load. From these measurements the design stresses were extrapolated using a tech nique for fitting an extreme value distribution to the measured data. Design stresses should be derived such that they provide a sufficient safety level of the bridge. After the semi-probabilistic analysis for all the bridge elements, for one bolted connection in the bottom flange of a main girder, a probabilistic calculation is performed in order to establish the safety level, avoiding all schemati zations and possible conservatisms in the calcula tion rules.

This paper describes an assessment method for the structural safety of an existing bridge during a calamity situation where one or more lanes are closed down. The method is aimed at determin ing the actual safety level of an existing high way bridge by focusing on the accurate determination of the actual traffic load effects. A probabilistic calculation is performed for a bolted connection in the bottom flange at midspan of one of the main

girders. It is aimed to assess the safety level of

the bridge according to EN 1990 and the require

Probabilistic modelling of hygro-thermal performance of building structure

Z. Sadovský, O. Koronthályová & P. Matiašovský

Institute of Construction and Architecture, Slovak Academy of Sciences, Bratislava, Slovakia

ABSTRACT

A probabilistic model of the hygro-thermal

performance of the internal surface of an external

wall is suggested. Particularly, the daily exceed

ances of the critical value of relative humidity on

the surface during the first year of its transition

from ‘as built’ state to the quasi steady state are

studied.

The time dependent internal/external loads are

represented by one concrete realization, related to

the climate parameters of the site and the activi

ties of inhabitants. In calculations, the hourly

measurements of the external temperature, air

relative humidity and solar radiation over one year

period are adopted. The indoor air temperature

is considered as practically constant, which cor

responds to the use of an ideal heating system.

The indoor air relative humidity results from the activities of inhabitants and the external climatic conditions. Among the quantities characterising building

structure composition, three selected material functions—water vapour permeability, moisture diffusivity and thermal conductivity are described by random variable parameters. The probabilistic model relates to the deterministic 1D simulation of heat and moisture transfer through the building structure, which has been algorithmised in the code NEV3. The time dependent values of relative humidity on internal surface of an external wall resulting from NEV3 calculations are analysed for daily durations of the critical threshold exceedances. Employing the Poisson spike process, the first-passage probability of exceeding a considered duration, conditioned by the actual values of the material parameters, is determined. The total probability is calculated by FORM.

Probabilistic models of thermal actions for bridges

J. Marková

Czech Technical University in Prague, Klokner Institute, Czech Republic

ABSTRACT

The paper is focused on the probabilistic models

of thermal actions. It is foreseen that the thermal

models will be applied for the probabilistic verifi

cation of bridges and other structures. The ther

mal models may also be used for the calibration of

partial factors and reduction factors of thermal

actions.

The basic variables influencing the effects of

thermal actions on structures include climatic

agents, operating process temperatures, charac

teristics of construction works and properties of

atmosphere and terrain. Random properties of

these variables may significantly affect the proba

bilistic analysis.

Four basic components of temperatures are dis

tinguished as given in EN 1991-1-5 (2005). Shade

air temperatures have considerable effect on the

uniform temperature component being mainly

influenced by the daily and seasonal changes, the

location of the site (altitude above the sea level,

configuration of terrain) and the wind velocity.

Solar radiation influences the temperature differ

ence components in the horizontal and vertical

direction and partly also the uniform temperature

component.

Variation of the upper bound of temperatures

x sup with the skewness α considering Weibull distri

Figure 1. Variation of the upper bound of tempera

tures x sup (μ,σ,α) in m, the characteristic and design

values of temperatures with the skewness α for Weibull

distribution.

0 x sup (μ , σ , α) T d T k α 0,1 0,2 0,3 0,4 0,5
0,6

0

10

30

40

50

M. Huber, P.A. Vermeer & C. Moormann

Institute of Geotechnical Engineering, University of Stuttgart, Stuttgart, Germany

M.A. Hicks

Delft University of Technology, Delft, The Netherlands

ABSTRACT

1 DESIGN PROBLEM FROM

A RELIABILITY PERSPECTIVE

The presence of uncertainties and their signif

icance in relation to design has long been appre

ciated. The engineer recognizes, explicitly or

otherwise, that there is always a chance of not

achieving the design objective. This element of risk

arises, in part, from the inability to assess loads and

resistances with absolute precision. Traditionally,

the engineer relies primarily on empirical factors

of safety to reduce the risk of adverse perform

ance (collapse, excessive deformations, etc.) to an

acceptable level. However, the relationship between

the factor of safety and the underlying probability

of failure is not a simple one. A larger factor of

safety does not necessarily imply a smaller prob

ability of failure, because its effect can be negated

by the presence of larger uncertainties in the design

environment. In addition, the effect of the factor

of safety on the underlying probability of failure is also dependent on how conservative the design models and the design parameters are, according to Phoon (1995). As stated by Phoon (1995), the problem associated with the traditional method of ensuring safety can be resolved by rendering broad, general concepts, such as uncertainty and risk, into precise mathematical terms that can be operated upon consistently. This approach essen tially forms the basis of Reliability Based Design (RBD), in which uncertain engineering quantities (e.g., loads, capacities) are remodelled by random variables.

2 SUMMARY AND CONCLUSIONS

Within this contribution, the concept of RBD has been explained for two problems in shallow tunnel ling. For the problems of tunnel heading stability and the design of the tunnel lining, a cohesive, fric tional soil was assumed.

For the probabilistic evaluation of the heading

Small failure probability assessment based on subset simulations:

Application to a launcher structure

C. Elegbede & F. Normand

Astrium, RAMS and Nuclear Safety Analysis Department, France

ABSTRACT

The standard formulation of structural reliability problem consists of integrating the probability density function of the random vector describing the structure, onto the failure domain. It is com mon to use Monte Carlo simulation or numerical scheme for the purpose. The difficulties appear when one wants to assess very small failure prob abilities with good precision using Monte Carlo simulations. The number of simulations may not be reasonable despite the use of variance reduc tion techniques. Therefore, a good alternative to classical Monte Carlo may be the subset simula tion approach proposed recently by Au et al. which bypasses the need to simulate rare samples for esti mating small probabilities. By introducing inter mediate failure boundaries, the failure probability is expressed as a product of conditional probabil ity, the evaluation of which only requires simula tion of more frequent events. In this paper, some investigations are performed to tune and assess the subset simulation algorithm. Subset simulation algorithm is described and the choices of the algo rithm parameters are discussed. With the basic stress-strength model for which analytical and exact numerical results are available, the failure probability has been assessed. This enables us to have an idea on the number of simulations to be performed according the

target safety failure in consideration. The results obtained with the sets of benchmark show the advantage and the efficiency of subsets simulations. The results obtained with the sets of benchmark shows the advantage and the efficiency of subsets simulations. An algorithm based on subset simulation is assessed. The buckling probability of launchers thin-walled cylindrical structure, subjected to safety requirements, is studied as application of the method for axial compression and external pressure. In addition, a benchmark is provided to illustrate the efficiency of the method used. Subset simulations give the same results as classical Monte Carlo simulation but is less costly time consumer. In engineering point of view, these results are relevant, particularly, for structural analysis if one wants to link reliability code to finite elements code.

Uncertainty analysis of ultimate limit state of steel bar structures

Z. Kala

Brno University of Technology, Brno, Czech Republic

ABSTRACT

The objective of the present study is an analysis of the influence of number of members under tension on the general random load-carrying capacity of a structure. The analytical mathematical model was applied for calculation of load-carrying capacity. The analytical mathematical model was applied for calculation of load-carrying capacity. For structure presented in Fig. 1, it is necessary to consider that the load-carrying capacity of any supporting member under tension is higher than the effect produced by the load F. The load-carrying capacity of each member under tension is the statisti

cally independent random quantity determined as

a multiple of cross-section area and of yield point.

The general load-carrying capacity of a structure

is equal to the minimum value of load-carrying

capacity of individual members under tension.

Eight structures were solved with the number of

members from 2 to 9. The random load-carrying

capacity depends on the random area and on

random yield point, and these are the quantities

known from experimental research. The statisti

cal analysis was evaluated by means of the Monte

Carlo method for 100 000 simulations.

The change both of mean value and standard

deviation of load-carrying capacity of the struc

tures is evident. With increasing number of mem

Figure 1. System of members under tension.

Updating partial factors for material properties of existing structures

in a Eurocode framework using Bayesian statistics

R. Caspeele & L. Taerwe

Department of Structural Engineering, Ghent University, Ghent, Belgium

ABSTRACT

The assessment of existing structures becomes

increasingly important and influences asset plan

ning and decision making. However, currently

a certain duality exists between on the one hand highly complex calculation methods and probabi listic or semi-probabilistic design methods for the design of new structures and on the other hand the current practice for the assessment of existing structures which most often relies on the (subjec tive) judgment of the investigating engineer.

The way in which laboratory and/or in-situ test results are incorporated in the safety assessment of existing structures can and should be improved and a better consensus should be looked for with respect to the required safety elements (e.g., target safety levels, partial factors, …) for existing struc tures and more particularly for those which have experienced deterioration. This would result in a coherent, less conservative and more objective basis for establishing improved criteria to decide when preventive actions should be taken and when and to what level an existing structure should e.g., be strengthened in order to meet the safety requirements.

This paper briefly describes some basic ideas regarding an updating procedure with respect to partial factors for material properties, considering a semi-probabilistic design philosophy that incor

porates a Bayesian updating technique and is com

patible with the current framework provided by the

Eurocodes.

Normal-gamma and lognormal-gamma distri

butions form a class of natural conjugate priors

that can be used to easily update hyperparameters

for the probability density functions of material

properties.

Further, a reduction factor is derived based on a

simplified Level II approach in order to update the

partial factors for material properties as given in

the Eurocodes. More specifically, alternative values

for the reliability index can be taken into account

(considering cost optimization and remaining

working life) and the additional information by

in-situ and laboratory testing can be translated

into an adjusted value for the partial factor of the material property under consideration. Figure 1 illustrates this reduction factor ω γ in case the representative value X rep of the material property corresponds to a 5% fractile, considering further also a reliability index for new structures as β′ = 3.8 and a prior predictive coefficient of variation δ′ = 0.15. Figure 1 illustrates the influence of the ratio ′ δ δ ′′ X X of the posterior to the prior predictive coefficient of variation (based on the Bayesian updating of the hyperparameters) on the reduction factor ω γ for different values of the target reliability index β'' = β t for existing structures. Based on these reduction factors, the updated partial factor can be calculated as: γ ϖ γ γ γX exist X Rd, = ≥ (1) with γ X the partial factor available in the Eurocodes in case of new structures and considering additionally that the reduced partial factor for the material property in case of existing structures

should not be smaller than the model uncertainty. Finally, the developed methodology is illustrated in case of the partial factor for concrete strength. Figure 1. Influence of the ratio δ X ”/ δ X ’ on the reduction factor ω γ considering X rep = X k (α R = 0.8, β’ = 3.8, δ’ = 0.15). This page intentionally left blank System reliability analysis This page intentionally left blank

A fast augmentation algorithm for optimizing the performance

of repairable flow networks in real time

M.T. Todinov

Oxford Brookes University, Oxford, UK

ABSTRACT

Repairable flow networks are a very important

class of networks. Particular examples are the

production networks, communication networks,

transportation networks, energy distribution net

works and supply networks. An essential feature of

repairable flow networks is that a renewal of failed

components is taking place after a certain delay

for repair. There is no exaggeration in stating that

most of the real flow networks are in fact repair

able flow networks. Analysis and optimisation of

repairable flow networks is a new, recently initiated

area of research.

The paper continues the research on repair

able flow networks by stating and proving a new

theorem related to restoring the maximum flow in

repairable flow networks. The maximum flow in a

repairable flow network after a failure of several components can be restored very quickly by a two stage procedure. The first stage consists of augmenting the dual network with a new source and a new sink as much as it is possible. The second stage follows the first stage and consists of augmenting the dual circulation network until all outgoing edges from the new source are fully saturated. The initial edge flows in the dual circulation network are the resultant edge flows obtained after augmenting the dual network.

On the basis of this theorem, a very efficient augmentation algorithm has been proposed for restoring the maximum flow in repairable flow networks after a failure of several components. For a single failed component, or few failed components, the average running time of the proposed algorithm is $O(m)$, where m is the number of components in the network. The running time of the proposed algorithm increases linearly with the size of the network and, currently, it is the fastest available algorithm for restoring the maximum flow in repairable flow networks.

The very high computational speed of the proposed algorithm makes it possible to control and optimize the performance of flow networks in real time. Upon

failure, the network flows need to be redirected quickly in order to restore the maximum output flow. This is important for example for production networks, power distribution networks, computer networks, emergency evacuation networks, etc. The algorithm is also suitable for designing discrete-event simulators of production systems, where, in order to track correctly the variation of the output flow, the maximum flow needs to be calculated many times, after each component failure and return from repair. The paper also presents for the first time a study on the link between the topology of complex flow networks with redundancy and their threshold flow rate reliability—the probability that on demand, the output flow from the network will be equal to or greater than a specified threshold value. Determining the threshold flow rate reliability for repairable flow networks with redundancy is particularly important for telecommunication networks. For these, a small part of the network (often only a single path from the source to the destination) is used for a data transfer. Failures of hosts, routers and communication lines are frequent, and are inevitably associated with downtimes for repair. An important part of the proposed algorithm is the algorithm for restoring the maximum flow after component failures. By using the simulator, we show that the topology of repairable flow networks has a significant impact on the threshold flow rate reliability. Two networks built with identical type and number of components can have very different levels of the threshold flow rate reliability. The paper also shows that the threshold flow rate reliability depends strongly not only on the network topology but also on the size of the network. With increasing the network size, the influence of the network topology increases significantly.

A Monte Carlo simulation based dependability analysis

of a non-Markovian grid computing environment with software

rejuvenation

V.P. Koutras

Department of Financial and Management Engineering,
University of the Aegean, Chios, Greece

S. Malefaki

Department of Engineering Sciences, University of Patras,
Rio Patras, Greece

A.N. Platis

Department of Financial and Management Engineering,
University of the Aegean, Chios, Greece

ABSTRACT

Grid computing is an innovative technology for complex systems with large scale resource sharing, wide area communication and multi institutional collaboration. Its main advantage is that it enables sharing, selection and aggregation of a wide vari ety of resources, including supercomputers, data resources, storage systems that are geographically distributed. In this paper, a grid system with star topology is considered, consisting of a Resource Management System (RMS) and n distributed Root Nodes (RNs). The lifetime distribution of the RMS is assumed to be exponential while its repair time follows a general distribution. Moreo ver, it is assumed that all the RNs have a common lifetime and repair time distributions. The lifetime distribution of each RN is exponential and the repair time distribution is a general distribution. Each of the RNs can be either in the functioning state or in the failure state. Additionally, the RMS is assumed to experience software aging phenom ena due to resource exhaustion. To counteract such phenomena, a preventive technique called soft

ware rejuvenation is adopted. Due to the structure

of the system, it is not important to be aware of

which of the components are functioning but only

of the number of the working components. Hence,

the state space of the model presented, depends on

the state of the RMS’s software and on the number

of available nodes. The system can be considered as

operational when the RMS is available and simul

taneously at list one of the n nodes is operational.

Although the evolution in time of each com

ponent of the system is described by a continuous

time semi-Markov process, this is not the case for

the whole system. Thus, in order to study the main

dependability measures of the aforementioned sys

tem, the well known formulas for the main reliability

An adapted application of FMEA in the identification of critical

dynamic failure modes of digital reactor protection systems

G. Wang

Technology and Engineering Center for Space Utilization
Chinese Academy of Sciences, Beijing, China

S. Li

M.A.R.S. Technology & Engineering Solutions Ltd. Beijing, China

ABSTRACT

In digital Instrument & Control (I&C) systems,

the existence of interactions between software and hardware components could incur functional failures in the system level. A digital Reactor Protection System (RPS) comprises complex voting algorithms, switching (fail-safe) mechanisms and communicating networks that could interact to cause the system to fail in dynamic ways. The timing of component failures and subsequent control policies has much impact on the system performance. Although risk-informed decision-making has not been implemented in the review of digital I&C systems yet due to that there presently exists no universally accepted methods for modeling digital system reliability, it is significant that an effective approach must be employed to adequately identify digital system failure modes for decision-makings on design alternatives during the development of such a digital RPS. A comprehensive understanding of these functional failure modes is extremely important in the initial design phase. However, the widely applied traditional Failure Mode and Effect Analysis (FMEA) shows its inadequacy in addressing the interactions. This paper is based on the works in the early development stage of a digital RPS. It is concerned with the dynamic fail

ure modes in digital I&C systems and proposes a Timeline approach as a tool to implement comple mentary qualitative analyses based on the FMEA results. The Timeline approach shows its capacity to obtain understanding of how the digital I&C systems react and compensate a component failure in a very short time. While it is concluded that the proposed method can be used to obtain qualita

An analysis of applying RCM methodology in a Brazilian thermal power plant

P.H.C. Lins, T.V. Garcez, M.H. Alencar & A.T. de Almeida

Federal University of Pernambuco, UFPE, Recife, Brazil

ABSTRACT

Recently, competition among companies, the globalization of business, the growth of mecha nization and automation in addition to the con stant technological changes and the implications of these for industries on issues related to the environment have been major factors which have brought about changes in the structure of compa nies. In this scenario, maintenance actions, which are part of the production process, can influence a company’s approach to competition, as well as its business strategy. The availability of an asset is highly correlated with how it is managed. Any

strategy must include a plan for maintenance activ

ities because failures generate unplanned actions.

One of the biggest challenges for companies with

regard to maintenance is to decide what techniques

should be used in their organizations in order to

improve the performance of assets and to reduce

maintenance costs. Therefore, the implementation

of approaches related to maintenance has been

studied in order to guide companies on how to

manage this process better. Among the approaches

most used in the maintenance industry, RCM

(Reliability-centered Maintenance), an approach

that started in the commercial aviation industry,

stands out. According to Deshpande & Modak

(2002), RCM offers the most systematic and effi

cient process for addressing an overall program

matic approach to optimizing the maintenance of

plant and equipment.

In this context, this paper presents an analysis

of applying RCM methodology in a natural gas thermoelectric power plant, located in Brazil. This power plant studied has three turbines in a combined cycle system, two of them being driven by natural gas and the third one, by steam. Power plant systems whether directly or indirectly involved in the process of power generation are quite complex and interconnected. Therefore, should these systems fail, this can easily lead to the plant shutting down. In this scenario, the role of maintenance becomes even more important and acute. Implementing RCM contributes positively to improving the operation of the

plant as well as to maintenance planning. Thus, in this paper, introductory aspects of RCM methodology, the segment in which the company operates, and how the system under study fits into this scenario are described by way of contextualizing the process. Then, an examination of the steps for implementing the approach proposed is presented, particular emphasis being placed on the stages of selecting functions, analyzing failure modes and choosing relevant and effective maintenance activities. Finally, a summary of the most important points in the process is made by analyzing the results, the difficulties found, and the items that need to be improved. REFERENCE Deshpande, V. & Modak, J. 2002. Application of RCM for safety considerations in a steel plant. Reliability Engineering and System Safety 78: 325–334.

An approach for coupling single component failure event with different common cause groups

Duško Kančev

Jožef Stefan Institute, Ljubljana, Slovenia

Marko Čepin

University of Ljubljana, Ljubljana, Slovenia

ABSTRACT

This paper introduces a new approach for consideration of single component failure in different Common Cause Component Groups (CCCGs) within Probabilistic Safety Assessment (PSA) modelling. Common cause events are a subset of dependent events in which two or more component fault states exist at the same time, or nearly so, and are a direct result of a shared cause. (Mosleh et al., 1988). Several different parametric models exist for qualitative representation and quantification of depend

ency between equipment failures within Common Cause Failure (CCF) analysis. Some of them are the alpha factor, beta factor, binominal failure rate, multiple Greek letter. Although each of the models is characterized with certain specifics, all of them share the same general idea. This common idea is the fact that component failure probability, i.e., each components failure space, can be divided to independent and dependent, common cause affected portion. The relation between both portions is determined with different parameters defined within the specific parametric model selected (Cepin 2010). The motivation for the study presented herein is the incapability of one of the most widespread PSA softwares (Relcon AB 1998) for simultaneous assignment of one single component failure event in more than one CCCG within the fault tree analysis technique. The occurrence of such a scenario where a sin

Automated generation of a reliability model for a system undertaking phased missions

S.J. Dunnett & K.S. Stockwell

Loughborough University, Loughborough, Leicestershire, UK

ABSTRACT

There are various mathematical models available to assess the reliability of a given system, these

models relate the performance of the system to the performance of the components of which it is comprised and can be used to determine the failure probability or failure frequency of the system in question. The models can be applied at the design stage to investigate alternative design options and influence the development of the system. They can also be used to prove that the system will perform to the required standard once its design has been finalised. However the most beneficial way to use the models is at the design phase when there is the most flexibility in changing the design in response to the predicted performance. Currently there is software available to perform the mathematical analysis of the model but the construction of the model, used as input to the software, is undertaken manually. This is quite a lengthy process and can limit the usefulness of the model, as during the time the models are being developed for a specific sys tem design, and analysed, the system design inde pendently progresses and evolves. Therefore the model and its influence lag behind the actual real ised design. Another limiting factor is that design teams do often not have the expertise required to construct the models and it is therefore passed to a

specialist group to perform the task. Hence result

ing in a loss of overall control and project cohe

sion. One way of improving this situation would be

to automate the construction process. This would

enable the performance of alternate system designs

to be obtained quickly, allowing for the optimal

system design to be selected before progressing. In this work a procedure is developed to automatically generate a reliability model for a system undertaking a phased mission. Such a mission is made up of consecutive time periods, known as phases, within which the system may have to meet different requirements for successful completion of the phase. System failure during any phase will result in mission failure. Due to the complexity of modelling phased missions simulation techniques have been adopted with the model developed based upon Petri Nets. These provide a graphical modeling tool for dynamic system representation and are very flexible in the system features that they are capable of modelling. The procedure outlined in this work takes as input a description of the system, including the system structure, its usage, phase information and component failure and repair data. From this information decision tables are developed for the components that consider all possible combinations of inputs and component states and their influence on the component output. For systems undertaking phased missions some of the components outputs are also dependent on the phase, this information is also included in the decision tables. For components with different modes of operation, operating mode tables, describing the effect on the operating mode of different inputs and component states are also developed. Using these tables and the system topology distinct Petri nets are generated that model the component failure and repair, the interactions between components within the system and the phase progression and mission success or failure. These nets can then be used to simulate the system reliability.

Contribution to mission profile effect onto sequential system reliability

M. Koucky

Technical university, Liberec, Czech republic

D. Valis

University of Defence, Brno, Czech republic

ABSTRACT

Complex mechatronic systems sometimes do work in difficult and adverse environment. Such environment may affect the system's performance and also dependability characteristics. Since we use complex systems with one shot items we need to know basic characteristics of such a system. The paper deals with advanced mathematical methods used for field data assessment in order to prove presumed impact of mission profile and system real operation profile onto system reliability. Thank to the collected data set it is assumed that operation of the system is actually a kind of time series. The paper presents identification of the time series model, its parameters' estimation and prediction of system characteristics—like reliability/survivability function of the system for instance. Since the model of the time series has not been known, correlations with other system can be further determined and mission duration estimated. This estimation helps to organize support and operation of the system. This contribution is supposed to contribute to

procedures of reliability calculations of the com

plex (in this case a weapon) system as an object

under investigation. We would like to present ways

how to determine some characteristics of reliabil

ity performance of the set which may be influ

enced by a mission profile. The goal of this paper

is also to verify the suggested solution in relation

to some functional elements which might be influ

enced by the mission profile. Since the system ful

fils a required function in a very specific manner

we focus on the mission profile impact (Koucky &

Valis 2007, Valis & Koucky 2008).

The object under investigation “PL-20 aircraft

gun” was designed for the needs of the Czech Air

Force and it was fielded into its armament as an

onboard weapon for the L-159 advanced light

combat aircraft. It refers to a 20-mm calibre twin

gun, the automatic function of which is actuated

by powder gases from its barrels. A failure of a

round of these automatic weapons might result

Dependability analysis activities merged with system engineering,

a real case study feedback

R. Cressent, V. Idasiak & F. Kratz

PRISME / ENSI de Bourges, Bourges, France

P. David

Grenoble-INP / CNRS G-SCOP UMR5272, Grenoble, France

ABSTRACT

The design of modern innovative systems requires the use of processes able to supervise the project, from the needs expression to the system exploi tation. Those processes form the System Engi neering (SE) deployment. SE activities manage the engineer's tasks to ensure the perenniality of requirements, the following of made choices and the capitalization of the generated technical knowledge. The dependability aspects have to be integrated more directly into SE processes, and currently efforts still have to be made in that direc tion. To support the interaction between SE and dependability study, our research team developed the MéDISIS methodology (David et al., 2010) (Cressent et al., 2011).

During former projects with various industrial partners, we described processes that were added to MéDISIS in order to integrate several depend ability study activities to our partner's SE proc ess. In this paper, we model the activities and the knowledge involved in their SE process and join the requested dependability studies. Thanks to this model, we point out the needs that MéDISIS

has to cover in terms of knowledge collection and organization. We underline the central role of the DBD (Dysfunctional Behavior Database), illustrat ing how SysML permits to collect and organize the knowledge created by the analysis of professional processes using Parametric Diagrams and Inter nal Block Diagrams. To describe how MëDISIS actions easily fit in a larger Model Based System Engineering (MBSE) strategy, this paper qualifies all the benefits we observed during a real industrial project.

To illustrate this deployment of MëDISIS in a relevant context, the results, obtained recently, will be presented following a six steps merged process. First, the design activities of SE are realized using SysML as a supporting language: requirements formalization (Requirements Diagram), technical

Fast mission reliability prediction for unmanned aerial vehicles

J.D. Andrews

University of Nottingham, UK

J. Poole & W.H. Chen

Loughborough University, UK

ABSTRACT

There is currently a significant interest in the use

of autonomous vehicles. One such example is the ever increasing use of Unmanned Aerial Vehicles (UAVs), particularly in military operations. UAVs also have potential civil applications which would require demonstration that they are able to respond safety to any potential circumstances, such as the occurrence of component failures, the emergence of threats such as other aircraft in the neighboring airspace, and changing weather conditions. The likelihood that an aircraft will successfully com plete any mission can be predicted using phased mission analysis techniques. The predicted mission unreliability can be updated in response to chang ing circumstances. In the event that the likelihood of mission failure becomes too high then changes have to be made to the mission plan. If these cal culations could be carried out fast enough then the quantification procedure could be used to estab lish an acceptable response to any new conditions. With a view to using the methodology in this con text this paper investigates ways in which phased mission analysis calculation time can be reduced. The methodology improves the processing capabil ity for a UAV phased mission analysis by taking into account the specific characteristics of the fault

tree structures which provide the causes of phase

failure. It also carries out as much of the quanti

fication as possible in advance of the mission plan

being formulated.

The calculations carried out prior to the mis

sion definition are referred to as the off-line calcu

lations. The final unreliability prediction requires

information about the specific mission configura

tion and has to be carried out following the mis

sion specification and is referred to as the on-line

analysis time.

For a UAV, power supplies and utilities (pneu

matic or hydraulic supplies) for systems frequently

effect all phases of a mission. On an aircraft cer

tain key aspects of functionality, such as thrust,

How IEC 61508 can be used to design safe offshore wind turbines

L. Dai & I.B. Utne

Department of Marine Technology, Norwegian University of Science and Technology, Trondheim, Norway

M. Rausand

Department of Production and Quality Engineering, Norwegian University of Science and Technology,

Trondheim, Norway

ABSTRACT

Offshore wind energy is today an emerging

industry with relatively small margins for profit.

A number of studies are currently carried out on the reliability analysis of different subassemblies or components in Offshore Wind Turbines (OWTs). However, the protection systems are generally overlooked.

IEC 61508 is a generic standard which is applied on safety related systems in a range of different sec tors. Its application starts with risk analysis of the system, and identification of the criteria related to the risk reduction and the tolerability of risk. Most of the time, the operation of offshore wind farms is unmanned. Thus, damage to the OWTs is the primary concern for safety, and financial losses are the main consequences. Several cost elements may contribute to financial losses, including the direct turbine damage cost, the follow-on cost on pro duction interruption and repair/dismantlement, and the potential cost related to security of power supply, possibility of losing subsidies, and person nel injury/fatality.

Several common hazardous events in OWTs are introduced in this paper, which are rotor over-speed, generator overload or fault, excessive vibration, and abnormal cable twist. The perform ance of OWTs is significantly influenced by the

system configuration and environmental condi

tions. Therefore, practical experience is of great

importance to analyze the initiating causes of the

hazardous events and the initiation likelihood.

In practical application, more hazardous events

might be identified with the techniques suggested

in IEC 61508. These hazardous events should be

investigated to improve learning and reduce the

probability of future events. Learning from experi

ence should also be used to define safety require

ments, which are further allocated to the various

protection layers.

An OWT is equipped with control and protec

Impact of different minimal path set selection methods on efficiency of fault tree decomposition

V. Matuzas & S. Contini

European Commission, Joint Research Centre, Ispra Establishment, Italy

ABSTRACT

The Level-1 PSA analysis of a nuclear power plant

is based on ET and FT techniques. The analysis of

ET accident sequences implies the analysis of very

complex fault trees. The main factor that prevents

the exact analysis of such large fault trees is insuffi

cient computational resources (mainly insufficient

working memory to store the BDD or the MCS

depending on the approach). Current FT analysis

methods use several efficient algorithms to reduce

the complexity of the FT model in order to be

able to determine at least an approximated result.

The problem however is that the approximation

may be an under estimation of the accident fre

quency and there is no method able to determine

the truncation error on complex trees. Hence, new

methods are needed to improve the quantification

procedures.

In recent papers (Contini & Matuzas 2011a,

Contini & Matuzas 2011b) a new method to

analyse complex fault trees was proposed by the

authors. The fault tree is decomposed into a set of

mutually exclusive simpler fault trees up to their

dimensions are compatible with the available com

putational resources. Then, the results of the exact

analysis (using the BDD approach) of all simpler

trees are composed to obtain the exact results for

the original un-decomposed complex fault tree.

The decomposition is based on the events mak

Issues of reliability in mobile working machines—inquiry study

Antti-Ville Itäsalo & Asko Ellman

TUT, Tampere University of Technology, Tampere, Finland

Tero Välisalo

VTT Technical Research Centre of Finland, Tampere, Finland

ABSTRACT

This paper deals with issues of reliability of the mobile work machines. Mobile work machines need to operate very reliably so that the working operation and the delivery of the products won't be disturbed. For this reason the work machine buyers have begun to require more exact reliability and maintenance information and possibly out of-service times about the work machines. They also want to know the overall lifetime cost of the machine.

Another interesting thing is the transformation of manufacturers to maintenance services provid ers. The profitability of the maintenance services depends on the ability to arrange the maintenance operations in order to avoid additional mainte nance operations due to unexpected failures or minimize the time consumed for them. In other words the malfunctioning of devices should be able to be controlled. The management of the reli ability issues of the work machines is difficult due to the special characteristics of their use which are

varying loads, demanding operating conditions

and small manufactured series.

The study is based on the inquiry for which 11

Finnish companies have corresponded. The vari

ety of the work machines concerned is wide: from

forest machines to lifts. The operating environ

ments of the machines are also quite different. For

the inquiry a wide representation of persons that

are involved in the different stages of the design

and manufacturing process was needed. The inter

viewed workers included engineers, product man

agers, maintenance managers or the experts of the

reliability.

The focus at the inquiry is to determine the main

Management of factors that influence common cause failures of safety

instrumented system in the operational phase

M. Rahimi, M. Rausand & M.A. Lundteigen

Department of Production and Quality Engineering, Norwegian University of Science and Technology,

Trondheim, Norway

ABSTRACT

Common Cause Failures (CCFs) are serious

threats to the reliability of Safety Instrumented

Systems (SIS). System vulnerabilities to CCFs may

be introduced in all phases of the system life cycle,

and especially in design, installation. Many of these vulnerabilities are the results of inadequate decisions and acts by the SIS designers, the installation crew, the operation and maintenance personnel, and the plant management. In the design phase, a significant effort is often devoted to avoid CCFs, for example, by implementing diversity.

This paper is focused on the operational phase. At the start of this phase, the hardware architecture and the components are settled and will usually remain unchanged in the whole operational phase, unless there is a call for modification. During the operational phase, the SIS reliability will mainly be influenced by the (i) environmental conditions, (ii) the operational and maintenance/testing procedures, and (iii) the actual human interactions with the systems. These influences may have impact on both random hardware failures and systematic failures. For CCFs, the influences on systematic failures are the most important.

This paper focuses on the third type, i.e., the CCF vulnerabilities influenced by the actual human interactions and the possible human errors committed during these interactions. The human errors will again be influenced by organizational factors.

The link between human and organizational fac

tors and CCFs in SISs is undeniable and has been

documented in a range of investigations.

A high number of CCF models have been pro

posed to incorporate the effects of CCFs into

quantitative risk and reliability assessments. Most

industries, however, suffice with the simple beta

factor model, which was introduced by Fleming

(1975).

The beta-factor model is preferred mainly

due it’s simplicity. This model has only one extra

parameter, the beta-factor, β, which is the frac

tion of CCFs among all failures of a component.

Modelling of dynamical dependability by using stochastic processes

J. Chudoba

Technical University of Liberec, Liberec, Czech Republic

ABSTRACT

This paper on the topic of “Modelling of dynamical

dependability by using stochastic processes” has

the main aim of expanding the Markov analysis

(in dependability) by adding an instrument, which

allows learning and describing time and perform

ance dynamics of complicated systems, especially

network structure. The base hypothesis of the

Markov analysis is that failure and repair rates

between two postures are constant.

The instrument for time dynamics can solve

tasks whose failure and repair rates are not con

stant and also solve repairs in predetermined main

tenance. Mathematical solving of this problem is

based on a construction of differential equations

with non-constant parameters and their solution.

The Runge-Kutta method is used for components,

which are as “good as old”. The Monte Carlo

method is usually used for components of a sys

tem, which are as “good as new”.

Performance dynamics can be described as

systems with multiple counts of the same items.

Resultant dependability of these items depends

on the production volume and the combination

of items, which are in use, or in active and passive

redundancy. An example can be mentioned as modelling of dependability of an electrical network and systems for railways and roads. Practical solving of this project was shown on the modelling of a compressor station and adjacent lines of the gas pipeline RWE Transgas. After instantaneous unavailability, a solution is possible to determine the probability that this gas pipeline system is not able to provide gas distribution to customers in required amounts. This could mean that the provider can’t provide gas distribution in the required qualities or another example can be that gas pipeline becomes overloaded etc. Conventional software engines in dependability didn’t solve these problems at that time. This dissertation thesis may help on a large scale by an efficient evaluation of probability of the creation on catastrophic failures by the modelling of complicated systems. Thanks to the revaluation of modelled causes of

dependability it is possible to decrease the probability of cataleptic failure. This can be achieved, for example, by more efficient maintenance, or multiple component redundancy. If the probability of cataleptic failure is effectively decreased, it would bring a reduction of cost resulting from the frequency of gas distribution failure and also the total time of failure.

Qualitative analysis of a BDMP by finite automaton

Pierre-Yves Chaux

LURPA, Cachan Cedex, France

EDF R&D, Clamart, France

Jean-Marc Roussel & Jean-Jacques Lesage

LURPA, Cachan Cedex, France

Gilles Deleuze

EDF R&D, Clamart, France

Marc Bouissou

EDF R&D, Clamart, France

École Centrale Paris, Chateney-Malabry Cedex, France

ABSTRACT

Many studies which have been carried out on pre

dictive risk modelling and assessment target two

complementary objectives (Henley and Kumamoto

1981). On the one hand, quantitative analyses aim

at calculting the failure rate of the modelled system

or of one of its subsystems. On the other hand the

qualitative analyses aim at determining the sce

narios which lead to the failure of the whole sys

tem. While those scenarios are in most cases only

constituted by basic components failures, they may also include repairs of these components.

The Boolean Driven Markov Processes (BDMP) were created to include all the Electricite De Francé expertise in the construction and analysis of reliability models (Bouissou and Bon 2003). While staying close to Static Fault Tree models (Stamatelatos, Vesely, Dugan, Fragola, Minarick, and Railsback 2002), BDMPs extend the fault tree capacities by allowing to model both the failures and repairs of basic components. This extension also enables the description of the redundancies between components and between complex sub systems constituted by a number of components, which can be redundant one from another.

The main goal of this study is to conduct a qualitative analysis of a BDMP while setting aside all its capacities to model and conduct quantita tive analysis on the reliability of a system. The qualitative analysis consists in enumerating all the sequences of repair and failure events that are implicitly described by a BDMP. To explicitly describe those combinations, this study is con ducted within the languages and Finite Automata (FA) theories. For that, each scenario of failures

and repairs is translated into a sequence of events.

The set constituted by those sequences (or words)

Reliability analysis of phased-mission systems with phase mission backup

Xiaoyue Wu & Qi Liu

College of Information Systems and Management, National University of Defense Technology,

Changsha, Hunan, China

ABSTRACT

This paper proposes a Continuous Time Markov Chain (CTMC) model approach for the reliability analysis of Phased-Mission Systems (PMS) with phase mission backup. The spaceflight Tracking, Telemetry and Command (TT&C) system is an important technological supporting system providing services for spaceflight mission in consecutive phases. Sometimes, the mission success of TT&C depends not only on the success of each phase, but also depends on the redundancy of mission implementation between phases. For example, the mission failure during current phase can also be completed during the following phase. Therefore, there exists PMS that has phase mission backup for a given mission phase. To the best of our knowledge, this kind of PMS has not been investigated by researchers.

For the reliability analysis of such kind of

PMS, we build a CTMC model for each mission

phase as for conventional PMS. For each i ∈ N, let

π i (t) = P{X(t) = i} represent the probability that the

system is in state i, at time t, and π(t) = (π 1 (t), …,

π n (t)). Then, the state probability vector of the sys

tem after time t can be given as

π(t) = π(0)e Qt

Assume there is only one critical mission phase

Ph i with phase mission backup (Figure 1). Let Ph j

be the mission backup phase for Ph i . Both phases

Ph i and Ph j have their own missions, denoted as M i and M j respectively. If M i is failed during the mission time of Ph i , then it is arranged to be executed again during the mission time of Ph j If M i is failed again in Ph j , then it is said that mission M i is failed for the PMS, that is, the whole mission of PMS fails since one of its mission failed. For the mission phase which provide mission backup for other phase, if the mission of its backuped phase fails, then it will be decomposed into two subphases. The success of one subphase requires the success of its original mission and the failed mission of the previous phase. The mission success of another subphase only needs the accomplishment of its own original mission. Regarding the success or failure of the backuped mission phase as the initial states condition with different probabilities, the mission reliability of the backup phase can be found by solving the CTMC. By combination of all these results with different probabilities, the total mission reliability can be calculated. Let the whole mission of PMS be denoted as M, then the mission reliability of the PMS R PMS is the sum of the reliabilities of the two exclusive cases as follows R R R f PMS PMS S i i f + = + 1 2PM P { }M success ul M success ul in Phn Pr{M successful M fail in Ph i i n } A simplified PMS with three phases is used to illustrate the application of our approach. The numerical results shows that by phase mission backup, the mission reliability of

the PMS is increased by 0.0064 from 0.9559.

Figure 1. Mission phase and its backup phase. i Ph j Ph i T j T 1j i T T= 2j j i T T T= - i M j M j M i M 1j Ph 2j Ph

1i t 2i t 1j t 2j t 3j t

Reliability analysis of the electronic protection systems with mixed

m-branches reliability structure

A. Rosiński

Warsaw University of Technology, Warsaw, Poland

ABSTRACT

In the article are presented questions connected

with the electronic protection systems.

Into the group of the electronic protection sys

tems we can include:

- Intruder alarm system,
- System Control Access,
- Closed Circuit TeleVision,
- Fire alarm systems,
- Systems of external terrains' protection.

Projecting the electronic safety protection sys

tems it should be considered the stage of the threat

(according to valid standards) stepping out in the

protected object, particularly when this objects

relates to the special objects (e.g., the protection

of airport, railway stations). Than having the

directives defines the minimum number of units

from what the system has to composed, we can

approach to the choice of the type of alarm central

station and co-operating with it devices. The use

on this stage of the presented in the article method

of the analysis of reliability structures makes pos

sible the formation of the values of the probabili

ties of staying in the respective states: full ability,

the impendency over safety and unreliability of

safety. It should be however considered the fact,

that applying of the surplus results in enlargement

of the financial value of the system.

The introduced method can also be used to the

modernization already existing and the exploited

electronic protection safety systems. If there

Reliability analysis of vacuum sewerage systems using the total

probability theorem

Katarzyna Miszta-Kruk

Warsaw University of Technology, Poland

ABSTRACT

Small towns having a flat terrain topology decide

to introduce unconventional solutions to waste

water systems in relation to gravity sewers. Those

solutions include inter alia vacuum sewerage sys

tems which according to the carried out sociologi

cal studies are acceptable systems by end users. It

is believed that those systems are more reliable

than conventional ones; however it has not been

yet in any way confirmed by reliability research or

dissertations.

The research methodology and the reliability

model of the vacuum sewerage system, using the

theorem of the total probability, have been devel

oped and gave rise to the quantitative evaluation of

the reliability of the system individual components.

As a consequence, it enables the quantitative esti

mation of values of reliability indices of the entire

vacuum sewerage system. It also allows using the

term reliability to quantify its specific values.

Reliability analysis of network systems, which

include sewerage systems, consisted of describing the structure of the system with its division into III subsystems, defining elements in each subsystem, defining reliability states and determining probabilities of staying in those states using the theorem of total probability. Reliability structures of isolated subsystems represent interconnections of the system elements from the viewpoint of their failures impact on the reliability of the subsystems. It is assumed that elements forming subsystems are two-state elements. Reliability of the vacuum sewerage system was defined for two cases i.e., when the system is able to take sewage from the entire area (full suitability), and when it is only possible to discharge sewage from part of the area (partial suitability). The key input to the model are failure intensity values gathered from operational reliability research of 4 sewage systems that was carried out over a period of 2 years. System reliability expressed by probability of full suitability was estimated through determination of probabilities of individual elements suitability and of conditional probabilities.

Requirements for dependability management and ICT tools in early stages of the system design

P. Valkokari, T. Ahonen & O. Venho-Ahonen

VTT Technical Research Centre of Finland, Tampere, Finland

H. Franssila

University of Tampere, Tampere, Finland

A. Ellman

Tampere University of Technology, Tampere, Finland

ABSTRACT

The findings of our paper are results of an on-going research project which has its focus on depend ability management in design process and from a pre-study which was used for defining the objec tives of the research project. Our paper focuses on the practical needs of companies for methods and tools for reliability management at various stages of product development processes. The pre-study revealed that there has not been a major investment to the research dedicated to dependability manage ment for a decade at European level. However, at the same time there has been a change in compa nies' strategies because of an ongoing change in the business environment. System providers are cur rently facing severe global competition. In order to

maintain their competitiveness, system providers are transforming into life cycle service providers. Therefore, actors, that are willing to carry out this transformation, need to expand their understanding on their products' lifecycle. The transformation also sets new requirements for the dependability management processes and for tools and methods used to support that process.

We specifically focus on the machine industry sector in Finland and the needs of manufacturers in that sector, while they are transforming into providers of the life cycle services. The management of the dependability issues of this industry sector is quite challenging due to, for instance, the special characteristics of the working machine use environment. Machines need to be designed for varying loads and demanding operating conditions. At the same time manufactured series are small which limits the sources of reliability data.

In our paper, we address the needs identified in a survey conducted in our research project. Based on the survey, we recognize the perspectives of persons that are representing different organizational positions in the dependability management process. Based on the results of the survey and the complementary industrial interviews, we are able to propose next steps for defining the dependability management processes inside

the machine industry sector. Especially these processes are required for the early stages of the system design. The survey reached 35 professionals from 11 companies. The 35 experienced professionals, chosen by the contact persons of each company, represented the design function (12), product management (5), maintenance and services (9) and reliability management expertise (9). The results indicated that further information is needed regarding certain important perspectives. Therefore an interview study was initiated in order to further explore the current and future challenges related to dependability management at practical level. The interview study was carried out by interviewing 22 persons from four different organizations. The results of the survey and the interviews should support companies when selecting appropriate reliability management tools needed during the different phases of the system design. Based on the results of our research, we find it important to be able to define the process descriptions and practical approaches for dependability management. Thereafter, we are able to focus on the following development steps identified: – Clarification of operational reliability data collection and its usage at various levels of organization – Methods to compare the effects of operating conditions on the machine's reliability performance – Enhanced maintenance program planning – The ability of the component provider to deliver data on component reliability – Development of practical LCC/LCP calculation models for measuring economic effects of dependability.

Safety and Reliability Decision Support System

K. Kolowrocki & J. Soszynska-Budny

Gdynia Maritime University, Poland

ABSTRACT

The contents of the Safety and Reliability Deci

sion Support System—S&RDSS is presented. The

S&RDSS is composed of the methods of complex

technical systems operation processes modeling,

the methods of unknown parameters of complex

technical systems operation, reliability, availability,

safety models identification, the methods of com
plex technical systems reliability, availability and
safety evaluation and prediction, the methods of
complex technical systems reliability, availability
and safety improvement and the methods of com
plex technical systems operation, reliability, availa
bility, safety and cost optimization. The procedure
of S&RDSS usage in reliability analysis, prediction
and optimization of an exemplary system is illus
trated as well.

The aim of this paper is to present and to
apply a guide-book recently developed by the
authors and including the general reliability, avail
ability and safety analytical models of complex
non-repairable and repairable multi-state techni
cal systems related to their operation processes
(Kolowrocki & Soszynska 2010).

Presented in the paper the guide-book Safety
and Reliability Decision Support System—
S&RDSS (Kolowrocki & Soszynska 2010) is
based on the results given in the monograph
(Kolowrocki & Soszynska-Budny 2011) concerned
with the methods of complex technical systems
operation processes modelling, the methods of
complex technical systems reliability, availability

and safety evaluation and prediction, the methods of unknown parameters of complex technical sys tems operation, reliability, availability, safety mod els evaluation, the methods of complex technical systems reliability, availability and safety improve ment and the methods of complex technical sys tems operation, reliability, availability, safety and cost optimization.

The procedure of the S&RDSS usage should start from the scheme-algorithm item S&RDSS 0, and next either to study if it is necessary or to omit its introductory item S&RDSS 1 and to continue with the items S&RDSS 2–15. The user should fol

The model of reusability of multi-component product

A. Jodejko-Pietruczuk & M. Plewa
Wrocław University of Technology, Wroclaw, Poland

ABSTRACT

Reverse logistics understood as the process of man aging reverse flow of materials, in-process inven tory, finished goods and related information has become one of the logicians' key areas of interest. Literature survey that has been done around the theme of the reverse logistics area, allowed to set out this article aims and objectives. The model pre sented in this paper refers to the theme ofreusing of

returned product components inmanufacturing of new products. Great majority of models deal with single–element system or with the assumption that reused elements are as good as new. Proposed model develops the previous ones by releasing both assumptions and gives the base to determine some of reusing policy parameters such as: threshold work time of returned element that can be used again, warranty period for the product contain ing elements which have some history of work, the size of new elements' stock necessary to ful fil production planes. The model is presented and tested for two-element series system, but it is very simple to be developed to the case of x-element, series system.Effects of analytical calculations of the presented model are confirmed and fulfilled by simulation results.

The usage of recovered components in a produc tion decreases production costs but also increases the risk that additional costs occur because of larger amount of returns during warranty period.

The objective of the model is to find the threshold work time T for returned elements that equalises potential cost and profits of the reusing policy:

[E(C WO (T W ,T))–E(C WN (T W))]C O = C B – C R – C M

E C R R R C WO B A B ( ) T T W , ( ) = - ( ) T T W + ( ) T W ( ) T ⎡ ⎣ ⎢ ⎤ ⎦ ⎥ 1 0

E(C WO (T W ,T)) = [1-R B (T W)R A (T W)]C O

n = (1 - R A (min(T,T W)))R B (min(T,T W))

[E(C WO (T W ,T))-E(C WN (T W))]·n·C O =

A methodology to study complex biophysical systems with global

sensitivity analysis

Q.-L. Wu & P.-H. Cournède

INRIA Saclay Ile-de-France, EPI DigiPlante, France

Ecole Centrale Paris, LabMAS, France

J. Bertheloot

INRA, UMR 0462 SAGAH, Beaucouzé Cedex, France

ABSTRACT

Functional-structural models of plant growth (FSPM) aim at describing the structural development of individual plants combined with their eco-physiological functioning (photosynthesis, biomass allocation, in interaction with the environment). The multi-biophysical processes described in FSPMs and their complex interactions make it difficult to identify the key processes, control variables and parameters. The objective of this study is to explore how global Sensitivity Analysis (SA) can help the design of such complex models in two aspects: first, quite classically, in the parameteriza

tion process and secondly by providing new bio
logical insights and diagnosis.

We consider a complex functional-structural model, NEMA (Bertheloot, Cournède, & Andrieu 2009), describing Carbon (C) and nitrogen (N) acquisition by a wheat plant as well as C and N distributions between plant organs after flowering. This model has the specificity to integrate physi ological processes governing N economy within plants: root N uptake is modeled following: High Affinity Transport System (HATS) and Low Affin ity Transport System (LATS), and N is distributed between plant organs according to the turnover of the proteins associated to the photosynthetic apparatus. C assimilation is predicted from the N content of each photosynthetic organ. Inputs of Nitrogen fertilizers are fundamental to get high yielding crops and a production of high quality with the required protein content. This required a proper understanding of root N uptake regulation and of N determinism on yield and production. Complex interactions exist between root N uptake, N remobilization to grains, and photosynthesis, whose regulatory mechanisms remain far from clear. In our application, analyses are conducted

using Sobol's method and an efficient computa

tion technique derived from (Saltelli, 2002), and

several outputs of interest are considered. More

A study of uncertainties in active load carrying systems due to scatter

in specifications of piezoelectric actuators

S. Ondoua & H. Hanselka

System Reliability and Machine Acoustics SzM, Technische Universität Darmstadt, Darmstadt, Germany

R. Platz & J. Nuffer

Fraunhofer Institute for Structural Durability and System Reliability LBF, Darmstadt, Germany

ABSTRACT

In this paper, uncertainty in an active load-carrying

system with an inserted single piezoelectric stack

actuator presented in Enß et al. (2010) is investi

gated. The piezoelectric pre-stressed stack actuator

exerts a controlled lateral force on a beam column

critical to buckling to stabilize it against a short

time acting lateral disturbance force.

Generally, mechanical loading, the system's

ambient temperature and components specifica

tions such as actuator maximum free stroke Δl_{max} ,

actuator blocking force F_B , beam stiffness C_S and

beam geometry are typical influences that affect

the system performance. If these influences are

subject to greater scatter, uncertainty occurs and

the system’s performance deviates from its prede

fined manner. Especially uncertainty in controlled

active components like sensitive piezoelectric stack

actuators may lead to the above deviations.

In this work, the focus of investigation lies on

the statistical determination of the influence of

scatter of the piezoelectric actuator’s assumed

blocking force, maximum free stroke, maximum

electric driving voltage capabilities and stiffness

of column on actuator’s force-stroke-performance.

For that, the actuator’s dynamic behavior due to

scatter of actuator’s force F a and stroke Δl A capa

bility is described with the actuator’s force-stroke

diagram, see Figure 1.

Stochastic and estimated uncertainty in the

configuration process of the active system due

to normally and uniformly distributed scatter in

An environmental risk assessment of a contaminated site based

on extended uncertainty analyses

M.F. Milazzo

University of Messina, Messina, Italy

T. Aven

University of Stavanger, Stavanger, Norway

ABSTRACT

In the context of contaminated sites, risk assess
ments have a dual purpose: to determine the level
of contamination and to assess the effectiveness
of remediation measures. Risk assessment is often
defined as the process that estimates the likelihood
of occurrence of adverse effects to humans and
ecological receptors as a result of exposure to haz
ardous chemicals, physical and/or biological agents
(US EPA 1989).

The commonly used risk assessments for such
problems are based on dose-response curves pro
ducing probabilities and expected values. Typi
cally best estimates are produced, and sometimes
also (subjective) probabilities are used to describe
the uncertainties. In the paper we have pointed to
the need for extending these assessments to place
stronger emphasis on uncertainties. The key chal
lenge is to address uncertainties hidden in the
background knowledge (assumptions) that the
probabilities are based on.

A recently developed risk framework (Aven
2010) designed to better reflect such uncertainties
is presented and applied to the case study, a site
whose contamination is due to both past (related
to the handling of chemical fertilisers) and cur

rent activities (related to the existence of a land

fill of mercury sludge). Following this approach,

a set of uncertainty factors are identified and

assessed. The assessments of uncertainty factors

Comparing Ordered Weighted Averaging (OWA) and Copeland score

for composite indicators in the field of security of energy supply

Claudio M. Rocco S.

Universidad Central de Venezuela, Caracas, Venezuela

Stefano Tarantola

Institute of the Protection and Security of the Citizen, JRC, European Commission, Ispra, Italy

Anca Costescu Badea

Ecole Nationale Supérieure de Mines de Saint-Etienne, France

Ricardo Bolado

Institute of Energy, JRC, European Commission, ES Petten—The Netherlands

ABSTRACT

Composite indicators have been used in several

fields as a practical way to synthesize differ

ent attributes or indicators of objects. The basic

idea is to find a proper form of combination or

aggregation rule for the individual indicators using,

in some cases, additional information. In general,

different performance measures based on different

definitions may lead to different rankings of the

countries. This situation could be controversial for a Decision-Maker (DM), whose responsibility is, for example, to achieve a better performance level.

In this paper we compare two procedures to define composite indicators for the security of energy supply in the European Member States (MS), obtained by two different aggregation rules derived from the Group Decision Theory.

In [Badea et al., 2011], the authors proposed a procedure, based on Ordered Weighted Averag ing (OWA) to rank MS using PMs derived from an energy model, assessing different aspects of the security of supply. OWA is a parametric aggrega tion rule, which allows to test both compensatory and non-compensatory aggregations, and to embed weights. PMs are also aggregated by using a simple but efficient procedure, the Copeland Score (CS), a non-parametric ranking technique that does not require any information from the DM.

The security of energy supply is defined as the availability of reliable and affordable supplies of energy. Eight indicators are selected. The data are based on the results obtained with the PRIMES model and published in [EU 2007]. The compari son is made using a data set related to performance

measures for the security of energy supply in the European Member States, for years 2010 and 2030. The results show that the composite ranks from CS have a high correlation with the ranks produced by OWA for a risk neutral DM preference (α = 1). Figure 1 shows simultaneously the comparison between CS and OWA for alpha = 0, 1 and 1000 [Badea et al., 2011]. A simple sensitivity analysis Figure 1. Comparison between countries ranking in 2010: CS vs. OWA: using the optimistic preference (α = 0); the risk neutral preference (α = 1) and using the pessimistic preference (α = 1000). 0 5 10 15 20 25 30 BE BG CZ DK DE EE IE GR ES FR IT CY LV LT LU HU MT NL AT PL PT RO SI SK FI SE UK CS 1000 1 0

shows that CS and OWA with α = 1 have also a

similar behavior when there is uncertainty in the

input data. Finally CS and OWA with α = 1 give

ranking of countries that are more stable.

Badea, AC., Rocco, C.M., Tarantola, S. & Bolado, R.:

Composite indicators for security of energy supply

using ordered weighted averaging. Reliability

Engineering and System Safety (2011) doi:10.1016/j.

ress.2010.12.025. EU 2007: European Energy and Transport, Trends to 2030 – Update 2007, European Commission, DG TREN.

Generalized expressions of reliability of series-parallel

and parallel-series systems using the Transferable Belief Model

Felipe Aguirre, Mohamed Sallak & Walter Schön

Laboratoire Heudiasyc, UMR CNRS 6599, Université de Technologie de Compiègne, France

ABSTRACT

Probability theory is well suited to treat

uncertainties when their origin comes only from the

natural variability of components' failure (aleatory uncertainty). On the other hand, if the uncertainties are due to incompleteness, imprecision or ignorance of the reliability data (epistemic uncertainty), several other theories can be used. The Transferable Belief Model (TBM) (Smets & Kennes 1994) which is an interpretation of the Dempster Shafer theory has been proven as a well suited theory for the treatment of aleatory and epistemic uncertainty in the reliability analysis (Sallak, Schön, & Aguirre 2010, Aguirre, Sallak, & Schön 2010). Nevertheless, past experiences have proven that the computational cost of the TBM based model grows exponentially with the size of the system. Actually, the computational time depends greatly on the size of the system. In the paper it is shown that a system of 8 components takes 10 min, a system of 9 components takes 1 hr and a system

Importance analysis in risk-informed decision-making of changes to Allowed Outage Times addressing uncertainties

S. Martorell, M. Villamizar, J.F. Villanueva & S. Carlos

Department of Chemical and Nuclear Engineering, Universidad Politécnica de Valencia, Valencia, Spain

A.I. Sánchez

Department of Statistics and Operational Research, Universidad Politécnica de Valencia, Valencia, Spain

ABSTRACT

A number of problems have been identified connected to TS that can jeopardize plant safety (Bizzak et al., 1987). The development of PRA (Probabilistic Risk Assessment) and its applica tion since the early 80’s to analyze TS changes has brought the opportunity to review TS consistency from a risk viewpoint, i.e., addressing the impact of the changes on plant safety on the basis of the risk information provided by the PRA, with particular attention to the role of the STI (Surveillance Test Intervals) included within the SR (Surveillance Requirements), and of the AOT (Allowed Outage Times) included within the LCO (Limiting Condi tions for Operation).

Nowadays, regulatory bodies are encouraging the use or PRA where practical, consistent with the state-of-the-art, to support a risk-informed regulatory framework. The US Nuclear Regula tory Commission (NRC) issued RG 1.174 (2002), which is a key element in this framework to sup

Bizzak, D.J., Stella, M.E. & Stukus, J.R. (1987). “Identi fication and Classification of Technical Specification Problems”, EPRI NP-54-75. Electric Power Research Institute.

EPRI 1016737 (2008). Electric Power Research Institute,

“Treatment of Parameter and Model Uncertainty for

Probabilistic Risk Assessments”.

Martorell, S., Villamizar, M., Villanueva, J.F., Carlos, S.
&

Sanchez, A.I. (2010). Risk-Informed decision-making

on changes to Allowed Outage Times addressing

uncertainties. European Safety and Reliability Con

ference (ESREL), Rhodes. RG 1.174 (2002). “An Approach For Using Probabilistic Risk Assessment In Risk-Informed Decisions On Plant-Specific Changes To The Licensing Basis”, USNRC. RG 1.177 (1998). “An Approach For Plant-Specific, Risk-Informed Decision making: Technical Specifications”, USNRC. NUREG 1855 Vol. 1 (2009). “Guidance on the Treatment of Uncertainties Associated with PRAs in RiskInformed Decision Making”, USNRC.

Importance analysis of multi-state system based on structural function

methods

E. Zaitseva & V. Levashenko

University of Žilina, Žilina, Slovakia

ABSTRACT

Binary-State System (BSS) and Multi-State

System (MSS) are basic mathematical model in

reliability analysis. BSS is used allow description of

initial system as system with two state: reliable and

unreliable or functioning and failure. There are a

lot of methods for estimation system based on this

representation. MSS is mathematical model in reli

ability analysis that is used for description system with some (more than two) levels of performance (availability, reliability). MSS allows present the analyzable system in more detail than traditional Binary-State System. The MSS has been used for representation and reliability analysis of systems, such as, the manufacturing, production, water distribution, power generation and gas and oil transportation.

There are different directions for estimation of MSS behaviour. One of them is importance analy sis. Importance analysis is used for MSS reliabil ity estimation depending on the system structure and its components states. Quantification of this is indicated by Importance Measure (IM). They have been widely used as tools for identifying system weaknesses, and to prioritise reliability improve ment activities.

Authors of the paper (Levitin et al., 2003) have been considered basic IM for system with two per formance level and multi-state components and their definitions by output performance measure. The principal approach for calculation in (Levitin et al., 2003) is universal generating function meth ods. In paper (Ramirez-Marquez & Coit 2005)

have been generalized this result for MSS and have

been proposed new type of IM that is named as

composite importance measures. New methods

based on Logical Differential Calculus for impor

tance analysis of MSS have been considered in

paper (Zaitseva 2010) and new type of IM has

been proposed. These measures have been named

as Dynamic Reliability Indices (DRIs).

The mathematical tool of Multiple-Valued Logic

Integrated approach to assessment of risks from VCE’s using phast risk

and FLACS

N.J. Cavanagh & G. Morale

DNV Software, London, UK

ABSTRACT

Accidents like Buncefield and Texas City have put

the risks from explosions high on the agenda of

both regulators and operators. Models like TNO

Multi-Energy and Baker-Strehlow-Tang have been

used extensively in assessing the risks associated

with such facilities. Over recent years, a number

of projects have been completed to provide guid

ance on the application of these models including

the GAME, GAMES and RIGOS joint industry

projects (see for example Cavanagh et al., 2009,

Cavanagh 2010).

However, the calculated overpressure when using these models as part of a QRA has been seen to be highly dependent on the assumptions made when breaking a plant up into a number of regions of congestion and confinement. For example, the well known GAME correlations for the Multi Energy model (Eggen, 1998) relate peak side-on overpressure to specific geometric properties of the congested region and material properties of the flammable gas within the region. These have been seen to be very sensitive to the assumptions made when defining regions of congestion.

CFD sub-models can be used to assess maximum peak side-on overpressure or maximum flame speed for particular congested regions within your plant, as well as evaluating the extent of the region more accurately. Then, using the Multi-Energy or

Monte Carlo and fuzzy interval propagation of hybrid uncertainties

on a risk model for the design of a flood protection dike

P. Baraldi, N. Pedroni, E. Zio & E. Ferrario

Politecnico di Milano, Milan, Italy

A. Pasanisi & M. Couplet

Electricité de France, Chatou, France

ABSTRACT

In risk analysis, uncertainty is conveniently distinguished into two different types: randomness due to inherent variability in the system behavior (aleatory uncertainty) and imprecision due to lack of knowledge and information on the system (epis temic uncertainty) (Helton 2004).

Traditionally, probabilistic distributions have been used to characterize both types of uncer tainty. However, resorting to a probabilistic rep resentation of epistemic uncertainty may not be possible when sufficient data is not available for statistical analysis or information is of qualitative nature (Helton 2004). As a result of the potential limitations associated to a probabilistic repre sentation of epistemic uncertainty under limited information, a number of alternative representa tion frameworks have been proposed (Aven & Zio 2010). Possibility theory, in particular, may be attractive for risk assessment, because of its repre sentation power and its relative mathematical sim plicity. The rationale for using possibility (instead of probability) distributions to describe epistemic uncertainty lies in the fact that a possibility distri bution defines a family of probability distributions (bounded above and below by the so called possi

bility and necessity functions, respectively), which account for the expert's inability to select a single probability distribution and, thus, the imprecision in his/her knowledge of the epistemically uncertain parameters/variables (Baudrit et al., 2006).

In this paper, four methods for constructing possibility distributions are taken into account and a hybrid method, that jointly propagates probabi listic and possibilistic uncertainties combining the Monte Carlo technique with the extension prin ciple of fuzzy set theory (Baudrit et al., 2006), is considered and compared with a pure probabilistic method for uncertainty propagation. The compar ison is carried out with reference to a risk model concerning the design of a protection dike in a resi dential area closely located to a river with potential

Procedures for aggregating experts' knowledge and group decision

model approaches

T.V. Garcez, A.T. de Almeida-Filho & A.T. de Almeida

Federal University of Pernambuco, UFPE, Recife, Brazil

ABSTRACT

When objective information is complete, when there is sufficient historical data or when the stabil ity of the process of generating such data is guar anteed, it is possible to generate probabilities or

probability distributions from these data. But gen
erally, in decision making and risk assessment (Zio,
1996), such information is not always complete or
available, or when there is a need to consider uncer
tainty, experts must quantify their judgments and
generate a subjective probability distribution.
In the event that the decision maker wants to
acquire as much information as possible, he/she
can consult other subjects who have more infor
mation or knowledge, preferably someone who is
skilled in the area of interest (expert), and thus
he/she can make use of multiple experts. Therefore
making use of an expert in the decision-making
process is of fundamental importance.
Winkler et al. (1992) list several reasons why the
knowledge of multiple experts must be combined,
(i) where the combined distribution produces a
better evaluation than an individual distribution
from both the psychological perspective (when it is
expressed that more heads are better than one) or
from the statistical perspective (when the average
of the samples is better than one sample), (ii) the
combined distribution can be thought of as a form
of consensus, (iii) it is more reasonable and practi
cal to use a single distribution probability when a

more thorough analysis is needed.

When the probability distributions represent the respective judgments of several experts, one of the resulting distributions can be “thought” as a consensus of experts’ decisions. Thus, the prob lem of determining this distribution can only be dealt with as a probability distribution consensus/ aggregation /combining problem. (Hampton et al.,

Sensitivity analysis of repetitive shock machine’s vibration energy

J. Wan, B. Chen & Q.T. Wang

College of Basic Education of Command Officer, National University of Defense Technology,

Changsha, China

ABSTRACT

The Repetitive Shock (RS) machine is one of main vibration testing equipments in the fields of Reli ability Enhancement Testing (RET) in recent days. However, the middle and low frequency vibration energy of the RS machine is usually lower, which limits its applications. The sandwich vibration plate is one main part of the RS machine. It is sig nificant to study the influence of vibration plate’s material parameters on the transform character istic of the middle and low frequency energy of pneumatic vibrators, and then choose the proper

material parameters to improve the middle and low frequency vibration energy of the RS machine.

The sandwich vibration plate is made up of four layers from up to down: the first layer is a polymer plate; the second layer is an aluminum alloy plate; the third layer is made up of four aluminum bars fixed around the second plate; and the fourth layer is also an aluminum alloy plate. In this paper, the MSC.Patran and MSC.Nastran softwares are adopted to perform the sensitivity analysis of the middle and low frequency vibration energy on the material parameters of the first layer of the sandwich vibration plate.

Before the sensitivity analysis, the efficiency and precision of the MSC.Nastran software for the dynamic characteristic computation is validated by means of the comparisons of a single layer plate's computational results and the experimental results tested and analyzed by the Brüel & Kjær pulse system and ME's scope system.

The 3-D finite element model of the sandwich vibration plate is established by means of the

Figure 1. Composition of RS machine. Vibration subsystem
Vibration subsystem Assistant equipments

Vibration

plate Pneumatic vibrators

Uncertainty analysis in probabilistic risk assessment: Comparison

of probabilistic and non probabilistic approaches

Dominique Vasseur, Tu Duong Le Duy & Anne Dutfoy

Risk Management Department, Electricity of France R&D, Clamart cedex, France

Laurence Dieulle & Christophe Bérenguer

University of Technology of Troyes, UMR STMR, Institut Charles Delaunay/LM2S,

Troyes Cedex, France

ABSTRACT

In order to better control the safety of its nuclear power plants, EDF developed Probabilistic Safety Assessments (PSA). Such studies involves the development of models that delineate the response of systems and of operators to initiating events that could lead to core damage or a release of radi oactivity to the environment. The development of a PSA consists in building all the possible scenar ios starting from an initiating event and calculating the probability of these scenarios. Each event of a scenario represents the failure (or the success) of a system mission or an operator mission. To allow the quantification of the scenarios, each mission system is modeled using a fault tree. PSA make it possible to evaluate the safety of the plants and to

rank the plants components with regard to their risk contribution. PSA indicators are thus used to make decisions relative to plants design or proce dures modifications, or to maintenance program optimization for example. To get robust decisions, it is necessary to take account of uncertainties in decision making process.

Uncertainties in PRA model are mainly epis temic ones and can be roughly split into two categories: parameter and model uncertainties. Epistemic uncertainty represents lack of knowl edge with respect to the models or to the appropri ate values to use for parameters that are assumed to be fixed but poorly known in the context of a particular analysis. The model uncertainties are

Uncertainty analysis of nanoparticles for cancer photothermal therapy

D. Barchiesi, S. Kessentini & T. Grosges

Université of Technology of Troyes, France

ABSTRACT

The treatment of diseases like cancer is a major societal issue. One of the ways to achieve this goal uses injected metallic nano-particles for burning the diseased tissue. This mode of therapy is known to be efficient, but remains currently in development.

Some constraints have to be fulfilled for actual medical applications. First the particles have to be small enough to be renally eliminated and compat ible for their use in tissues, while maintaining a suf ficient thermal efficiency as well as a reproducible method of fabrication and control of their size. Despite a few papers devoted to their optimiza tion, at our knowledge, neither sensitivity analysis nor study of the propagation of uncertainties, have been conduct to help to focus on the improvement of appropriate engineering process.

The basic operating principle of such metallic particles after embedment in cells, is based on their heating by an adequate illumination which passes through the biological tissues but is highly absorbed by the particles. The conversion of illumination in heating enables the local burning of the target cells. The model of this phenomenon is based initially on the resolution of Maxwell's equations which govern the interaction between light and matter, and the computation of the energy that is absorbed by the metallic particles (Mie's theory).

We propose an analysis of the propagation of uncertainties on the experimental parameters, through the model: the geometrical properties of

the particles (radius and thickness of the metal

coating if they are assumed to be spherical), and

the material characteristics of the involved met

als under illumination (complex optical index as a

function of the illumination wavelength). For this,

we use our former studies of optimization, giving

the best parameters to get the highest temperature

of the particles, and we consider a tolerance on its

acceptable value. Then, we deduce a hypercube of

acceptable parameters space, from realizations of

a boundary adapted Monte-Carlo method. The

Uncertainty analysis via failure domain characterization:
Unrestricted

requirement functions

L.G. Crespo

National Institute of Aerospace, VA, US

S.P. Kenny & D.P. Giesy

NASA Langley Research Center, Hampton, VA, US

ABSTRACT

This paper studies the reliability of a system for

which a parametric mathematical model is avail

able. The acceptability of the system depends upon

its ability to satisfy several design requirements.

These requirements, which are represented by a set

of inequality constraints on selected output met

rics, depend on the uncertain parameter vector p.

The system is deemed acceptable if all inequalities are satisfied. The constraints partition the uncer tain parameter space into two sets, the failure domain, where at least one of them is violated, and the safe domain, where all of them are satis fied. The reliability analysis of a system consists of assessing its ability to satisfy the requirements when p can take on any value from a prescribed set. The most common practice in reliability analy sis is to assume a probabilistic uncertainty model of p and estimate the corresponding probability of failure. Sampling-based approaches (Nieder reiter 1992, Kall and Wallace 1994) and methods based on asymptotic approximations (Rackwitz 2001) are the engines of most (if not all) of the techniques used to estimate this probability. Reliability assessments whose figure of merit is the probability of failure are strongly depend ent on the uncertainty model assumed. Quite often this model is created using engineering judgment, expert opinion, and/or limited observations. The persistent incertitude in the model resulting from this process makes the soundness of the reliability analyses based on failure probabilities question able. Furthermore, the failure probability fails

to describe practically significant features of the

geometry of the failure event. Some of these fea

tures are the separation between any given point

and the failure domain, the location of worst-case

uncertainty combinations, and the geometry of the

Uncertainty assessment of reliability estimates for safety instrumented systems

H. Jin, M.A. Lundteigen & M. Rausand

Department of Production and Quality Engineering, Norwegian University of Science and Technology,

Trondheim, Norway

ABSTRACT

Reliability estimates play a crucial role in decision

making related to design and operation of safety

instrumented systems (SISs). Unfortunately, the

SIS is a highly complex system whose perform

ance can seldom be fully understood. A reliability

estimate is highly influenced by the simplifications

and assumptions about the SIS as well as its oper

ating environment, and therefore always subject to

uncertainty. If the decision-makers are not aware

of the level of uncertainty, they may misinterpret

the results and select a SIS design that is either too

complex or too simple to provide the necessary

risk reduction.

In the context of decision-making related to a SIS, we define uncertainty as a measure of the decisionmaker's lack of confidence in SIS reliability performance. The paper is limited to so-called low-demand systems where the SIS reliability is judged based on its Probability of Failure on Demand (PFD). The PFD is subject to both aleatory and epistemic uncertainty. The focus is given to epistemic part in this paper.

This paper aims to elucidate the issue of uncertainties in relation to the estimation of SIS reliability. A new approach is proposed for (i) how to determine the level of uncertainty and (ii) how to take the uncertainty into account for SIS related decision-making.

Based on its sources, epistemic uncertainty is further divided into completeness, model, and parameter uncertainty. Methods are proposed to account for uncertainty caused by each of these categories. Qualitative assessment is suggested to determine the unknown and known completeness uncertainty level, and their contributions are combined to obtain the overall completeness uncertainty. This uncertainty is given as one out of five uncertainty levels. Model uncertainty is controlled

by using prescribed consensus models. When using

such models, the model uncertainty is considered to

be broadly acceptable and this uncertainty is there

fore not further considered in the decision-making

process. The uncertainty associated with various

input parameters are propagated into the reliability

estimate by means of Monte Carlo simulation. In the proposed approach, the inputs to SIS related decisions are changed from PFD avg to a situation as shown in Fig. 1: A completeness uncertainty level and a uncertainty distribution of the reliability estimate. In order to ease the decision process, we still use a single PFD value for decisions. But it takes into account the epistemic uncertainty. This is achieved by basing the PFD value selection on the completeness uncertainty level. The basic principle is that the higher the uncertainty is, the more conservative the decisions should be, hence more confidence in the selected PFD value. A detailed PFD selection strategy is suggested in Table 1. The proposed approach is illustrated by a case study of a High Integrity Pressure Protection System (HIPPS). The results show that the PFD value for decisions in a very high completeness uncertainty situation is about three times the value when the completeness uncertainty is very low. It is evident that SIS related decisions would be influenced. Therefore we conclude that an uncertainty assessment of the SIS reliability estimates is a valuable additional input in the SIS related decisionmaking process. PFDavg Deci sion Deci sion Consensus models Uncertainty dist. of PFD Uncertain parameters Completeness uncertainty level Without uncertainty assessment With uncertainty assessment Figure 1. Inputs to SIS related decisions. Table 1. Selection of PFD value for decisions. Completeness uncertainty LL L M H HH Percentile in PFD dist. 50 60 70 80 90

Uncertainty propagation methods in dioxin/furans emission estimation models

G. Ripamonti & G. Lonati

DIIAR-Environmental Section—Politecnico di Milano, Milan, Italy

P. Baraldi & F. Cadini

Dipartimento di Energia—Politecnico di Milano, Milan, Italy

E. Zio

Ecole Centrale Paris and Supelec, Paris, France &
Dipartimento di Energia—Politecnico di Milano, Milan, Italy

ABSTRACT

Environmental Impact Assessment (EIA) is

required for public and private projects likely

to have significant impacts on the environment.

Due to its important role as decision-aiding and

informative tool, the EIA procedure must be an

open and transparent process leading to robust

and reproducible outputs.

In this context, the EIA of waste incineration

plants is usually developed with particular regards

to the potential impacts on air quality by means of

the following three main step: i) estimation of the

source atmospheric emissions, ii) estimation of pol

lutant dispersion in the atmosphere, and iii) assess

ment of pollutant concentrations at the receptors.

Unfortunately, uncertainties affect all these three

steps due to the complexity of the environmental

issue, in which scarcity of data and lack of knowl

edge are common practice. In particular, the final

EIA outputs are seriously affected by the uncertainty

of the values of the source emission estimation.

This work, focused on the emission assessment of a planned new waste gasification plant, has been conceived as a preliminary study to understand the applicability of the methods developed to describe uncertain variables to the whole EIA procedure, in order to provide a more realistic and objective description of the environmental impacts.

Probabilistic Methods (PMC) have been developed to describe uncertain variables by Probability Distribution Functions (PDFs) that are then propagated through the model by Monte-Carlo (MC) simulation. However, due to the scarcity of data typical of the environmental context, the analyst is often obliged to force statistically unjustified PDF on data on the basis of his subjective judgement. This subjective and arbitrary view of probability adds not declared assumptions in the analysis, causing a loss of transparency in the procedure.

Recently, various studies have brought evidence that under limited information availability uncertainty may be better described by possibilistic distributions and propagated by fuzzy interval analysis. Hybrid probabilistic-possibilistic MonteCarlo methods (HMC) have been developed to propagate both probabilistic and possibilistic uncertainty representations. In this work both a standard PMC and a HMC method are applied to an uncertainty propagation analysis in an emission estimation model for dioxins and furans (PCDD/Fs) for the new gasification plant. The emission model computes the

emitted PCDD/F mass flow Q based on the PCDD/F concentration C D in the emitted flue gas, and on the flue gas production V F . The PMC method describes the uncertainty in both C D and V F in terms of PDFs and propagates it by a MC sampling simulation. The HMC method combines a MC sampling of the PDF of C D and a fuzzy interval analysis of V F , whose uncertainty is described in terms of a possibilistic distribution due to data scarcity. The analysis shows that the HMC method allows separating the contributions to the output uncertainty due to C D (probabilistic) and V F (possibilistic). In particular, the HMC results define for the PCDD/F mass flow a belief-plausibility band extending by a roughly ±20% around the output distribution provided by the PMC method. The HMC method seems to process and communicate uncertainty more “transparently”, clearly highlighting the contributions that, conversely, are hidden in the single PDF resulting from the PMC method. Furthermore, the information provided by the HMC outputs is more consistent with that available for the input parameters. The satisfactory outcomes of this first study foster future works towards the extension of the HMC method to the remaining stages of the EIA procedure, and in particular to the assessment of the environmental fate of the pollutants and to the human health risk assessment for both carcinogenic and non-carcinogenic pollutants.

Variance based sensitivity analysis of interactive buckling

Z. Kala

Faculty of Civil Engineering, Brno University of Technology, Brno, Czech Republic

ABSTRACT

Steel is a material with high resistance, and

therefore it is made possible for designers to design

light, slender structure. The more a member is slen

der, the more its load-carrying capacity influences

buckling. In systems, it is necessary to solve the sta

bility of the whole structure. The frame structures

represent a typical example of a system consisting

of more members.

The frame structure is characterized by the fact that members influence each other mutually. Interactions among input random imperfections and the influence of both of them on the ultimate limit state of steel frame structures are analyzed in the present paper. The interactions are studied on behalf of the global sensitivity analysis. The objective of these studies is to find how change of boundary conditions becomes evident in the influ ence of input imperfections on the load-carrying capacity. The variance-based method due to Sobol was applied.

In the paper, there is elaborated an analysis of the influence of boundary conditions on the results of sensitivity analysis of I-section symmet ric portal steel plane frames. To be able to study the clear stability problem of systems, frames loaded on the top of columns were solved. Two types of boundary conditions were solved. The first steel frame has rotation and translation fixed boundary conditions of both column ends. The second steel plane frame is similar to previous frame with the exception that there is no rotation restrain at the column ends.

The geometrical beam nonlinear finite element

solution of the load-carrying capacity was applied.

The sensitivity indices were evaluated applying the

LHS method. The sensitivity analysis results show

that the proportion of factors influencing the load

carrying capacity is strongly dependent on bound

ary conditions.

The frames are typical lean-on systems. For the

first frame, load-carrying capacity is significantly

Differential importance measures estimation through Monte Carlo

and importance sampling techniques

S. La Rovere

NIER Ingegneria, Bologna, Italy

P. Vestrucci & M. Sperandii

DIENCA, University of Bologna, Bologna, Italy

ABSTRACT

The assessment of the RAMS (Reliability, Avail

ability, Maintainability and Safety) performances

of systems generally includes the evaluation of

the “importance” of its components and/or of

their “basic parameters”. The computation of the

Importance measures requires the evaluations of

the system performances for different values of the

input variables. It can be seriously time-consuming

if the solution of the model requires the application

of simulation techniques. Specifically, we refer to the estimation of the time-dependent unavailability of systems made up of repairable components, through an Indirect MonteCarlo simulation.

We propose the use of the Importance sampling techniques for the estimation of Differential Importance Measures, through one simulation of the model. All the output variables (system unavailability for different values of the input variables) are computed contemporaneously, on the basis of the same sequence of the components which cause the system state transitions, events type (failure/repair) and transition times for each trial.

The “basic procedure” requires the adoption of the “Forced specific transition” and “Forced transition rate” techniques. A number of analytical calculations substitute a number of simulations, reducing the computational time. A preliminary reduction of the variance on the output variables is obtained.

The presence of redundant components and the typical values of the failure and repair probabilities generally lead to the “rare events” condition. In this case, the “Forced System Transition technique” can be applied, assuring the occurrence of at least a system failure within the (residual) mission time.

Without lose of generality, we refer to a Net

worked system. We describe the procedure to be

applied for the changes in the components (edges)

transition rates, in order to estimate the first order

Differential Importance Measure for components

(edge and user node) and parameters and the Total

order finite change sensitivity index for parameters.

The results coming from the application of the

Importance measures with finite changes: The relationship between

Fussell-Vesely and total order reliability importance

E. Borgonovo

Department of Decision Sciences and ELEUSI, Bocconi University, Milan, Italy

Bocconi University, Italy

C.L. Smith

Department of Risk, Safety and Reliability, Idaho National Laboratory, Idaho Falls, ID, US

ABSTRACT

Importance measures are usually conceived either

for extreme or for small changes. Risk achievement

worth or risk reduction worth provide information

on the effect of a component being always failed

or always working. Fussell-Vesely (FV) quantifies

the fractional contribution to risk of a component

and is, therefore, a status quo risk measure (Cheok

et al.1998). The Birnbaum (Birnbaum 1969) differ
ential (DIM) (Borgonovo and Apostolakis 2001)
and criticality importance measures (Borgonovo
2007) rely on small changes. However, in some
applications, components are subjected to finite
changes (ageing, inspection and maintenance plans
etc.) and one needs to account for interactions
(Borgonovo and Smith 2011). The problem of
incorporating interactions in importance measures
has been addressed in a stream of research extend
ing the Birnbaum and differential importance
measures for including interactions (Armstrong
1995, Zio and Podofillini 2006, Do Van et al. 2008,
Borgonovo 2010, Do Van et al. 2010).

In this work, we study the relationship between
FV and the total order reliability importance
measure (D_T). We look for conditions under which
these two importance measure coincide. Findings
indicate FV is fractional contribution to risk (sta
tus quo), while D_T is a fractional contribution to
risk-change. They coincide if a system is initially in
a state of perfect reliability.

Armstrong, M. (1995). Joint reliability-importance of
elements. IEEE Transactions on Reliability 44 (3),
408–12.

Birnbaum, L. (1969). On the importance of different

elements in a multielement system. Multivariate analy

sis, New York: Academic Press 2. Borgonovo, E. (2007). Differential, criticality and birnbaum importance measures: An application to basic event, groups and sscs in event trees and binary decision diagrams. Reliability Engineering & System Safety 92(10), 1458–1467. Borgonovo, E. (2010). The reliability importance of components and prime implicants in coherent and noncoherent systems including total-order interactions. European Journal of Operational Research 204(3), 485–495. Borgonovo, E. and Apostolakis, G. (2001). A new importance measure for risk-informed decision making. Reliability Engineering & System Safety 72(2), 193–212. Borgonovo, E. and Smith, C. (2011). A study of interactions in the risk assessment of complex engineering systems: An application to space psa. Operati forthcoming. Cheok, M.C., Parry, G.W. and Sherry, R.R. (1998). Use of importance measures in risk-informed regulatory applications. Reliability Engineering & System Safety 60(3), 213–226. Do Van, P., Barros, A. and Berenguer, C. (2008). Reliability importance analysis of markovian systems at steady state using perturbation analysis. Reliability Engineering and Systems Safety 93(1), 1605–1615. Do Van, P., Barros, A. and Berenguer, C. (2010). From differential to difference importance measures for markov reliability models. European Journal of Operational Research 204(3), 513–521. Zio, E. and Podofillini, L. (2006). Accounting for components interactions in the differential importance measure. Reliability Engineering and System Safety 91, 1163–1174.

On imprecision in relation to uncertainty importance measures

R. Flage & T. Aven

University of Stavanger, Norway

P. Baraldi

Polytechnic of Milan, Italy

E. Zio

Ecole Centrale Paris and Supelec, France

Polytechnic of Milan, Italy

ABSTRACT

A number of Uncertainty Importance Measures (UIMs) have been proposed in the literature to extend classical risk and reliability importance measures in the presence of epistemic uncertainty; ref. e.g. Aven & Nøkland (2010) and Borgonovo (2006). Uncertainty importance measures typi cally reflect to what degree uncertainty about risk and reliability parameters at the component level influences uncertainty about parameters at the system level. The definition of these measures is typically founded on a Bayesian perspective where subjective probabilities are used to express epis temic uncertainty; hence, they do not reflect the effect of imprecision in probability assignments, as captured by alternative uncertainty representation frameworks such as imprecise probability, possi bility theory and evidence theory. In the present paper we consider the issue of imprecision in relation to uncertainty importance measures. We define a (Relative) Imprecision Removal Impor tance Measure ((R)IRIM) to evaluate the effect of removing imprecision. Two extents of imprecision removal are indicated: reduction to a probabilistic representation (type I) and removal of epistemic

uncertainty (type II), the latter a special case of the former. In the present paper focus is put on type II imprecision removal; as further work we suggest to also consider type I imprecision removal. In a numerical example we consider a system consisting of three independent components, where compo nent 1 and 2 are connected in a parallel configura tion which is again connected to component 3 in a series configuration. Epistemic uncertainty about the availability of each component is described possibilistically as shown in Figure 1. Table 1 shows that the suggested Imprecision Importance Meas ure (IIM) ranks component 3 as the most impor

Uncertainty in importance measures: Developing the Epistemic Risk Achievement Worth

E. Borgonovo

Bocconi University, Italy

C.L. Smith

Idaho National Laboratory, ID, US

ABSTRACT

Reliability importance measures are essential tools to support decision-making in several operational applications (Cheok et al., 1998, Borgonovo and Apostolakis 2001, Borgonovo and Smith 2011, Ramirez-Marquez and Coit 2005).

Risk or Reliability Achievement Worth (RAW) is one of the most widely employed importance measures. RAW is defined as the ratio of the reliability (or risk metric) value attained when a component is failed over the base case value of the reliability. Both the numerator and denominator are typically point estimates. Thus, the current definition of RAW is not reflective of a decision maker's degree of belief (state of information) in the problem at hand, when epistemic uncertainty (Apostolakis 1990, Apostolakis 1995, Patè-Cornell 1996) is present.

Epistemic uncertainty can, however, be considered in two ways. In Modarres and Aggarwal (1996) and Borgonovo (2008) the variability in importance measure results generated by epistemic uncertainty is analyzed. Specifically, in Modarres and Aggarwal (1996) the distribution of importance measures is studied. In Borgonovo (2008) the influence of epistemic uncertainty in the safety categorization of SSCs is studied. In these works, uncertainty analysis is conducted on both the importance measure values and ranking in a Monte Carlo propagation. In other words, one computes the importance measure values for dif

ferent possible realizations x x x M1 2 , ,..., of the

probabilities. In so doing, one is informed about

her/his uncertainty in the ranking.

In this work, we propose an extension of RAW

to the case in which epistemic uncertainty is taken

into consideration. We call the new importance

measure Epistemic RAW (ERAW). ERAW con

siders the effect of the component being down

not only on the reliability point estimate but on

its distribution generated by epistemic uncertainty.

We discuss the properties of the new measure for

Adaptive residual-based maintenance policy for a deteriorating system

in dynamic environment

Xuejing Zhao

School of mathematics and statistics, Lanzhou University, Lanzhou, Gansu, China

Mitra Fouladirad & Christophe Bérenguer

Université de Technologie de Troyes, Institut Charles Delaunay, UMR CNRS 6279, STMR,

Troyes, France

ABSTRACT

Optimal replacement problems for deteriorating

systems have been intensively studied in the past

decades (Wang 2002). Many models are developed

for systems with increasing degradation evolving

in a stationary environment. However in most industrial applications, the system is influenced by different risk factors, which are called explanatory variables (covariates). These variables describe the dynamical environment in the experiments of life science and engineering Singpurwalla (1995). An extensive literature on identification and application of covariates model, including the ory and practical application, has addressed, e.g. Makis & Jardine (1992), Bagdonavicius & Nikulin (2000), Zhao et al. (2010).

This paper investigates the adaptive residual based maintenance policy to utilize the information of the observed covariates state for a monotone deteriorating system. The increments of the degra dation are modeled by a stochastic Gamma proc ess. The covariates process is supposed to be a time-discrete homogeneous Markov chain with finite state space and the covariates effect on the deterioration is modeled by a multiplicative expo nential function.

It is supposed that the system can only be observed by inspections. In this framework, the system is correctively replaced if the deterioration level exceeds a fixed level called failure threshold.

To avoid the failure the system is preventively

replaced if the deterioration level is higher than

the preventive threshold but still lower than the

corrective threshold. Replacements take place only

in inspection times and a non-periodic inspection

An adaptive sequential maintenance decision for a deteriorating system

with covariates and maintenance constraints

Elias Khoury, Estelle Deloux, Antoine Grall & Christophe Bérenguer

Institut Charles Delaunay and STMR UMR CNRS 6279—Université de Technologie de Troyes, Troyes, France

ABSTRACT

In the last decades, the interest of decision making

in maintenance has increased in order to reduce

the associated costs and/or improve the durability

and the reliability of a system. Intensive research

activity on maintenance modeling has produced

a lot of models for optimizing its scheduling.

Condition-based maintenance (Wang 2002) is par

ticulary efficient in terms of economical benefits

and also in terms of system safety performance

for a gradually deteriorating system when a condi

tion variable is measurable. Actually, the pronos

tic is the prediction about the future state of the

system. The most used pronostic is to predict how

much time is left before a failure occurs (Jardine

et al., 2006). This time is usually called Residual Useful Lifetime (RUL). The information about the actual condition of the system and the environment in which it evolves can be both used in pronostic. The condition-based maintenance combined to the pronostic leads to the predictive maintenance approach that would be more efficient, however, research about it is still limited (You et al., 2010). The main objective of this paper is to develop a predictive maintenance policy based on all the available information on the system and its environment.

In this context, we consider a gradually deteriorating system operating under an uncertain environment that impacts the degradation. The system is continuously monitored and it is assumed that its degradation level is always available. The system is subject to constraints, maintenance actions can not be planned at any time (Dekker and Dijkstra 1992), it is possible only at fixed times called “maintenance opportunities”. This corresponds to several cases for example aeronautic field, nuclear facilities, off-shore firms, etc. The information on the future environment and the upcoming maintenance opportunities is available, it should be then

integrated in the maintenance decision model to

provide better performance. However, it is only

Condition-based maintenance strategies for a partially observable

deteriorating system

E. Deloux, M. Fouladirad & C. Bérenguer

Université de Technologie de Troyes, Institut Charles Delaunay, UMR CNRS 6279 STMR, Troyes, France

EXTENDED ABSTRACT

In this paper the aim is to propose a condition

based maintenance policy for a deteriorating sys

tem in uenced by the environment in which its is

evolving. The term Condition-Based Maintenance

(CBM) is used to signify the monitoring of a sys

tem for the purpose of maintenance. Information

through monitoring is used to determine the cur

rent health status of a system and based on this

information maintenance actions are performed

to avoid failure. CBM has the potential to greatly

reduce costs by helping to avoid catastrophic fail

ures and by more efficiently determining mainte

nance action times.

One method for performing CBM is by using

measurements on the deterioration level of the

system. For a system subjected to CBM program,

inspections are performed to obtain proper infor

mation about the deterioration state of the sys
tem. In order to avoid a failure occurrence hence a
resulting period of inactivity of the system (dura
tion between the instant of failure and the fol
lowing inspection) a preventive replacement takes
place when the system state enters in a particular
state (or when the deterioration level exceeds a pre
defined threshold).

Most of works concerning the problem of
decision making about monitoring and main
tenance consider monotically deteriorating sys
tems in a statical environment, see (Wang (2002),
Abdel-Hameed (1975), Bérenguer et al., (2003),
van Noortwijk (2009), Dieulle et al., (2003)).
Recently more interest and attention are given to
deterioration models including explanatory vari
ables (covariates). These variables describe the
dynamical environment in the experiments of
life science and engineering and they are often
expressed by the proportional hazards model, see
(Singpur-walla (1995)). These variables can be
some times monitored by inspections and some

Christian Paroissin
Université de Pau et des Pays de l'Adour, Pau, France

Landy Rabehasaina

Universite de de Franche-Comté, Besanon, France

ABSTRACT

Gamma process is one of the most popular stochastic process to model degradation of device in reliability theory (see the review by van Noortwijk). Here we propose and study a gamma process integrating covariates which evolves according to a Markov jump process (which is assumed to be independent of the underlying gamma processes). For lack of simplicity we restrict ourselves to a two-states Markov process (or binary Markov process), but it can be extended to a multi-state Markov process. This Markov process with two states 0 and 1 such that transition rates between 0 and 1 (resp. 1 and 0) is λ (resp. μ), and represents the environment in which the device is used. For instance assume that the device could be used under nominal stress (state 0) or accelerated stress (state 1).

The degradation process (D(t)) is described through the increments of two independent gamma processes whose parameters depend on the state of covariates. If the covariates are in state 0, then the degradation process will be governed by a gamma

process with parameter (§, α 0) and if the covari

ates are in state 1, then the degradation process

will be governed by a gamma process with param

eter (§, α 1) with α 0 α 1 (the average degradation

is larger under higher solicitation use than under

nominal condition).

The first problem we consider is the distribution

of the hitting time T c of a fixed level c by a such

Markov modulated gamma process. Since (D t) has

increasing paths, it follows that it is sufficient to

study the distribution of D(t) for any t 0. We

have obtained an integral representation of the

cumulative distribution function F T c of T c by conditioning on the occupation time Δ 0 (t) of state 0 between the interval [0, t] (see the papers by Sericola for a study of this random variable). Then we have deduced a stochastic order (in the usual sense) between hitting times. Indeed let us denote by T c ( ) 0 the hitting time when μ = 0 and by T c ( ) 1 the hitting time when λ = 0. We proved that T T c st c T st c (1 ( ) 0 ≺ . At least we discuss about a simple problem of optimal maintenance. Assume that the degradation level of a device can be measured only during inspections (i.e. no continuous monitoring). We also assume that at each replacement the device is replaced by a new one or is perfectly repaired (AGAN) and that the replacement/repair duration is negligible. At least replacement occurs only after an inspection (in particular there is no replacement at failure times). Such maintenance scheme is a case of the so-called block replacement policy. Hence one can be interested in determining the optimal inter-inspection delay δ ∗ . To do it, consider the two following different costs: the cost c r for replacing the device and the unavailability cost c u . The asymptotic cost per unit of time is given by: C c c F r u T c ∞ ( ) = + ( ) du ∫ δ δ u . 0 Let us denote δ ∗ the minimum of this cost function. It has been proved that δ ∗ is finite if E[T c] > c r /c

u and is infinite otherwise. We provide a numerical illustration of this problem which leads to conjecture that: δ δ δ ∗ ∗ ∗ . ( ) 1 ( ) 0

Preventive maintenance optimization for a degrading system subject

to shocks with degradation-dependent maintenance costs

M.C. Segovia & P.E. Labeau

Service de Métrologie Nucléaire, Université Libre de Bruxelles, Belgium

ABSTRACT

Systems deteriorate due to continuous usage and

aging, and they might be subject to random shocks

that accelerate their deterioration.

The deterioration of a system entails a reduc

tion of its global performances and eventually

leads to its failure. A system working in a deterio

rated condition might increase operational costs

(because of larger energy consumption, delays in

the production, reduction in productivity …), and

an unplanned replacement also turns out to be

quite costly. To limit the consequences of a system

working in a deteriorated condition, preventive

maintenance is performed.

Classical preventive maintenance policies

(Barlow and Proschan (1996)) are considered in the

study of a system subject to shocks and wear-out

studied by Segovia and Labeau (2010). In the latter

model, shocks cause damage to the system, influ

encing the wear-out process and accelerating its

degradation. The study of the system is achieved by

means of phase-type distributions (Neuts (1981)).

Shocks occur with inter-arrival times following

phase-type distributions and the lifetime of the

system between shocks is also phase-type distrib

uted, its phases referring to the different levels of

degradation of the system. These degradation lev

els are associated to thresholds on the cumulated

damage caused by the successive shocks under

gone by the system. The magnitude of the different

shocks follows a phase-type distribution too. The

system can stand a limited number of shocks: fol

lowing the arrival of the nth one, the system fails.

The system also can fail due to wear-out before the

arrival of the nth shock. Under these assumptions,

the analytical expression of the survival probability

function of the system was obtained.

The present paper extends the previous model by

Statistical modelling of aeronautical turboshaft engines ageing

from field and repair data feedback including preventive maintenance

A. Billon, P. Darfeuil & S. Humbert

Turbomeca, Bordes, France

L. Bordes & C. Paroissin

Université de Pau et des Pays de l'Adour, Pau, France

ABSTRACT

The aim of our studies is to propose a statistical model of turboshaft engines ageing behaviour in order to improve the reliability level assessment. Field and repair data feedback are used to fit our model. This model takes into account components whose failure mechanisms are in competition with respect to a final event and preventive maintenance policy. We want to estimate reliability of the main engine components and, for instance, optimize the preventive maintenance policy.

This article proposes a methodology in order to study the impact of a scheduled maintenance pol icy on one component reliability. First we present the model of one component ageing behaviour whose parameters are estimated from field and repair data feedback. Because these data account preventive maintenance policy, we will propose a method in order to estimate the component ageing behaviour without scheduled maintenance.

We consider a system with a single component whose several failure mechanisms compete with respect to the component failure. The following is

the global methodology proposed to estimate the

preventive maintenance policy impact.

First we estimate the component ageing model

from field and repair data feedback. As a conse

quence, we estimate the ageing model including the

preventive maintenance policy applied in service

(the information about the maintenance operations

is implicitly included in field and repair data feed

back). This model put in competition two Markov

processes whose parameters are estimated with the

maximum likelihood method. Then we define an

ageing model which takes into account a preven

tive maintenance policy. In this new model, the

maintenance is explicitly modelled. To fit param

eters of this new model, we minimize the distance

Special topics: Multiple Criteria Decision Aid (MCDA) and risk analysis This page intentionally left blank

Assessing sustainability and risks: About using a Multi-Criteria

Decision Aid methodology within an organization

M. Merad

INERIS, Verneuil-en-Halatte, France

N. Dechy

IRSN, Fontenay aux Roses, France

F. Marcel

INERIS, Verneuil-en-Halatte, France

ABSTRACT

The Sustainable Development (SD) principle is difficult to implement within the Organization. There is rarely an optimal solution in SD but most frequently a need to build compromises between conflicting aspects and risks such as economic, social and environmental ones. Moreover, information is rarely available and precise. In this paper we have used a Multi-Criteria Decision Aid (MCDA) methodology to cope with these difficulties. MCDA methodology offers the opportunity to avoid monetization of the different dimensions of the SD. These dimensions are not substitutable for one another and all have a role to play. MCDA is a branch of decision theory where actions or alternatives are chosen considering several points of view or criteria, assuming that the Decision Maker (DM) has all the information at his/her disposal concerning the alternatives, i.e., they are fully described by a vector of attributes which is supposed to be known without uncertainty. Two main features of this kind of problem make it difficult to solve. The first one is that attributes describing alternatives are heterogeneous, i.e., they represent different physical (or economical, subjective …)

entities like price, size, color, weight, etc. and may be numerical or not. Hence a first difficulty is to make them commensurable in some sense. The second feature is that points of view or criteria are more or less important to make a decision, and most often they are conflicting or interacting in some way, so that it is not obvious to find how to combine them for reaching a final overall opinion. There are several possible aggregation procedures in MCDA methodology. We have proposed a method to choose an adequate aggregation procedure for SD problems. Outranking approach (i.e., ELECTRE) easily solve the commensurateness problem by making pair wise comparisons. Mono-criterion synthesis approaches (i.e., MAUT approaches) rely on the construction of utility functions, which can be fairly difficult because of commensurateness problems, but then easily reach a final decision by combining utilities or scores of all criteria. In this paper we have implemented two aggregation procedures to rank SD actions: ELECTRE III at a strategical level of decision and MAUT method based on the Choquet integral at an operational level of decision within an expertise Institute. Both methods present advantages and difficulties in a real life situation. The implementation of the ELECTRE III method for the ranking of 22 SD actions offer the opportunity to discuss incomparability situations where the actors involved can discuss their different visions and opinions about the implementation of the SD actions. Let us note that this method is easy to understand and communicate, perhaps due to the fact that the actors involved were familiar with this method that was used in daily situations for risk management and risk analysis problems (i.e., pesticide ranking, industrial accident scenario ranking, etc.). The implementation of the MAUT method based on Choquet integral was very helpful at an operational level. First, the engineer culture

within the Institute is familiar with numbers and they appreciate the results of this method that offer the possibility of having a final score on actions that respect the incommensurability between the criteria. Second, this method offers the possibility of building a real interaction between the Analyst and the DM and testing the coherence on the action ranking. REFERENCE Merad, M. 2010. Aide à la decision et expertise en gestion des risques, ISBN: 978-2-7430-1265-6. Lavoisier.

Expertise and decision-aiding in safety and environment domains: What are the risks?

Myriam Merad

INERIS-BP 2, Verneuil-en-Halatte, France

Wassila Ouerdane

Ecole Centrale Paris—Département Génie Industriel, Châtenay-Malabry Cedex, France

Nicolas Dechy

IRSN, Fontenay aux Roses, France

ABSTRACT

Should the Analyst/Expert consider the impacts of his final recommendations in risk analysis and risk management processes? What are the risks induced by the practice of a decision aid activity in risk analysis and risk management processes? Is it possible to assess the quality of a decision aid activ ity? How can we do that and who has the legitimacy to do that? Such questions were raised by looking at the experience feedback after catastrophe of Texas City 2005, Toulouse 2001, Challenger 1986,

Katrina 2005, … where for each major accident, we can notice that some analysts have provided to some Decision-Maker the necessary information, but these information was considered only after the disaster (see Llory and Montmayeul, 2010).

On one hand, in the decision aiding literature, the analyst has, in general, the aim to support the Decision Maker (DM) in order to: express his pref erences, to structure the decision problem and to frame the final decision. Moreover, the role of the analyst is clearly distinguished from the DM by the fact that the former is involved neither in the decision situation nor in the implementation of the corresponding recommendations. His main objec tive is to help or aid in constructing the criteria of decision and the recommendations and at least to adapt them to the need of the DM, who has the responsibility of the final decision (ex. choosing a propertied mitigation measure).

On the other hand, the safety and environmental scientific and expertise community is often facing tricky and strategic decision situations. Therefore, the necessity to take into account and to reply to such question has been raised. Different answers were distinguished, depending on the discipline, the

role played by the Analyst (s) in risk management

process and to his (their) institutional position (s). For instance, many social scientists, especially those who work on experience feedback and accident investigation have argued in favor of the independency of the Analyst or Board of Investigators (Analysts) (ESReDA, 2009, Dechy and Dien, 2007; Dien et al., 2007) and have pointed the exemplary investigation done by the CAIB 1 about the accident of the space shuttle Columbia in February 1st, 2003. Some others, working in the field of risk perception and risk governance have insisted on the need of a more transparent and democratic process of expertise and decision-making in risk analysis and risk management processes and also on the problem of validation (Renn, 1998; Reid, 1999; Assmuth and Hilde, 2008; Rosqvist, 2010). Indeed, since stakeholders are impacted and affected by the decisions and the conclusions of the expertise, they should be consulted and involved in the decision aid and in the decision processes. Others scientists have focused on the difficulties of coping with the complexity of a decision aid context and situation and choosing the right model (Gertman et al., 1996; Horlick-Jones, 1998; Lagergren, 1998; Amendola, 2001; Fairbrother et al., 2007). This paper will discuss the difficulties of being an Analyst in risk analysis and in risk management processes and proposes new concepts and discussions based on MCDA literature and practices. 1 Columbia Accident Investigation Board.

MCDA tools and risk analysis: The decision deck project

B. Mayag, O. Cailloux & V. Mousseau

Laboratoire de Génie Industriel, École Centrale Paris, Chatenay-Malabry, France

ABSTRACT

MultiCriteria Decision Aid aims at helping one

or more Decision Makers (DMs), guided by one

or more analysts, to prepare and make a decision

where more than one point of view has to be con

sidered. Its objective being not to force a decision

at any cost, MCDA can range from a rational

structuring of the decision problem to the elabora
tion of a decision recommendation. In this context,
many methods and algorithms have been proposed
in the literature. These methods can be schemati
cally divided into two classes of methodologies:

- The outranking methods proposed by the European methodological school. Their objec tive is to build, using pairwise comparisons, a relation on a set of alternatives called the outranking relation, and to exploit it in order to solve MCDA problems (choice, sorting or ranking). To this category belong the ELEC TRE methods (Figueira, Mousseau, and Roy 2005) and PROMETHE (Brans, Mareschal, and Vincke 1984).
- Methods based on the multi-attribute utility theory proposed by the American methodologi cal school (Keeney and Raiffa 1976). The goal of these methods is to build a numerical repre set of alternatives. Methods from this category include MAUT (Dyer 2005), MACBETH (Bana e Costa, Corte, and Vansnick 2005).

The interconnexion between MCDA and risk analysis has been proved. MCDA methods can be used to solve risk analysis problems such as:

• Computation of a risk scale: it can be done by

using MCDA methods as ELECTRE TRI or

by MACBETH methodology when the scale is

quantitative;

• The evaluation of remediation solutions after an

accident.

We present in this paper the Decision Deck (D2)

Parametrize a territorial risk evaluation scale using multiple experts

knowledge through risk assessment examples

Olivier Cailloux & Vincent Mousseau

Laboratoire Génie Industriel, École Centrale Paris, Châtenay-Malabry, France

ABSTRACT

Assessing the risk levels associated with geographi

cal zones involves multiple, and often conflicting,

point of views, relevant for a Decision Maker

(DM), or expert (who is either a single person

or a collegial body): a zone may have a low risk

according to one criterion while being exposed to

a critical risk according to an other one. Examples

of such criteria include the presence of a school or

the percentage of vulnerable persons in the zone.

Associating a risk level to a zone involves aggregat

ing these point of views. This article suggests to use

the tools developed in the domain of multicriteria

decision aiding, which enable a formal approach to that aggregation problem when assessing risk.

Multicriteria (MC) decision aiding aims at recommending a decision which is consistent with the value system of the DM.

Various methodologies have been proposed to support DMs facing a MC decision problem (Keeney and Raiffa 1976, Roy 1996, Bouyssou et al., 2006). In this paper, we consider the multicriteria (MC) sorting problematic to represent qualitative risk assessment models. The MC sorting problematic concerns ordinal classification of alternatives, here, zones, and consists in assigning each alternative to one of some pre-defined categories, here, risk levels ordered from the worst risk level to the less serious one. They can be e.g.: {Critical risk, Medium risk, Low risk}. The MC sorting method used here is a simplified version of ELECTRE TRI.

The assignment of a zone to an appropriate risk level relies on the zone's intrinsic value, i.e. a vector of risk factors associated with the point of views involved in the problem, and a set of subjec sidered DM and known as a MC sorting model.

These preferential parameters may be elicited in a

direct way, but this is often difficult as it requires

the DM to undertand the fine details of their use

in the considered MC sorting method. That is why

Generating quantitative cause-consequence explanation for operator support systems

Akio Gofuku & Masahiro Yonemura

Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan

ABSTRACT

It is important to generate operator support infor

mation for taking a suitable counter action depend

ing on a plant condition. This study proposes a

technique to explain quantitatively the effect of a

counter action by combining a qualitative causal

ity propagation technique [Gofuku 2004] based on

a functional model and a numerical simulation.

The reasoning process of a qualitative reason

ing is basically to trace the influence of a cause

along the connections of symbols in the model.

This process is similar to that of human when

he/she considers and explains how a cause influ

ences. The qualitative reasoning can generate all

possible paths to be influenced by a cause. On the

other hand, a numerical simulation can predict a

future condition of a plant when an anomaly hap

pens or an operator action is taken. Considering the advantages and disadvantages of both a qualitative reasoning and a numerical simulation, this study combines complementally a qualitative reasoning based on an MFM model [Lind 1990, Lind 1994] and a static numerical simulation.

There are several steps in the proposed technique to generate quantitative explanation information of the effects of a counter action. By converting the information of a counter action into suitable formats, a numerical simulation and a qualitative reasoning based on an MFM model are conducted in parallel. The numerical values predicted by a numerical simulator are used to select correct influence propagation paths from the generated paths by the qualitative reasoning based on an MFM model. Then, the numerical values are incorporated into the linguistic explanation on the effect of the counter action along the selected paths.

The applicability of the proposed technique is examined by applying the technique to an oil refinery plant. A static numerical simulator is developed based on the simple mathematical models of

G. Gola

Institute for Energy Technology, Halden, Norway

M. Lind

Technical University of Denmark, Department of Electrical Engineering, Elektrovej, Lyngby, Denmark

H.P.-J. Thunem, A.P.-J. Thunem, E. Wingstedt & D. Roverso

Institute for Energy Technology, Halden, Norway

ABSTRACT

Innovative modeling approaches, techniques, and solutions are needed to support the monitoring and diagnostic requirements of current and future nuclear power plant designs. Longer fuel cycles, reduced staffing, higher intrinsic safety and other related factors are all likely to play an important role in shaping these requirements in the direction of additional flexibility, robustness and automa tion when compared to the systems and techniques that are currently used or being developed today. Online monitoring techniques based on data reconciliation are currently available for early fault detection, i.e., for identifying abnormal residu als between measured and estimated parameters. Nevertheless, the actual analysis and interpreta tion of these results is typically a manual process. If one envisions the likely centralization of condi tion monitoring functions in fleet-wide monitoring

centers, then it becomes evident that supporting functions such as automated diagnosis would become an all-important requisite.

In this paper, a modeling technique known as Multilevel Flow Modeling (MFM) is used within an innovative diagnostic scheme for automating residual analysis in nuclear power plants. MFM based approaches have been successfully applied to diagnostics and to modeling of power systems. The goal-and-function orientation of MFM exploits the principles of qualitative reasoning. MFM presents the plant at different levels of abstraction by defining the functions performed by the components toward the achievement of spe cific goals. Functions and goals are connected via causal relations. The propagation (backwards for fault diagnosis, forwards for prognostic purposes) of the information (e.g., related to system or sensor faults) is carried on by resorting to a model-based reasoning approach. Once the goal-and-function representation is defined, evidence about the plant state is collected and processed by a rule-based causal reasoning (i.e., a system which combines a number of generic rules with the actual casual relationships between functions specified in the MFM model) eventually resulting in the identification of abnormal states of some functions. The physical meaning of the MFM reasoning provides the diagnostic response. Within the novel

diagnostic scheme hereby proposed, a plant monitoring system called TEMPO developed at the Norwegian Institute for Energy Technology based on physical modeling and data reconciliation is used to analyze process measurements and possibly detect abnormal residuals. This information is translated into functional evidence for the MFM model and is used to trigger the reasoning process which eventually leads to the identification of the possible causal paths and associated root causes. The TEMPO-MFM scheme has been applied to diagnosing faults in the secondary loop of the Loviisa-2 Pressurized Water Reactor (PWR) located in Finland. Evidence concerning residuals of different types is collected and translated into the corresponding states of the MFM functions. The reasoning system is triggered by one single abnormal residual and one causal path is identified and physically interpreted. Overall, the on-line diagnostic scheme hereby proposed has indeed proved considerable potential advantages. In fact, the qualitative, linguistic-oriented representation of the plant coupled with the description in terms of goals and functions makes the approach very powerful to handle the diagnosis of complex systems and facilitates the operator communication. Furthermore, the MFM representation of the system can be also used as an off-line tool to analyze faulty scenarios. In this view, triggering events can be manually inserted in the MFM causal reasoning and the resulting cause paths can be investigated for diagnostic purposes.

Reasoning about causes and consequences in Multilevel Flow Models

M. Lind

Department of Electrical Engineering, Technical University of Denmark, Kongens Lyngby, Denmark

ABSTRACT

The paper describes the use of Multilevel Flow

Models (MFM) for reasoning about causes and

consequences in complex dynamic processes. Rea

soning in MFM models derives its power from

representation of process knowledge on several

levels of specification. The principles described in

the paper have been used in the implemented in a model based reasoning system.

The basic ideas of MFM have been developed by the author and his research group and by research groups in several other countries. The research originated in problems of representing complex systems in Human Machine Interfaces for super visory control but has developed into a broader research field dealing with modeling for design and operation of automation systems for safety criti cal complex plants. An up to date introduction to MFM is presented in (Lind, 2011).

MFM has been exploited for solving vari ous diagnosis and control problems (Lind 1981, Fang & Lind 1995, Gofuku & Tanaka 1999, Petersen 2001) and for on-line alarm analysis (Larsson 2002). Applications for fault tree gen eration and risk analysis have been investigated by (Yang & Zhang & Peng & Yan 2007, Rossing & Lind & Jensen & Jørgensen 2009). MFM has been used for a range of industrial processes. Gola et al. (2011) describe an application of MFM for nuclear power plant diagnosis and Rossing et al. (2009) describe an MFM model of a distillation column in a study on risk analysis.

The paper presents novel results showing how

process knowledge is efficiently represented and

used in MFM for reasoning about events. It is

shown that MFM represents process knowledge

on four levels of specification. Three of the lev

els are discussed in detail in the paper and it is

shown that the knowledge encoded on these levels

is efficient for formulation of strategies for rea

Using an agent-oriented framework for supervision, diagnosis

and prognosis applications in advanced automation environments

H.P.-J. Thunem & A.P.-J. Thunem

Institute for Energy Technology, OECD Halden Reactor Project, Norway

M. Lind

Technical University of Denmark, Denmark

ABSTRACT

Building and managing advanced automation

environments for current and future nuclear reac

tor generations requires a full understanding of

the risks and benefits associated with the increased

complexity of dealing with all activities that in one

way or another involve the automated process.

In that regard, the usability aspects of the associ

ated techniques and their contribution to increased

(or decreased) situation awareness for various

human-automation constellations during the mod
ernization of reactor plants or engineering of new
ones need to be investigated and clarified. Equally,
a variety of deficiency modes as well as emergency
scenarios must be carefully assessed.

Available and emerging techniques and tools for
advanced supervision and control are based on a
wide range of different methods for qualitative and
quantitative engineering and analysis purposes. Dif
ferent categories of these methods target different
problem areas. Furthermore, even methods within
the same category can be mutually distinct, as they
might assume certain properties about the systems
on which they are developed to operate. Thus, the
methods and their supporting techniques and tools
need to be applied in combination. To find their
most suitable combinations, it is necessary to inves
tigate their strengths and weaknesses.

This paper describes how an agent-oriented
framework as a common supporting base for vari
ous methodologies and their tools can be used for
Supervision, Diagnosis and Prognosis (SDP) appli
cations in advanced automation environments.

The framework itself is developed on the basis of
a theory assuming that all socio-technical systems

are multi-purpose and made of human, organi
zational and technical agents that together with
their assets can fulfill various purposes, depending
on their different manners of interrelations and
interactions.
The framework, called ShapeShifter, was for
the first time described in a paper published in

Automatic derivation of qualitative and quantitative safety requirements for aircraft systems

P. Bieber, R. Delmas & C. Seguin

Onera Centre de Toulouse, France

M. Bretschneider

Airbus Operations GmbH, Hamburg, Germany

ABSTRACT

Aircraft functions such as “Control the aircraft speed on ground” can be performed thanks to a set of system functions such as “Control wheel brak ing” and “Control thrust reversion”. Safety require ments associated with aircraft functions come in two forms: quantitative requirements, which con strain the mean probability per flight hour of the function loss, and qualitative requirements, which constrain the size of minimal combinations of fail ures leading to the function loss.

At early stages of the development of an air craft, designers have to derive safety requirements for system functions consistently with the aircraft function requirements. This paper describes a method and associated tool which allow to assist the derivation of safety requirements. The approach derives constraint satisfaction problems from the

set of minimal combinations of system function failures leading to an aircraft function loss, which we call a failure condition. These constraint satisfaction problems describe requirements that system functions should enforce in order to satisfy the aircraft function requirements. These problems are solved using either very efficient pseudo-Boolean (linear constraints over variables that take values in 0,1) or MILP (Mixed Integer Linear Programming) solvers. A set of requirements is extracted from the solutions of these constraint satisfaction problems and proposed to the designers. The approach also takes into account user provided constraints that help the tool to focus on more interesting solutions.

With respect to qualitative requirements, the method looks for minimal sets of functions that must be independent in order to enforce the aircraft function qualitative requirements. The problem is formalized as constraints relating the size of each minimal combination of function failures with the independence of these functions. An optimization criterion is defined in order to guide the solver towards solutions that contain a minimal number of pairs of independent system functions. With respect to quantitative requirements, the method allocates

maximal failure rates to system function such that the mean probability of the loss of an aircraft function remains under a given bound. The method also takes into account latent failure (e.g., failures that are not necessarily detected as soon as they occur), through a parameter called the check interval, representing the duration between two consecutive maintenance checks, and allocates maximal check intervals to functions. The problem is formalized as linear constraints on the logarithm of failure rates and the logarithm of functions of check intervals. This simple formalization is enabled by considering the worst-case flight probability of the failure condition, by evenly distributing the bound over all minimal combination of failures, and by assuming that maintenance checks are periodic, synchronized on their first occurrence, and that their possible values form a finite harmonic series. A tool implementing this approach was developed. It offers a graphical user interface that helps the user derive safety requirements. The user selects a number of aircraft failure conditions and defines their severity and probability budget. The user may require that some pairs of system functions shall or shall not be independent. It is also possible to require that some functions have their check intervals allocated from a subset of the default set of allowed values, or that a system function failure rate remains within user defined bounds. The tool then reads the files containing the failure conditions, and generates the constraint satisfaction problems that are then solved using appropriate external tools. When solutions are found, output files are produced, which associate each system function with a maximal probability, a check interval, and a list of other system functions from which the considered function shall be independent. The approach is illustrated on examples taken from aircraft deceleration and electrical generation and distribution applications. These examples are used to perform a first assessment of the method interest and tool performance.

Method of analysis of the relation between serious incident

and accident in air traffic

J. Skorupski

Warsaw University of Technology, Warsaw, Poland

ABSTRACT

Air transport is a complex system combining

advanced technical systems, operators (air traf
fic controllers, pilots) and procedures. All these
elements work in a large spatial dispersion, but
are closely interrelated. Safety is one of the most
important criteria for assessing the transport proc
ess. In air transport the last few years resulted in
attempts to standardize the methods and tools of
risk management, particularly in determining the
acceptable (tolerable, target) level of safety TLS.
This concept is based on the number of accidents
with regard to the volume of traffic. In many coun
tries, however, there have been no air accidents in
recent years. In this case, a reliable determination
of the TLS value is impossible.

In this paper an original approach of solving
this problem is proposed. Analysis of the various
events in air traffic indicates that for the events
classified as serious incidents, there would be suffi
cient occurrence of only one additional conducive
factor, or the termination of only one inhibiting
factor, to a serious incident turned into an acci
dent. This observation is the basis for proposing
the method, which aims to determine the relation
ship between serious incident and accident in air
traffic.

General algorithm of the method is as follows:

1. Development of a model of a serious air traffic

incident as a Petri net.

2. Reduction of the network, which consists in

elimination of places and transitions that do

not affect the transformation of the incident

into accident.

3. Development of the scenarios transforming an

incident into accident.

4. Development of a model of an accident, tak

ing into account reduction of the network and

all the possible scenarios as defined in previous

section. 5. Determination of reachability graph and reachability set of developed Petri net. This stage of the algorithm is also part of a validation process of the model. 6. Reduction of reachability graph, which is also specific for this method and is presented in the paper. 7. Isolation of system states representing the transformation of the incident into accident. 8. Analytical or simulative determination of total probability of accident. Petri nets are used for modelling. They provide a convenient way to describe many types of systems. Especially a lot of applications they found in software engineering, where they are used particularly to describe and analyze concurrent systems. Type of net used, depends on individual case and objective of analysis. In cases where the searched probability depends solely on events of the type of logical conditions (as in the example presented in this paper), or only on events that are characterized by the time-it is preferable to use the analytical variant. In cases when both types of event shave an important role in transforming the incident into an accident-simulation variant is more efficient. Coloured timed Petri nets are an important and convenient tool for analysis of traffic processes in air transport. Research performed has shown its usefulness in analyzing traffic safety problems. They are also efficient modelling tool in other modes of transport. Thanks to this method, on the basis of serious

incidents statistics, one can make a forecast of the number of accidents and thus determine the value of the TLS. As an example illustrating the method a serious air traffic incident, which occurred in August 2007 at Warsaw airport is presented. It shows the opportunities offered by the application of this modelling technique.

Towards model-based functional hazard assessment at aircraft level

S. Maitrehenry & S. Metge

Airbus Operation S.A.S., Toulouse, France

Y. Ait-Ameur

ENSMA-LISI, Poitiers—Futuroscope, France

P. Bieber

Onera, Toulouse, France

ABSTRACT

In recent years, the use of models to assist safety analyses of aircraft systems has increased signifi cantly. Techniques, such as fault tree generation from formal models using AltaRica, are clearly identified in the Airworthiness Recommended Practices (ARP 4754a and ARP 4761), as new means to ensure that proposed architectures fulfil their safety requirements. If we want to extend the use of these models, it seems especially interesting to support preliminary safety analyses performed at aircraft level. We focused on the aircraft FHA (Functional Hazard Assessment) which consists of an exhaustive review of all aircraft functions

in order to identify and classify potential func

tional failures, taking into account the impact of

their effects on the aircraft, its occupants and its

environment. This analysis is crucial to the design

of the aircraft, as it allows the identification of

all safety requirements which will be allocated to

embedded systems.

Therefore, it is crucial to identify, minimize and

solve the potential limitations in the realization

of the aircraft FHA. The two identified areas of

improvement for this analysis are:

- The need to describe explicitly and determine

precisely the effects of a failure scenario from

the contribution of each aircraft level functions

to the fulfilment of the flight.

- The need to search for the most relevant failures

combinations and to determine their effects. This

analysis gains in importance because the embed

ded systems are more and more integrated.

We propose an innovative modelling approach

that takes into account functional dependencies

and flight procedures in order to evaluate the

effects of functional failures. Aircraft architects define reference dynamic models of operational and functional sequences. These models are organized in three layers. The first layer describes the sequence of flight phases, including both nominal phases such as Take-Off (TO) and degraded phases such as, Rejected Take-Off (RTO). The

second layer is the operational level. It models, for each flight phase, the sequence of actions performed by the different actors connected to the aircraft (the pilot, cabin crews, passengers, maintenance crews etc). Finally, the functional layer shows the sequence of aircraft functions needed to perform each action. The reference design models alone are insufficient to analyse dysfunctional behaviour. Therefore, we complete them with a formal description of aircraft behaviour in case of failure. Consequently, the resulting AltaRica models can be simulated to directly visualise the effects of failure scenarios. Furthermore, we can perform automatic analyses with the help of a minimal cut set generator to search for the most relevant failure combinations that should be submitted to the safety analysts. Chemical and process industry This page intentionally left blank

Consequence analysis of SI cycle hydrogen production plant coupled

to a nuclear reactor

T. Ruiz-Sánchez

Centro de Investigación en Energía, Universidad Nacional Autónoma de México, Mexico

J.L. Francois & P.F. Nelson

Departamento de Sistemas Energéticos, Facultad de Ingeniería, Universidad Nacional Autónoma de México, Mexico

M.J. Cruz-Gómez

Departamento de Ingeniería Química, Facultad de Química, Universidad Nacional Autónoma de México, Mexico

ABSTRACT

The use of high temperature heat from nuclear

reactors (e.g., the Very High Temperature Reac

tor, VHTR) to thermochemical cycles would pro

vide another route to hydrogen production with

high efficiencies, ranging from 40 to 60%, depend

ing on the cycle. Currently, a process which has

increased efforts in research and development for hydrogen production is the Sulphur-Iodine (SI) thermochemical cycle. The operation conditions are generally hazardous in nature by virtue of intrinsic chemical properties of materials (hydro gen, acids, sulfides, etc.) or their temperature or pressure of operation or a combination of these. Fire, explosion, hazardous release or a combi nation of these are the hazards associated with materials operations. Aditionally, the coupling of a nuclear power plant to a chemical plant poses new safety issues that must be analyzed in order to design and implement safety measures to protect the facilities, the environment and the population. This safety measures can be: gas sensors location, emergency response plans, plant layout design, etc. In order to know the possible areas affected due to the release simulations were performed with the Phast computer program. In particular, in this work, hydrogen, sulphuric acid, sulphur dioxide, iodine, and hydridic acid were studied. The operating conditions of the SI hydrogen pro duction plant were taken from a combination of the General Atomics preliminary design, and the conditions of the optimized design of the Korea

Advanced Institute of Science & Technology; con

sidering a production of 1 kmol/s of hydrogen.

The weather conditions considered were those of

the Gulf of Mexico. The simulated leak diameters

were 1 inch for toxicity materials and 40 inches for

hydrogen.

The results show that, without considering

Sakaba, N. et al. 2007. Development strategy for

non-nuclear grade hydrogen production system cou

pled with the japan's HTTR. Proc. of ST-NH2. p. 355.

Boston, Massachusetts. United States Nuclear Regulatory Commission (USNRC). 2010. 10 CFR Part. 100.11, Determination of exclusion area, low population zone, and population center distance.

Evaluation of CO2 liquefaction processes with production availability

Youngkyun Seo, Kihong Kim & Daejun Chang

KAIST, Daejeon, Republic of Korea

ABSTRACT

One of the critical issues that the world is facing

is the global warming, mainly caused by carbon

dioxide emissions. One of the feasible solutions

is ship-based CCS (Carbon Capture and Stor

age). Liquefaction should be employed to meet

the economic feasibility. Since there are various

ways to liquefy CO2, evaluation of CO2 liquefac

tion processes is important in choosing the optimal

candidate.

This study comparatively evaluated twelve CO2

liquefaction processes in conceptual design stage.

The LCC (Life Cycle Cost) was estimated for the

candidate processes with production availability

taken into account as well as the CAPEX (Capital

Expenditure) and OPEX (Operational Expendi

ture). Production availability was estimated with

the commercial code, MAROS, based on the

Monte-Carlo simulation method. The failure rates

and the active repair times of the components con

tained in the candidate processes were collected

from the commercially available databases. Pro

duction availability was interpreted as the loss of

production of liquefaction of CO2 and added to

the LCC as being referred to EU-ETS (European

Union Emission Trading Scheme). It was found

that the production availability gave significant

impact on the estimated LCC so that the wrong

conclusion could be drawn on the best process

Figure 1. LCC with alternative processes.

Evaporation rate of acetone: Overview of correlations and sensitivity

analysis

S. Forestier, F. Heymes & G. Dusserre

Ecole des Mines d'Ales, Ales, France

L. Munier & E. Lapébie

Commisariat à l'Energie Atomique et aux Energies Alternatives, Gramat, France

ABSTRACT

Liquid rate of evaporation is one of the major concerns in chemistry industry and finds some applications in industrial risk assessment. This last point motivated researches to develop correlations quantifying it. This paper describes evaporation process from a thermodynamic point of view and from two balance equations. The energy equation describes the enthalpy variation as a function of heat fluxes (from the soil, from the environment around the pool and from heat consumption due to evaporation) presented in Figure 1.

This paper describes the different fluxes and the way to compute them. A special attention is devoted to mass balance equation and mass trans fer coefficient. This coefficient has been the topic of numerous studies and numerous correlations have been developed, so an overview of the different correlations in the literature is realized. The differences and common points between these correlations are developed and both global and local sensitivity analysis is realized for each correlation. The global sensitivity analysis relies on the study of the variance of the answer of the correlation with regards to the variance of the parameters of the correlation. The local sensitivity analysis is based upon the calculation of the differenciate of the correlation. Results of the global sensitivity analysis help determining

the most sensitive parameter while the ones from the local sensitivity analysis describes the shift between real and computed mass loss when the set of data employed differs from its real values.

Figure 1. Validity range of the different correlations.

Numerical simulation of pool fires in oil pipeline system

V.E. Seleznev & V.V. Aleshin

Physical & Technical Center, LLC, Sarov, Nyzhny Novgorod Region, Russia

ABSTRACT

As is well known, combustion of liquid fuel spilled on the terrain adjacent to the region of trunk line (or storage tank) rupture takes place as combus tion of a stream of its vapor in the air. One of the main tasks of the considered approach practical application is to obtain significant upper estimate of potential or analysis of actual consequences of heat damage for facilities adjacent to pool fire site at the rupture region of trunk lines transporting combustible fluids. At that it is necessary to take into consideration not only intensity, but also duration of fire.

The stream of vapor in the flame is maintained by continuous evaporation. The rate of evapora tion is determined by the rate of the heat flow coming from the flame to the liquid fuel. Oxygen required for combustion comes to the reaction

zone from the ambient air. The flame of the com busting liquid fuel can be treated as a diffusion flame. Accordingly, for the purpose of simulation, it is advisable to consider liquid fuel combustion as a specific case of liquid evaporation accompanied by combustion of non-premixed gases (vapor and oxidant).

High accurate simulation of pool fires is an extremely difficult task because of the complex and varied nature of the physical and chemical proc esses involved. As such processes, we can consider formation of a homothermic layer in liquid fuel, boiling and evaporation of the fuel, its splashing, ignition and combustion of liquid fuel vapors. Mechanisms of these processes may vary sub stantially, according to the type of fuel, the con dition and type of the soil at the accident site, weather conditions, etc. The paper describes a method for numerical simulation of combustion of liquid fuels transmitted through trunk lines and/or stored in tanks, with the aim of making estimative calculations of parameters of actual or potential pool fires.

In estimative simulation of fuel evaporation, the following simplifications and assumptions are

A modelling language for the resilience assessment of networked systems of systems

Roberto Filippini

Institute for the Protection and Security of the Citizen, JRC of the European Commission, Ispra, Italy

Andrés Silva

GIB Research Group, Universidad Politécnica de Madrid, Spain

ABSTRACT

Complex civil and industrial installations do not work in isolation, and in many cases they form net works of Systems of Systems (SoS). Examples can be found in modern infrastructures such as power grids, ICT communications and transportation networks (Valerdi 2008, Maier 1998). What mostly distinguish a networked infrastructure from a com plex system is the (non-foresighted) open architec ture. The diverse elements interconnect as long as they possess the requisites of interoperability. Nonetheless, several problems of integration exist when dealing with systems that are heterogeneous. More subtle issues come into play when considering hazards and malfunctions. Issues like interdepend ency and resilience are difficult to model and often beyond the capabilities of traditional tools of sys tem analysis.

This paper presents a language for modeling the resilience of networks and infrastructures, the Infrastructure Resilience-oriented Modeling Lan guage (I®ML). The language is heterarchical and cross-sectoral and broadens the scope of the rep resentation to all players that may take a role in operation scenarios and are relevant to resilience. The language is completed by tools for the analysis of interdependencies and resilience. The method ology is applied to a case study based on the NIST Guidelines for Smart Grid. The result is shown in Figure 1.

I®ML and its tools present analogies with other tools of system analysis, like FMEA, FTA and PRA. However it distinguishes from them, and presents interesting original contributions. One of these stands in the possibility of transforming the I®ML model into a Goal Dependency Struc ture (GDS). A GDS represents interdependencies among the components of an SoS in terms of goals. From the GDS it results straightforward to derive resilience scenarios by assuming that a goal

Ecole Centrale Paris–Supélec, Paris, France

Politecnico di Milano, Italy

R. Piccinelli & G. Sansavini

Politecnico di Milano, Italy

ABSTRACT

A number of Critical Infrastructures (CIs), such as power transmission networks, communication systems, transportation systems and oil/gas supply networks, provide essential services to Society. To guarantee these services, an analysis is neces sary of all the events that can cause damage or dis ruption of CIs; this requires an all-hazard approach that includes infrastructure deterioration and fail ure, natural disasters and accidents, but also malev olent acts (Pollet & Cummins 2009), (Waugh et al., 2004).

CIs are designed to be open and accessible, since they are optimized for efficiency and convenience. Thus, identifying the hazards of both failures and intentional attacks entails a different point of view on system vulnerability (Himes & Horowitz 2004), which includes also a measure of how accessible to terrorists a particular target is and the system damaging sequence of events that may be initiated after this target is attacked (Apostolakis & Lemon

2005).

In this paper, a framework for qualitative All HAZard ANalysis (A-HAZAN) is proposed. Starting from their functional role (task), the components of the CIs are broadly divided in three main categories: user, transmitter and provider,

Analytical model of low-rise building vulnerability curves

G.L. Pita & J.-P. Pinelli

Florida Institute of Technology, Melbourne, FL, US

ABSTRACT

Florida, due to its geographic location, and the ever increasing population on its coastline, is subject to potentially devastating hurricane damage. The failure of econometric models to predict the insured building losses produced by hurricane Andrew, which hit Florida in 1992, led to the adoption of computer-based catastrophe models. The Florida Public Hurricane Loss Model (FPHLM) is part of that change in paradigm providing a state-of the-art loss projection model with a transparent rationale opened to public scrutiny.

The development of vulnerability curves in the FPHLM follows an engineering approach, based on the development of computer models of generic building models, which are then subjected

to Monte Carlo simulation of hurricane loading.

The models integrate external and internal dam

age, and are validated against insurance claim

data. The methodology has been presented at sev

eral past ESREL conferences.

However, this process is laborious and compu

tationally intensive. The objective of this paper is

to propose an alternative single analytical model

for vulnerability curves of the most common commercial-residential buildings. The model is dependant on the building features only. Thus, with the building characteristics, a user can identify the parameters of the analytical model and build a vulnerability curve. The proposed model takes advantage of the extensive library of vulnerability curves from the FPHLM. An analytical model will be fitted to 72 vulnerability curves from the FPHLM of different building types described by 5 parameters: roof type (gable, hip), exterior wall (masonry, wood), number of stories (1 to 3), opening protection (shuttered, unprotected), strength level (strong, medium and weak). The behavior of the analytical model parameters will be explored through regression. A good fit for the model is the 6-parameter Verhulst model coupled with a hyperbolic tangent. The paper will describe the model, and it will provide a structural interpretation for its parameter. Such a model could be a successful complement to more sophisticated and time and resource consuming methods currently used to assess the vulnerability of buildings and other critical infrastructure.

Comparison of vulnerability and reliability analysis of technical

infrastructures

J. Johansson

Lund University Centre for Risk Assessment and Management (LUCRAM), Department of Measurement

Technology and Industrial Electrical Engineering, Lund

University, Lund, Sweden

H. Hassel

Lund University Centre for Risk Assessment and Management (LUCRAM), Department of Fire Safety

Engineering and Systems Safety, Lund University, Lund, Sweden

ABSTRACT

The society depends on reliable and robust services provided by technical infrastructures for its function (de Bruijne & van Eeten, 2007). The impact of large-scale outages due to the inherent vulnerabilities of technical infrastructures has been demonstrated, for example, by the power outage in the U.S. in 2003 and the power outages in Sweden due to the storms Gudrun in January 2005 and Per in January 2007. Two main approaches for acquiring knowledge required for understanding and improving technical infrastructures in this context are reliability analysis and vulnerability analysis (Murray and Grubesic, 2007). Reliability is the ability of a system, sub-system or component to perform a required function. Vulnerability, on the other hand, refers to the ability of a system to withstand specific strains. These two approaches have many similarities but also some differences with respect to what type of information they gen

erate about the system. In the present paper both reliability and vulnerability analyses are carried out and compared with the aim of investigating how the two approaches complement each other.

The analyses are carried out with respect to an electric power system, the IEEE RTS96 reliability test system; however, many of the conclusions can be generalized to other technical infrastructures.

An approach to model infrastructure systems, previously developed by the authors (Johansson and Hassel, 2010), is adopted in this paper. The representation of a system is separated into a structural model and a functional model. The reliability analysis is carried out using a sequential Monte Carlo approach and the aim is to derive a number of commonly used reliability indices. The vulnerability analysis is carried out adopting two different perspectives: global vulnerability and critical component analysis. The two approaches are the compared and contrasted, for example with respect to how well and what types of events and states that the analyses capture. We conclude that reliability analysis primarily provides important information about a system's likely behaviour, e.g., in terms how often outages can be expected per year, the average duration and magnitude of outages, etc. Most commonly the results of reliability analyses are presented as average values of these indices over a long period of time (e.g., over hundreds of years). Events that are estimated to have a low probability, often based on independence assumptions that are not always appropriate, will rarely be captured in a reliability analysis. As such, reliability analyses often provide rather limited

information about high-consequence-low-probability events. Thus the system's ability to withstand rare, unexpected, but still possible stresses and strains, which usually are associated with extreme consequences, are not captured. Vulnerability analysis especially strives to capture low-probability-highconsequence events; therefore, it can provide information which complements reliability information when it comes to a system's ability to withstand large-scale strains and stresses. Even though our best current knowledge and judgment gives rather small probability estimates of these stresses (but they nevertheless tend to happen, e.g., Canadian snow storm in 1998, North American blackout 2003, and earthquake followed by a tsunami in Japan 2011), if the negative consequences are very large then perhaps measures should be taken to ensure a robust and resilient system. At the same time, measures must also be taken for reducing the occurrence of more frequent less impact events, for which reliability analysis provides important information. It is concluded that vulnerability and reliability analysis give complementing crucial insights in securing the essential services to society that our technical infrastructures provide.

de Bruijne, M. & van Eeten, M. (2007). Systems that

Should Have Failed: Critical Infrastructure Protection

in an Institutionally Fragmented Environment, Jour

nal of Contingencies and Crisis Management, 15(1):

18–29.

Johansson, J. & Hassel, H. (2010). An Approach

for Modelling Interdependent Infrastructures in

the Context of Vulnerability Analysis, Reliability

Engineering & System Safety, 95(12): 1335–1344. Murray, A.T. & Grubesic, T.H. (eds.) (2007). Critical Infrastructure Reliability and Vulnerability, Springer, Berlin.

Complexity and vulnerability of Smartgrid systems

E. Kuznetsova & K. Culver

Econoving Chair in Generating Eco-Innovation, University of

Versailles Saint-Quentin-en-Yvelines, France

E. Zio

Chair Systems Science and Energetic Challenge, Ecole Centrale Paris–Supelec, Paris, France

Dipartimento di Energia, Politecnico di Milano, Milan, Italy

ABSTRACT

Smartgrids aim at creating a global, interconnected network of energy actors with improved design, resilient to the vulnerabilities of aging and failing components, natural disasters and human attacks, while at the same time monitoring, managing and optimizing energy flows. In this paper, we look at Smartgrids from the point of view of their com plexity and vulnerability. Such systems evolve from the designer conceptualization to complex struc tures and behaviors through engineering, updat ing and integration processes. At the engineering process level, elements are assembled by design to provide optimal, consistent and reliable operation, as well as functional safety (Ottino, 2004). As the system ‘lives’, its updating and integration occurs by insertion of new technology and extension of capacity to meet service demands with the required performance.

The paper recalls classical characteristics of complex systems, from the point of view of both

topological and behavioral properties, emphasiz

ing their particular relevance for Smartgrids. A cat

egorization of these characteristics is offered into

inherent, challenge-response and acquired groups

(Table 1). This enables identification of primary sources of system vulnerability related to the processes of engineering, updating and integration. Inherent characteristics are amenable to control, therefore, have minimum uncertainty impact on Smartgrid functioning. Challenge-response properties result from the continuous updating process in response to the evolution of the challenges to the Smartgrid function. Due to the uncertain and somewhat unpredictable evolving environment, the challenge-response properties of Smartgrids cannot be guaranteed through design, and their achievement is a challenge itself. The acquired characteristics arise as a consequence of the integration of the system in the complex socioeconomical environment which drives its functioning. This category regroups the major sources of uncertainty on the functioning of Smartgrids. The categorization of Table 1 could allow a preliminary qualitative ranking of the vulnerabilities with respect to the unforeseen character of their potential impact on Smartgrids functionalities, and can guide allocation and protection at the design and operation phases. A preliminary analysis is offered with regards to the methods amenable to be used for analysis of the identified vulnerabilities. REFERENCE Ottino, J.M. (2004). Engineering complex systems. Nature, 427(6973), 399. Retrieved from http://dx.doi. org/10.1038/427399a

Table 1. Categorization of Smartgrids complexity

characteristics. Smartgrids complexity characteristics

Inherent

(engineering) Challenge-response (updating) Acquired (integration)

Architecture Adaptive learning Vague boundaries

Heterogeneity Evolution and growth Selforganization

Self-similarities Self-healing Emergence

Decomposability Attack resistance Chaos multidisciplinary relations

Exploring critical infrastructure interdependency by hybrid simulation approach

Cen Nan, Wolfgang Kröger & Patrick Probst

Laboratory for Safety Analysis, ETH Zurich, Switzerland

ABSTRACT

The study of the interdependencies within and among Critical Infrastructures (CI) is an emerging research field since modern CI are increasingly important as well as automated and interlinked in complex ways to maintain their daily operations. These interdependencies often exert serious influences making CI more vulnerable, which is exacerbated by growing demands for more, often the same resources and timely information. Furthermore, a failure originating from a subsystem of one CI may cascade into other own subsystem(s) and even other infrastructure system(s). This has been demonstrated and highlighted by numerous major incidents such as several large-scale power blackouts (2001-2006). It is indispensible to understand these interdependency issues and tackle them through advanced modeling and simulation techniques.

The importance of preventing or at least mini

mizing negative impacts of cascading failures

caused by interdependencies has been recognized

and accepted, not only by governments but also by

the public, as a topic of CI Protection (CIP). The

purpose of the protection is not just to identify

the cause of failures and prevent them but also to

halt ongoing cascading or escalating events before

they affect other infrastructures. In recent years a

great effort has been devoted to study and analyze

interdependencies through a number of model/

simulation approaches. However, in the presence

of strong interdependencies, traditional math

ematical models such as graph theory often lack

the capability to provide sufficient insights and the

ability to adapt to failures of (sub) systems. A hybrid simulation approach, integrating various modeling/simulation techniques such as Agent Based Modeling (ABM) and High Level Architecture (HLA), is presented in this paper. This approach will not just improve the efficiency/ flexibility of each developed simulator but also decrease the complexity of the overall simulation platform. Each sector or infrastructure specific simulator will only be developed to represent its own system characteristics at the application layer. The information and control commands exchanged between simulators will be interpreted and processed at the communication layer over the network connection. The final goal of this approach is to provide insights into time-based cascading system behaviors as a result of interdependencies and detect vulnerabilities with the help of real-time simulations. Exploratory studies of two interdependent subsystems, i.e., a System Under Control (SUC) and its Supervisory Control and Data Acquisition

(SCADA), both essential parts of the Electric Power Supply System (EPSS), have been successfully conducted to demonstrate the feasibility and applicability of the proposed approach. Several experiments including a feasibility study experiment and a failure propagation experiment have been developed to visualize the propagation of cascading events across CI boundaries and indentify the presence of unknown or unexpected weaknesses of CI related to the interdependencies. Furthermore, a typical substation of the EPSS, comprising components from both SUC and SCADA, is to be analyzed in order to evaluate negative influences on the unavailability of the whole system due to interdependencies.

Failure scenarios in water supply system by means of fault tree analysis

B. Tchorzewska-Cieslak & K. Boryczko

Department of Water Supply and Sewage Systems, Rzeszow University of Technology, Rzeszow, Poland

M. Eid

INSA, Mont-Saint-Aignan, Rouen, France

ABSTRACT

A robust failure analysis should include the entire

water supply system (WSS), from source to tap.

Supply failure may thus occur in the raw water,

the treatment or the distribution. It could be either

quantitative or qualitative failure analysis. The

top failure event is defined as the “interruption in

water supply to the end-user”.

That may result in because of many partial fail

ure modes: the failure of the supply of water, a sec

ondary water pollution in the water-pipe network,

inadequate operational hydraulic conditions in the

network (low velocity rate, loss of flow, loss of pressure), or chemical instability of water.

The main aim of this paper is to present a method for the assessment of different failure scenarios in a given WSS using Fault Tree Analysis (FTA) (Lindhe et al., 2009). Fault tree presents graphically the interrelationships between a potential critical failure events having impact on the occurrence of a specific undesirable event that is called “a top event”.

In drawing up the tree we use the so-called functors (logic gates), specifying, among others, the logical product of events and the logical sum of events.

The paper describes the failure modes in the WSS and treats two examples of application–analysis.

The paper develops a methodology to determine the likelihood of the occurrence of the top undesirable event and to analyze different failure scenarios in the WSS network, taking into account different cause-effect relationships. A formal description of the whole fault tree is developed based on Boolean algebra. The analysis includes two main situations: lack of water and contaminated water supply.

Two examples of fault scenarios were presented, where the final event was top event (threat to life

and health) and where final event was secondary

contamination. Restriction for proposed methods

is necessity of possession exact data about cause

and-effect relationship between failure events of

From pre-crisis to post-crisis going through the peak

A. Laugé, J. Hernantes, L. Labaka & J.M. Sarriegi

Tecnun—University of Navarra, San Sebastián, Guipúzcoa, Spain

ABSTRACT

Managing a crisis is an uninterrupted process.

Before the crisis peak strikes, managers must con

centrate on developing preventive measures since

the potential impact of the crisis might be reduced

through these preparatory policies. When the cri

ses occur, resources and trained staff are needed

urgently in order to face them appropriately

diminishing their consequences and guaranteeing

the high level of resilience of organisations and

services. However, during the crisis peak, there is

no opportunity for building the needed resources

and knowledge if they have not been planned in

advance.

Therefore, for an effective crisis preparation, it

is essential to understand that the crisis does not

only involve the triggering event but it is a proc

ess that starts long time before. Actually, the crisis

lifecycle begins with the pre-crisis period in which crisis managers' main goal is to identify threats and vulnerabilities, reduce weaknesses, and prepare plans for dealing with future risks. The crisis peak phase is the most visible manifestation of the crisis caused by a triggering event and the amount and effectiveness of used resources depend on what has been done in advance, i.e., during the pre-crisis phase.

The aftermath of the most critical phase of the crisis does not mean that the crisis is completely finished. There can also exist longer term conse quences that create long tails of disruptions which have to be properly estimated to develop complete crisis assessments. This period encompasses the return to normal operation where affected equip ments and infrastructures have to be restored. It is also a reflection time to identify the crisis event origin and to evaluate the weaknesses in the crisis management providing feedback to correct mis takes for future crises.

There is the need of merging the knowledge of several agents from different sectors which are involved during a crisis to obtain this holistic perspective. For that reason, during the SEM

POC European project a workshop with the par

Interdependency analysis of CIs in real scenarios

E. Cagno, P. Trucco & M. De Ambroggi

Department of Management, Economics and Industrial Engineering, Politecnico di Milano—Milan, Italy

ABSTRACT

Since the adequate functioning of infrastructures is crucially sustaining societal and economic devel opment, their protection becomes more and more an important issue. Existing approaches related to network vulnerabilities refer to different scientific fields, e.g., physical network modelling, network economics, etc., yet each of them focuses only on one aspect of the problem and do not provide an overview of the different vulnerabilities related to a complex network. In addition, until recently, net work security and service continuity was a matter of concern mainly for the operators. As a conse quence, it is needed to tackle infrastructure protec tion and to have accurate decision support tools to address an issue which is not just technical but also societal.

Moreover some specific additional abilities are required to better match with the specific needs, such as: modelling the interaction between external

events and infrastructure; modelling all the types of interdependencies (Rinaldi et al., 2001); accounting for different types of impact over a wide set of targets (citizens, economic activities, CIs, natural and cultural heritages, etc.; Cagno et al., 2011).

These features have been provided by a new integrated formalism for the functional modelling of vulnerability and interoperability of Critical Infrastructures at regional level (Trucco et al., 2010). The model proved to be able to assess the propagation of impacts due to a wide set of threats. Therefore, the disservice can be propagated within the same infrastructure or to other CIs by means of the interdependence model which is able to model physical, cybernetic, geographic as well as logical interdependencies due to the overall economic and political realities and also the shift of the demand between two infrastructures that can provide the same or fully/partially replaceable service. The model is dynamic, since both the impact of the specific threat on a generic infrastructure node and the inoperability functions are time-dependent.

In the paper is highlighted how the new func

evolution algorithm

E. Zio

Ecole Centrale Paris—Supelec, Paris, France

Politecnico di Milano, Milan, Italy

L.R. Golea & G. Sansavini

Politecnico di Milano, Milan, Italy

ABSTRACT

Electrical grids are Critical Infrastructures (CIs) of fundamental importance for the sustainment of modern Societies. Their protection against random failures and malevolent attacks is a priority for all developed countries.

Current vulnerability analysis focuses on deter mining the most critical elements of the network to prioritize the distribution of reliability and secu rity investments on them. For example, the identi fication of feasible interdiction scenarios can lead to the identification of the network components which, when “hardened”, yield the best improve ment in system security. On the other hand, hard ening the network by modifications of its topology, i.e. via replacement of components or addition of redundancies, can be difficult, slow and expen sive. A more feasible alternative is line switch ing by the system operator following an attack/

failure. Indeed, this is common practice for facing over—or under-voltage situations, line overloads (Granelli et al., 2006), loss and/or cost reduction (Schnyder & Glavitsch, 1990), improving system security (Schnyder & Glavitsch, 1988), or a combi nation of these (Shao & Vittal, 2005). In this view, Network Protection (NP) optimization aims at finding the optimal set of lines to be switched off in order to limit cascade failure consequences. In large networks, this become a combinatorial opti mization problem.

In this paper, we address the NP optimization problem by a Modified version of the Binary Dif ferential Evolution (MBDE) algorithm (Wang et al., 2010). MBDE is a novel binary version of Differential Evolution (DE), developed to tackle binary-coded optimization problems, and thus suit able to solve our discrete combinational optimiza tion problem related to protection. The goodness

Organized Method for Secured Infrastructure Specifications

T. Derode & C. Elegbede
Astrium, Saint-Médard en Jalles, France
E. Garcia & P. Gilibert
Astrium, Les Mureaux, France

ABSTRACT

ASTRIUM Space Transportation as prime con
tractor is in charge of secured infrastructures
design. Among those projects we find safety and
security requirements levels rising from typical
industrial facilities where pyrotechnical devices
are implemented to nuclear facility dedicated to
deterrence forces. Risk analysis is fundamental for
secured infrastructures because of their aim, which
is in the most simplified acceptance, securing haz
ardous processes and/or protecting very sensitive
spots in the most simplified acceptance.
If secured infrastructures design is wanted to be
optimized, the project team must early take into
account a large field of constraints and require
ments steming from the global safety objective.
Moreover, the main difficulty in a risk analysis
which is to ensure an exhaustive analysis approach
must be considered.
During secured infrastructure risk analysis, dif
ficulties may come from the range and heteroge
neousness of sub-systems which compose it and
their own hazards. Of course, a lot of risk analysis
methodologies are available for each sub-system,
as a homogeneous entity, but a high level method
ology focused on the global secured infrastructure

is still needed.

Aims pursued for creating such a high level

methodology are to drive architecture through

drawing and hardening buildings, to allow a global

safety demonstration from safety objectives alloca

tion to compliance achievement, to ensure exhaus

tiveness, to create a link between sub-systems risk

analysis (winning results or giving requirements) and to create organized links with all teams contributing to the development like design specialists or hazardous phenomenon specialists. For that purpose, we present here a robust methodology called MOSIS (Organized Method for Secured Infrastructure Specifications) which is a systematic risk analysis method based on a conceptual and pseudo-geographic mapping of all component of the infrastructure. On this map, we identify all inside hazards sources (fire, explosion, toxic components, radiological materials, etc.) and external hazards sources (lightning, seism, hazardous materials transportations, etc.) and describe them in terms of hazard magnitude and feared event probability, based on the results of usual risk analysis methods or environmental data. Then all the components of the map are described as risk receptors, in terms of stress sensitivity and safety probabilistic objectives, broken down from the infrastructure head requirements. This step of safety objectives allocation may be very difficult early in the design but is highly important. The core of the analysis is then carried out with a matrix showing interactions between hazard sources and risk receptors. MOSIS points out how to involve transversal competences early in the project to perform an efficient risk analysis. The result of this analysis is a list of requirements in terms of architecture constraints (containment) and the complete list of safety design cases to be specified to sizing specialists. This methodology will be profitably carried out from the predesign phase and completed at each stage of the development.

Power grid reliability and vulnerability analysis

Andrija Volkanovski

Reactor Engineering Division, Jožef Stefan Institute,

Ljubljana, Slovenia

Wolfgang Kröger

Laboratory for Safety Analysis, ETH Zürich, Zurich, Switzerland

ABSTRACT

Main function of the power grid is to reliably transfer electrical energy from the generators to the loads. Its can gravely affect modern society directly and/or indirectly by debilitating operation of other infrastructures (Kröger, 2008).

The complexity and exposure to multiple inter nal and external hazards induce the inherent vul nerability of the power grid. Its complexity results from the large number of the constituting elements and non-linear dependency as well as dynamic change of the operational state parameters. The failures of the power grid elements can cascade and accelerate resulting in partial or full power blackout.

A new method for assessment of the reliability of the power grid and identification of most vul nerable elements within grid has been developed and will be presented. The reliability is evaluated through new set of measures of the power grid state including number and percentage of the overloaded interconnections (overhead lines and

transformers) and substations non-nominal volt

ages assessed from the operational parameters.

The parameters are assessed for both the normal

operational state of the power grid with no failed

elements and single failure of all interconnections

within the analyzed power grid. A highly optimized

power flow method (Volkanovski et al., 2009) is

used to assess the grid parameters represented

by the interconnections power flows; substations

voltages will consider the operational limits of the

elements and environmental conditions considered

through ambient temperature.

The reference power grid model has been devel

oped based on the high voltage Swiss transmission

system. The winter and summer snapshot input

files (UCTE, 2007) are used as input data, the local

geographical and meteorological data are used for

definition of the temperature zones. The winter

and summer reference models are modified in

order to develop additional case scenarios for the

assessment of the implications of increase of the

Datacentre European Medicines Agency, London, UK

Andres Silva

GIB Research Group, Facultad de Informatica, Universidad Politécnica de Madrid, Spain

ABSTRACT

With the increasing utilization of Internet serv

ices and cloud computing by most organizations

(both private and public), it is clear that comput

ing is becoming the 5th utility (along with water,

electricity, telephony and gas). These technologies

are used for almost all types of systems, and the

number is increasing, including Critical Infra

structure systems. Even if Critical Infrastructure

systems appear not to rely directly on cloud serv

ices, there may be hidden inter-dependencies. This

is true even for private cloud computing, which

seems more secure. The critical systems can began

in some cases with a clear and simple design, but

evolved as described by Egan to “rafted” networks.

Because they are usually controlled by one or a few

organizations, even when they are complex sys

tems, their dependencies can be understood. The

organization oversees and manages changes. These

CI systems have been affected by the introduction

of new ICT models like global communications,

PCs, the Internet. Even virtualization took more

time to be adopted by Critical systems, due to their strategic nature, but once that these technologies have been proven in other areas, at the end they are introduced as well for different reasons like costs.

A new technology model is happening now with some previous technologies (virtualization, dis tributing and utility computing, web and software services) that are offered in new ways and is called cloud computing.

The organizations are migrating more services to the cloud, this will have impact in their internal complexity and in the reliability of the systems they are offering to the organization itself and their cli ents. Not always this added complexity and associ ated risks to their reliability are seen. As well, when two or more CI systems are interacting, the risks of one can affect to the rest, sharing the risks. We intro duce the terms micro-dependability to define this concept. We will define micro-dependability in the

E. Ciancamerla & M. Minichino

ENEA, Rome, Italy

D. Lefevre

Terna, Rome, Italy

L. Lev

Israelian Electric Corp., Haifa, Israel

ABSTRACT

As evidenced by the occurrence of several cata
strophic events, the link between SCADA (Supervi
sion Control And Data Acquisition) systems and
the reliability of Power grids is well established.
Nowadays, SCADA communication links typi
cally rely on a proprietary network and on an even
public telecommunication network. Such a solution
grants no limits for transmission performances, but
introduces a number of potential failure points that
did not exist previously. Power grids and Telco net
works have a heavy impact on daily life and are typ
ically referred as Critical Infrastructures (CIs), since
their correct operation is essential for the everyday
life of our modern society. Each CI may be sub
jected to various kinds of malfunctions (i.e., logical
misconfigurations, compromised redundancy, pos
sible security breaches, loss of application data,
and degraded services) which may escalate and
propagate among CIs, due to their interdependen
cies. In the present paper, we discuss about depend
ability, performance and rerouting calculations of a
specific service delivered by a Power grid SCADA

system and the impact on the quality of power sup

plied to grid customers. In particular, we focus on

Fault Isolation and System Reconfiguration (FISR)

service that detects and isolates faults in Power

distribution grid and then reconfigures the grid

to supply again isolated customers. In delivering

FISR, SCADA system, Telco network and Power

grid act as a single heterogeneous network.

We combine analytical methods with simulation

schemas, using: i) WNRA, a Weighted Network

Reliability Analyzer, to account dependability

indicators of FISR service (source–destination

connectivity, availability and reliability), by a

probabilistic reasoning; ii) NS2, a discrete event

simulator, to account performance indicators

(packet round trip time, node throughput and

packet dynamical paths). A discrete event simula

tor fits very well to represent SCADA system and Telco network. Here, we use it even to represent Power grid, under specific modeling assumptions. Finally, we compute FISR response time that depends upon the previous dependability and performance indicators. To build realistic models we refer to an actual case study, named Reference scenario, defined with the expertise of Israel Electric Corporation (IEC) in the framework of MICIE EU Project (www.micie.eu). The dependability of FISR service has been investigated considering the network underlying FISR service first as a binary probabilistic network and then as a probabilistic weighted network. S-t connectivity (in terms of minpaths and mincuts), availability and reliability have been computed assuming as the source node in turn the main and the backup SCADA unit of SCADA

control centre and as the destination node one RTU (Remote Terminal Unit) of the RTU set. Service availability/ reliability at time t is intended as the probability of a service to be operational at time t/to be continuous from time 0 to time t. Service availability/ reliability depends upon the interconnected networks required for service delivery. A timely actuation of FISR service, consequential to a permanent failure of the grid, reduces the outage duration and then contributes to keep indicators of quality of power supplied to customers within prefixed values. On the contrary a delayed actuation of FISR service gets worst such indicators. We investigated s-t dynamical path intended as the path of nodes traversed by a packet, from a source to a destination and s-t Round Trip Time intended as the packet transmission time, from a source to a destination plus the ACK time. They have been computed between SCADA Control Centre and RTUs. Then, we investigated FISR response time intended as the time between the occurrence of loss of power supply to customers (due to a grid failure) and the restoration of power supply to customers. We correlated it with the duration of grid outage and the percentage of customers affected by the outage.

Some metrics for assessing the vulnerability of complex networks:

An application to an electric power system

Claudio M. Rocco S.

Universidad Central de Venezuela, Caracas, Venezuela

J.E. Ramirez-Marquez

SysDML, School of Systems and Enterprises, Stevens Institute of Technology, NJ, US

D.E. Salazar A.

DHS Center for Economic and Risk Analysis of Terrorism Events (CREATE), University of Southern

California, Los Angeles, CA, US

ABSTRACT

In this paper the topological behavior of the Italian

electric power network is evaluated. The power system

is modeled as a network G of nodes interconnected by links. Its vulnerability is evaluated through the use of some “classical” and recent metrics developed in the literature. These assessments allow managers and policy-makers aim to minimize the vulnerability of such systems to external events such as natural disas ters or man-made actions by identifying vulnerable and weak points. The analysis of the network reveals that some metrics (e.g., those related to Basic Con nectivity, Spectral Measurements or Spectral Scal ing Method) must be considered from a qualitatively point of view. Indeed their numerical values suggest that the network under study could be decoupled in an “easy way”. Only Importance and Community metrics allow assessing the reduction of the network vulnerability, for example, by adding new links.

The Italian high-voltage (380 kV) electrical transmission network is represented by an undi rected graph of n = 127 nodes and |E| = 171 trans mission elements (links) (Figure 1). The network has been catalogued by [Rosato et al., 2009] as a “scale free” complex network.

Some results from metrics analyzed:

Spectral Gap (G): The first and second largest eigenvalues of the adjacency matrix are λ 1 = 3.46866

and λ 2 = 3.40704. From here, the Spectral Gap is

0.06162, a low value which indicate that the network

has bridges, cut vertices and network bottlenecks.

Algebraic connectivity: λ 2 (G) (the second small

est eigenvalue of the Laplacian matrix) is 0.008497.

This is a small value and could be interpreted as

the network could be decoupled is an easy way.

Statistical analysis: Clustering coefficient (c): 0.179

Betweenness: Mean. 470.58

Network Centralization Index = 23.62%

The need for a new approach to road tunnels risk analysis

K. Kirytopoulos & K. Kazaras

Mechanical Engineering School, National Technical
University of Athens, Greece

ABSTRACT

A sustainable Trans-European Network is regarded

as one of the most crucial elements for economic

growth and creation of employment hence many

efforts have been made in order to develop and

operate safe highway networks. In parallel, with

the improvement of construction technology, road

tunnels have played an important role in develop

ing these new networks. As a result, the number of

road tunnels in Europe has increased rapidly over

the last years. However, this increasing number is

raising upfront an endogenous problem, which is the severity of accidents that may occur. Accidents in road tunnels may lead to heavy consequences for users, the infrastructure itself as well as the environment (Beard & Carvel, 2005).

In this context, the European Commission launched the Directive 2004/54/EC that sets basic requirements for tunnels exceeding 500 m and suggests, apart from the measures imposed based on tunnel length and traffic volume, the implementation of a risk analysis in several cases. However, the EU Directive does not indicate either the method for performing the risk analysis or the criteria for risk acceptance (EC, 2004). Consequently, a wide range of methods have been proposed, most of them based on Quantitative Risk Assessment (QRA; Piarc, 2008). Although QRA contribution to manage safety has been indisputable great in many fields such as nuclear power industry, QRA methods have limitations to capture the overall risk picture of complex socio-technical systems (Leveson, 2004). In such systems human errors during accident conditions, software failures, design errors and the safety culture of the system are not efficiently handled by the current QRA

methods (Apostolakis, 2004). This seems to be

Towards an integrated risk analysis framework for CO 2 Capture,

Transport and Storage

Jaleh Samadi & Emmanuel Garbolino

MINES ParisTech, Sophia Antipolis, France

ABSTRACT

During the history of engineering, models and modeling have been a support tool for engineers, managers and operators to have an overview of how the industrial system works in the lifecycle of a project. Computer models help actors to make decisions in order to maintain the system at a desired level of operation.

The systems we are designing are more and more complex. Such systems' behavior is unpre dictable because of the increasing dynamic com plexity within the system.

In 1956, Jay Forrester created "system dynamics" as a methodology to model complex systems and to study the system's behavior over time. Since then, system dynamics has been applied to various fields, from management to environmental change, politics, economic behavior, medicine, engineer ing, and recently for analyzing accidents and risks (Leveson 2004, Stringfellow 2010, Garbolino et al.,

2010).

In this article, we propose to integrate system dynamics and risk analysis methods in order to develop a dynamic risk analysis framework for Capture, Transport and Storage of CO 2 (CTSC) as an emergent technology.

Although several works have been carried out on risk management of CTSC, most of them involve one subsystem and essentially technical aspects of risk. Lessons learned of the industrial disasters show that a combination of technical, organiza tional and human constituents of risk results in occurrence of accidents (ARIA Inventaire 2010).

Therefore, we recommend to apply system dynam ics as a support for an integrated risk analysis of CTSC complex system. This approach allows us to consider the interconnections of different vari ables, which could make a failure happen in the system.

CTSC is a complex socio-technical system which includes not only three technical compo

Unreliability of water supply networks in the Polish towns based on the field reliability tests

M. Kwietniewski & K. Miszta-Kruk

Warsaw University of Technology, Warsaw, Poland

ABSTRACT

The field reliability test conducted in the real operation conditions is the basic of water net works unreliability assessment. This kind of tests has being conducted in Poland more than 35 years. The newest results of the tests for water networks in the biggest cities in Poland have been presented in the report. Data concerning failures of the pipelines have been gathering in the Geographi cal Information Systems in these cities. The unit intensity of failures (failures/km year) was used for pipeline unreliability/reliability assessment. This kind of index is very useful for assessment and reliability/unreliability different pipeline com parison. In particular the unit intensity of failures allows the preliminary assessment of technical state pipelines, which facilitates making decision about renewal of pipelines. This kind of index plays very important role in the decision making procedure of material selection to network construction. Analysis of the intensity of failures values from the last 10 years operation period of networks showed that Polish networks unreliability decreased close to 3 times. Although the progress intensity of failures of Polish networks is much higher than intensity of failures of networks in many European countries. The influence of the main factors i.e., instability of ground, value and changing of the water pressure in network, pipeline material on failure frequency of the water network was also presented in the paper. This page intentionally left blank Energy This page intentionally left blank

Aligning natural gas industry in an efficient and effective way towards

greenhouse gases emissions

T.V. Alvarenga

Det Norske Veritas Ltda., Rio de Janeiro, Brazil

ABSTRACT

Nations and companies are been forced to find alternative and sustainable energy sources to sup port their economic growth curves. Efforts to sustain these growth trends will be shortly 100% coupled with actions to reduce greenhouse gas emission. Indeed it tends to be a huge challenge, keep consistent growth trends without compromis ing the environment and sustainability principles. Major developments and countries have to foresee reasonable and effective means for dealing with their greenhouse gases emissions without compro mising their own development targets.

An integrated approach for combining Sustain ability and Safety into a RAM analysis, RAM2S (Reliability, Availability, Maintainability, Sustain ability and Safety) based on a powerful reliability simulation tool is proposed. It will allow to evalu ate and to assess an entire facility/system, taking into account alternatives to measure and control, for example, CO 2 and Methane emissions along entire system life-cycle. Part of the engineering

solutions studied relies on the possibility of to cap

ture and store CO 2 , in a real time basis, by connect

ing facilities to storage tanks, subsea reservoirs or

even salt domes.

This integrated approach would allow indus

tries to find out a more cost-effective alternative to

adapt their business into the global warming real

ity, overcoming the inherent greenhouse and global

warming threats.

Thus, it is sharp that the lack of quantitative

numbers clearly showing not only the GHG emis

sions generated by systems or mechanical failures

but also the potential operational losses along the

entire lifespan related to forced shutdowns moti

vated by limitations on the methane, CO 2 or any

GHG emissions might have being crucial to turn

off many potential engineering solutions. Based on

it, many of them could have been already imple

mented or further developed by any natural gas

industries' stakeholders by being then consistently

considered feasible or interesting under a cost and

Paul Scherrer Institut (PSI), Laboratory for Energy Systems Analysis, Villigen PSI, Switzerland

ABSTRACT

The comparative assessment of severe accident risks for major centralized technologies such as fossil (coal, oil, natural gas), hydro and nuclear energy chains is well established. However, corresponding evaluations for new renewables have recently received substantial interest due to their advances in technological development and market penetration.

The current analysis primarily builds upon objective information, for which various risk indicators can be calculated, reflecting a range of societal and environmental impacts of accidental events. The analysis of accidents in the fossil and hydro chains is based on historical data available from the database ENSAD (Energy-related Severe Accident Database), which has been developed and established by the Paul Scherrer Institute (PSI), and since its first release in 1998 has been continuously updated and extended. For nuclear energy a simplified Probabilistic Safety Assessment (PSA) was used to assess site-specific consequences of hypothetical accidents. Among renewable energy technologies, levels of maturity and penetration

are different, which is why for some technologies limited (compared to fossil chains) accident data was available (e.g., Wind, Photovoltaics (PV)), whereas for others estimates were based on approx imations and combined with literature studies and expert judgment due to lack of adequate historical experience (e.g., geothermal energy from Hot Dry Rock (HDR)). Results from comparative accident analysis include:

- Human health effects, i.e., expected fatality rates
- Environmental impacts: expected land contami nation due to radioactive release in the nuclear chain, and oil spills due to an accidental release from a tanker.
- Maximum credible consequences in terms of fatalities, land contamination, and oil spill size of a single accident as a measure of risk aversion.

These six risk indicators were then evaluated for

Modelling and maintenance optimisation for the next generation

of power plants

U. Aha, A. Manig & H.J. Krautz

Brandenburg University of Technology (BTU), Chair of Power Plant Technology, Cottbus, Germany

ABSTRACT

1 INTRODUCTION

In a stable voltage power network, the power pro
vided must equal the power demanded at every
moment. Electrical power can currently only be
stored in very small quantities and therefore power
generation to meet demand is a critical issue in the
energy industry. Due to the current cost pressure in
relation to ongoing savings in all areas, new power
plants must be optimised to the greatest possible
extent during the concept and design phases. The
inevitable fitting and integration of new and exist
ing components and technologies in the next gen
eration of power plants results in new possibilities
for combinations and connections, relating to the
process as well as maintenance, which have to be
evaluated.

2 CONCEPTUAL DESIGN

During the construction of new power plants,
many opportunities exist for the integration of
conventional as well as newly required components.
Classification into unchanged and slightly modi
fied, heavily modified or completely new power
plant components is useful. Through detailed
and structural observation and interconnection
of these components with the help of EBSILON ®
Professional, which enables design, dimensioning,

and calculation of power plant processes, extensive optimisation in the design phase is already possible. In an ongoing project at the Chair of Power Plant Technology, variations of the process in an Oxyfuel power plant are created using EBSILON ® Professional and are subsequently optimised. Modelling of the power plant process is performed not only to derive optimal efficiency, but should also guarantee availability as a result of the suitability and interconnectivity of the components. 3 MAINTENANCE OPTIMISATION To assess maintenance, the software tool INSTRA was programmed. INSTRA uses utility costs to assign every maintenance action a monetary value. Before INSTRA is used, some structural specifications for the power plant being investigated have to be made and a data set with maintenance jobs must be available. In an ongoing project at the Chair of Power Plant Technology, the concept of an Oxyfuel power plant is closely examined. In addition, the conclusions obtained are also transferrable to other types of power plants. By considering variations in the process structural specifications of the power plant, including configuration and the connection of components as well as their dimensions, can be determined. Thanks to cooperation with a local power plant owner, data relating to an Oxyfuel power plant were collected, for example maintenance data. Therefore the application of INSTRA is not only possible at Oxyfuel power plants. 4 CONCLUSIONS If the possibilities for optimisation in relation to the power plant process as well as maintenance are consistently used during the design phase, further essential cost savings associated with power plant operation are achievable. Due to optimisation of these aspects, significant impetus is given to lowering the expected costs of power generation for the next generation of power plants with carbon dioxide capture capabilities.

Numerical monitoring of natural gas delivery discrepancy for cities

energy preparedness

V.E. Seleznev & V.V. Kiselev

Physical & Technical Center, LLC, Sarov, Nyzhny Novgorod Region, Russia

ABSTRACT

In the last 20 years, operation of complex gas distribution systems has been associated with an acute problem of credible commercial account ing of natural gas supply under the deficiency of respective field measurements. This problem has a significant impact on large cities energy prepar edness as natural gas is vital both for citizens and thermal power stations. One of the most promising ways for solving the problem is numerical monitor ing of discrepancy.

Numerical monitoring of the discrepancy is based on a statement (for a specified time gap) and numerical solution of identification problem of a physically proved quasi-steady gas dynamics mode of natural gas transmission through specified gas distribution networks. In large communities, natu ral gas is supplied to the consumers using medium or low pressure ring mains, being several dozen kil ometers long. Gas from the supplier is transmitted to such mains through a Gas Transmission Net works (GTN) after its pressure is reduced by means of a system of gas reducers installed at inlet Gas

Distribution Stations (GDSs). Major parameters

of gas supplied by the gas transportation company

to the seller are also measured at the GDS outlets.

Here, major parameters of natural gas include its

flow rate, pressure and temperature.

Gas from inlet GDSs is delivered to the ring

main via the Connecting Gas Pipelines (CGP) net

work of the gas seller. Consumers receive gas from

the ring mains through outlet CGPs leading from

the ring main to the consumer. In the first approxi

mation, each consumer is considered independent

and provided with gas through one CGP, which is

completely associated with the consumer (called

“associated CGP” as the text goes). Consumer

independence means that the consumer’s gas can

not be delivered to other consumers.

Thus, the Gas Distribution Network (GDN)

Reliability and availability estimation of a photovoltaic system using

Petri networks

R. Laronde, A. Charki & D. Bigaud

LASQUO Laboratory, ISTIA, University of Angers, Angers, France

E.A. Elsayed

Rutgers University, NJ, US

P. Excoffier

GINGER CEBTP, Elancourt, France

ABSTRACT

Photovoltaic (PV) systems are installed all around the world to produce electricity from solar energy. However, photovoltaic modules and systems life time and availability have not been received great attention from researchers. These estimates are important to insure the performance (MTBF, number of outage days per year and steady state availability) of such a system over its life cycle. In this paper, we propose a methodology using Petri networks (Demri et al., 2008) to estimate the reliability and availability of a photovoltaic sys tem. The main advantage of Petri networks is the ability to simulate large systems with a complex configuration of its components, while consider ing many types of lifetime distributions. The main objective of this paper is to take into account the components' degradation and the power evolution of the photovoltaic system.

The system under study is a grid-connected photovoltaic system as shown in Figure 1 and the photovoltaic system Petri network is presented in Figure 2.

The major failure mechanics for crystalline silicon

modules are (Wohlgemuth & Kurtz 2011): Broken

interconnects, broken cells, corrosion, elamination

of encapsulants, encapsulant discoloration,

solder bond failure, broken glass, hot spots,

junction box failures and bypass diode failures.

Some mechanics are due to a degradation which

is possible to follow. To take into account failures

and degradation of PV modules and the other

components of the PV system, the MOCA-RP ©

Backup path calculation in diverse routing considering

shared risk link groups

José Silva

INESC Coimbra, Coimbra, Portugal

Teresa Gomes

Department of Electrical and Computer Engineering,
University of Coimbra, Coimbra, Portugal

INESC Coimbra, Coimbra, Portugal

Carlos Simões

Polytechnic Institute of Viseu, Portugal

INESC Coimbra, Coimbra, Portugal

ABSTRACT

Telecommunication networks must ensure a high

degree of availability and dependability. The path

that carries traffic under normal conditions is

designated Active Path (AP); when a fault occurs

which affects a given protected AP, the traffic in

the AP is then switched to a pre-establish protec
tion path, the Backup Path (BP). A SRLG is a set
of network links that share the same risk of failure.
Two paths are SRLG-diverse (or SRLG-disjoint)
if their links do not have a common SRLG. The
Active Path First (APF) heuristic finds an AP first,
followed by an SRLG-disjoint BP. However once
an AP is found, one may not be able to find an
SRLG-disjoint BP (even though it exists). This is
the so-called trap problem. In this work we will
review the Trap Avoidance (TA) algorithm, for
solving the SRLG diverse routing problem. The
basic idea of TA algorithm is that in order to cir
cumvent avoidable traps one must identify the risky
links that, if selected to be part of an AP, would
make it impossible to obtain the corresponding
SRLG-disjoint BP. A variant for TA algorithm,
designated as Modified TA (MTA) is proposed.
MTA uses new metrics for the link cost of the AP
and BP, which seek to distribute the traffic in the
network. It will be shown that this new variant
outperforms the original TA algorithm in several
relevant performance measures, with our without
backup bandwidth sharing.

Betker, A., Gerlach, C., Jäger, M., Barry, M., Bodamer, S.,

Späth, J., Gauger, C.M. and Kohn, M. (2003, July).

Reference Transport Network Scenario. Technical

report, MultiTeraNet Report. Gomes, T. and Craveirinha, J. (2010). An algorithm for enumerating SRLG diverse path pairs. Journal of Telecommunications and Information Technology (3), 5–12. Gomes, T. and Fernandes, L. (2010, October). Obtaining a SRLG-disjoint path pair of min-sum cost. In J. Rak, D. Tipper, and K. Walkowiak (Eds.), RNDM 2010–2nd International Workshop on Reliable Networks Design and Modeling), Number ISBN: 978-I-4244-7283-3, Moscow, pp. 116–122. Gomes, T., Craveirinha, J. and Jorge, L. (2009). An effective algorithm for obtaining the minimal cost pair of disjoint paths with dual arc costs. Computers & Operations Research 36(5), 1670–1682. Gouveia, L., Patrício, P. and de Sousa, A. (2008). Hop-constrained node survivable network design: An application to MPLS over WDM. Networks and Spatial Economics 8(1), 3–21. Hu, J.Q. (2003, March). Diverse routing in optical mesh networks. IEEE Transactions on Communications 51(3), 489–494. Li, G., Wamg, D., Kalmanek, C. and Doverspike, R. (2003, October). Efficient distributed restoration path selection for shared mesh restoration. IEEE/ACM Transactions on Networking 11(5), 761–771. Rostami, M.J., Khorsandi, S. and Khodaparast, A.A. (2007). CoSE: A SRLG-disjoint routing algorithm. In Proceedings of the Fourth European Conference on Universal Multiser-vice Networks (ECUMN'07), Toulouse, France. Pan, X. and Xiao, G. (2006, January). Heuristics for diverse routing in wavelength-routed networks with shared risk link groups. Photonic Network Communications 11(1), 29–38. Suurballe, J.W. and Tarjan, R.E. (1984). A quick method for finding shortest pairs of disjoint paths. Networks 14(2), 325–336. Todimala, A. and Ramamurthy, B. (2004, October). IMSH: An iterative heuristic for SRLG diverse routing in WDM mesh networks. In 13th International Conference on Computer Communications and Networks, ICCCN'2004, pp. 199–204.

Todimala, A. and Ramamurthy, B. (2005). A heuristic

with bounded guarantee to compute diverse paths

under shared protection in WDM mesh networks.

In IEEE Globlecom 2005, November 28–December 2,

2005, St. Louis, MO, USA, pp. 1915–1919.

Xu, D., Chen, Y., Xiong, Y., Qiao, C. and He, X. (2004).

On find-ing disjoint paths in single and dual link cost

networks. In IEEE INFOCOM 2004, Hong Kong. Xu, D., Xiong,
Y., Qiao, C. and Li, G. (2003, November). Trap avoidance
and protection schemes in networks with shared risk link
groups. Journal of Lightwave Technology 21(11), 2683-2693.

Bottleneck detection and forecasting in Message-Oriented-Middleware

B. Chew & J. Bigham

Queen Mary University of London, London, UK

ABSTRACT

In this paper, we introduce a model that describes

the performances of a broker in Message-Oriented

Middleware. The broker model is used to predict

the performance of the model in different sce

narios. These predictions could be use in detecting

bottlenecks and in gauging appropriate responses

to incipient bottlenecks (Wang 2010).

Previous work in (Gu et al., 2009) has shown

the ability to detect bottlenecks using a com

bination of Markov Models and Naïve Bayes

Classification as well as using Linear Models.

In this work, we use an Autoregressive Moving

Average eXogenous model to predict the behav

iour of the broker.

The ultimate aim is to construct models that

will predict when the broker will bottleneck. These

models can then be used to analyse the behav

iour of the broker by playing different “What-If”

scenarios and supporting decisions regarding

mitigation.

We have built a testbed to perform experiments

on the broker to collect performance data. There

are four software components here, they are: 1) the

test broker, 2) the monitor, 3) a producer, and 4) a

consumer. In our experiments, the single publisher

is referred to as the producer, while the single sub

scriber is referred to as the consumer.

The data from the broker is sampled once a sec

ond. The data is scaled by removing the mean and

the mean adjusted data is used for finding an ARX

model that fits the measurements.

The objectives are to find a model for predicting

Subscriber Rate based on Publisher Rate, and the

broker’s resource requirements based on the load

it has to handle.

The scope of this research is to detect bot

tlenecks at the broker. Bottlenecks are a form of

resource exhaustion. The available CPU and avail

Communications reliability analysis in networked embedded systems

Damien Aza-Vallina, Bruno Denis & Jean-Marc Faure

LURPA, ENS de Cachan, Cachan, France

ABSTRACT

Communication networks have replaced (or will replace in a near future) point-to-point connections in most of embedded systems. Whatever the benefits of this change for cost and flexibility, it implies to develop new methods to compute reliability of communications between the network terminal nodes.

Network components are indeed not merely composed of hardware but contain hardware and software parts. They can then fail in different manners, e.g., fail-silent or babbling. Moreover, some failures may propagate, i.e., the failure of a given component may prevent other components to communicate, even if they are faultless. Hence, classical methods ((Ball1976), (Rosenthal 1977), (Ghasemzadeh, Meinel, & Khanji, 2008)) to compute the reliability of a communication between two terminal nodes, probability that there exists between these two nodes at least one path whose all components are faultless, cannot be applied. These methods are based indeed on components models with only one failure mode and failure propagation is not considered.

The aim of this paper (1) is to tackle out this

issue by proposing a method to compute this prob

ability for networks whose components own several

failure modes and where failures may propagate.

The input data of this method are the components

models, in the form of continuous-time Markov

chains (Cassandras, & Lafortune 2006) which

may include several failure states, and the network

topology, in the form of a nondirected graph where

the nodes represent the network components and

the edges the physical connections between the

components.

For a considered couple of terminal nodes, this

topology is first analyzed so as to find not only all

minimum-length paths between these nodes but

also all components which do not belong to these

paths butcan be sources of failures that propagate

to the components of these paths. This analysis

permits to define, for each minimum-length path

and for each component of the network, the set

Designing a reliable protocol for web services based robots

interconnection

Henrik Madsen

DTU, Informatics, Lyngby, Denmark

Răzvan-Daniel Albu

Faculty of Electrical Engineering and Information

Technology, University of Oradea, Oradea, Romania

Florin Popenţiu-Vlădicescu & Radu Catalin Ţarcă

UNESCO Chair in Information Technologies, University of Oradea, Oradea, Romania

Grigore Albeanu

Spiru Haret University, Bucharest, Romania

ABSTRACT

In this paper we propose a reliable protocol for controlling a robots network. The RRCP is not just a protocol for Internet robot communication but also a complete software package. We illus trate the usage of RRCP on a Khepera III robots network. RRCP is designed over an infrastruc ture based on Web services. By adopting the RRCP, several robots can be operated using the same commands. For example, several robots by different types, supporting this protocol can be moved few meters forward or backward using a single command. The WS-based infrastructure and the Khepera III robots network are shown in the Figure 1. The web server hosts the website and the robot server software. Each robot can be controlled through the website interface. The number of controlled robots can be increased at any time because the solution relays on web serv ices and thus is scalable and interoperable. The

new generation of Khepera can move not just on

a tabletop but it is also designed to move on your

lab floor. Rough floor surfaces, carpets, and even

doorsteps are not a problem for the Khepera III.

The Khepera III architecture provides exceptional

modularity. Many parameters need to be consid

ered for designing a protocol and always there is

more than one solution. The protocol should be

independent from the programming language,

but in practice it is not always true. RRCP takes

a modular approach to connection establishment

with many types of robots. RRCP introduces the

CP (Control Protocol) concept. For each robot

type supported, RRCP invokes a different CP in

the connection establishment phase. For exam

Fabri, D., Lezzi, A. and Leo, T. (2006). ‘The Tiger project,

immersive telelaboratory’, Preprints 7th IFAC Sympo

sium on Advances in Control Education, 21- 23 June

2006, Madrid, 2006.

Flavien Peysson, Mustapha Ouladsine, Rachid Outbib,

Jean-Baptiste Leger, Olivier Myx and Claude

Allemand, JUNE 2009. A Generic Prognostic Meth

odolog Using Damage Trajectory Models, IEEE

transactions on reliability, VOL. 58, NO. 2. Fulya
Altiparmak, Berna Dengiz and Alice E. Smith, MARCH 2009. A
General Neural Network Model for Estimating

Telecommunications Network Reliability, IEEE transactions on reliability, VOL. 58, NO. 1. Peysson, F., Ouladsine, M., Outbib, R., Leger, J.-B., Myx, O. and Allemand, C. Oct. 2008. Damage trajectory analysis based prognostic, in 1st IEEE PHM Conference, Denver, CO, USA.

How to assess telecom service availability risks for crisis organisations?

E. Vriezekolk

Radiocommunications Agency Netherlands, Groningen, The Netherlands

University of Twente, Enschede, The Netherlands

R. Wieringa

University of Twente, The Netherlands

S. Etalle

Eindhoven University of Technology, Eindhoven, The Netherlands

University of Twente, The Netherlands

ABSTRACT

Crisis organisations, such as fire services, dis

aster relief and emergency medical care, nowa

days depend on telecommunications services in

an unprecedented manner. This dependency has

increased since net-centric operations have become

widespread. Unavailability of telecom services dur

ing a crisis may cost lives. In order not to be caught

unprepared, crisis organisations should therefore

perform a risk assessment on availability of their

telecom services.

The purpose of any risk assessment is to provide

decision makers and stakeholders with the neces
sary information on which they can base and justify
their judgement of risk acceptability and choices
for risk treatment. A risk assessment must therefore
accurately and comprehensively describe the risk.
Such a risk assessment must take many factors
into account. Some of these factors can be quanti
fied objectively, but many factors are of a qualita
tive or even subjective nature. We call these latter
factors social factors.

Many risk assessment methods are based on
expected damage, computed as product of prob
ability and effect. This approach can only be used
when effects can be expressed quantitatively; for
social factors this is not possible. Lacking a risk
assessment method, most crisis organisations do
not perform a risk assessment at all, and instead
rely on service level agreements with their telecom
service providers. But service level agreements are
also unsuitable, because they exclude disasters
and other exceptional circumstances: precisely the
type of circumstances in which crisis organisations
must operate.

In this paper we propose a structured way to
include social risk factors into qualitative risk

descriptions. This is an important step towards a

risk assessment method for telecom services used by crisis organisations which we are currently developing. Decision makers face several complications in this domain. The most important one is that, despite their best efforts, external stakeholders may criticize treatment choices, even to the point where they can be emotionally outraged. These protests can harm the decision maker's reputation and trust, and may force the decision maker to choose a different and suboptimal risk treatment. Decision makers therefore need to balance two risks: the risk to the target of assessment, and the risk of public response against their risk treatment choices. To investigate the importance of social risk factors, we performed a broad literature review. This review yielded 27 risk factors, which we grouped into four classes: physical properties, treatment aspects, and shared and personal attitudes. We then examined three examples of telecommunication service availability risks: health risks and exposure limits of electromagnetic fields, triple-play subscriptions, and the Dutch TETRA personal mobile radio system for emergency workers. These cases involved experts as well as the general public, and various causes for unavailability: regulatory restrictions, technical accidents, and conflicts between system design and actual usage. Our conclusion from the literature review and case studies is that classical, purely quantitative risk assessment methods are insufficient for telecom service availability risks for crisis organisations. Instead, their decision makers need risk assessment methods that include both objective, quantitative risk factors and social risk factors: the former are required for scientific rigour, and the latter are required to co-opt public approval. We are currently developing a risk assessment method for telecommunication services based on the insights presented in this paper.

Reliability evaluation of tactical internet based on cloud-mobility model

X. Wang & R. Kang

Department of Reliability and System Engineering, Beihang University, Beijing, China

ABSTRACT

As a military mobile ad-hoc wireless network,

Tactical Internet(TI) is mainly used in the division, brigade and below combat command units of data communication. However, dynamic and unpredict able topology has great influence on the successful completion of military tasks. As one of the most important performance measures of TI, reliability (the capacity of communication during movement) will be expected. However, reliability estimation of TI is to resolve. First, the factors of network reliability and relation between them haven't been integrated, such as mobility, dynamic connectivity, limited bandwidth and energy, path redundancy and components' failure et al., Second, the existing algorithms only consider relatively simple mobile features, assuming the nodes' movements are ran dom and independent of the others. However, in different applications and environment, the nodes' mobile patterns are quite different, and the net work performance index (network throughput, transmission delay, network energy consumption. ect) are all related to the dynamic positions of each node. For example, in civilian ad hoc network envi ronment, each node is independent of each other, and the nodes' movement has a strong random ness. Therefore, random waypoint mobility model

is commonly studied. While in TI, according to

the requirements of tactical tasks, nodes move in

particularly complex formatting, such as linear

queues, invert “V” formatting. Therefore, existing

tactical mobility models are no longer suitable for

the TI reliability.

This paper provides initial findings on Tactical

Internet reliability under tactical formatting, capac

ity and routing constraints. To ensure reliability is

achieved, this work describes the unique character

istics of TI, such as tactical intention, the fuzziness

of upper-level intention and the randomness of

lower-level mobility patterns. Cloud Model from

Artificial Intelligence with Uncertainty is imported

as a key algorithm to deal with the mobility model.

The new methods adapt to cloudy-mobility model

Resilience at interfaces—Improvement of safety and security

in distributed control systems by establishing guidelines
in collaboration

S.O. Johnsen

Norwegian University of Science and Technology (NTNU) and
SINTEF, Trondheim, Norway

ABSTRACT

Process control systems are a key part of industrial

production and in many industries the systems are

a part of the critical infrastructure, such as in the

oil and gas industry. SCADA, supervisory control and data acquisition, is used when we describe a distributed industrial control system, which is a system that monitor and control industrial proc esses. In the oil and gas industry the SCADA sys tems are controlling key production, and must be reliable and safe. Failures in SCADA systems may have large consequences; some incidents are described in Stouffer (2008).

Through networks and technology, SCADA systems are increasingly integrated with Informa tion and Communication Technology systems (ICT). As documented in Stouffer (2008), this creates new vulnerabilities and incidents that may lead to accidents, impacting health, safety, security and environment. To mitigate these challenges, the oil and gas industry in Norway has established a guideline, OLF104 (2006). In this paper we have discussed three key issues:

1. Has safety and security practice been influenced by the guidelines?
2. Has the guidelines increased knowledge?
3. What is suggested future research?

Through collaboration with stakeholders, we have documented how the guideline OLF104 has

impacted internal guiding documents and audits

performed by authorities. The implementation of

the guideline has been seen as a knowledge creat

ing process, as described by Nonaka and Takeuchi

(1995). Interfaces between the different actors,

placed at different geographical sites or in different

organizations have been of key interest.

All 16 issues in the OLF104 guideline has

entered into force from 2009-07-01, and industry

and the authorities use the guideline. The Petro

leum Safety Authority (PSA), is using and refer

Safety aspects of generic real-time embedded software model checking

in the fuzing domain

M. Larisch

University of Applied Sciences Northwestern Switzerland, Switzerland

U. Siebold & I. Häring

Fraunhofer Ernst-Mach-Institut, Germany

ABSTRACT

Software reliability of embedded software of

safety critical hard real-time one-shot devices is an

important issue for safety critical systems with high

risk potential, e.g. in the military fuzing domain.

In particular the avoidance of systematic software

errors of the code is of interest. This paper shows

how the formal software assessment method of

model checking (Clarke 2000) can be applied suc

cessfully in the fuzing domain.

Figure 1 represents the classical approach of

model checking. It is an automatic technique

that checks whether a model M satisfies a prop

erty ϕ. Here, the model M is generated out of a

generic fictitious sample C-code that could be used

in a fuzing system. The small generic real-time

Figure 1. Overview of model checking process used

within the fuzing domain.

Web server's reliability improvements using recurrent neural networks

Henrik Madsen

DTU, Informatics, Lyngby, Denmark

Răzvan-Daniel Albu

University Street, Oradea, Romania

Ioan Felea

University Street, Oradea, Romania

Grigore Albeanu

Spiru Haret University, Bucharest, Romania

Florin Popenţiu-Vlădicescu & Radu Catalin Ţarcă

UNESCO Chair in Information Technologies, University of Oradea, Oradea, Romania

ABSTRACT

In this paper we propose a Neural Network Predic

tion Model (NNPM) for the reliability forecasting, based on the data collected from an experimental Web server system. The results demonstrate the capability of the Recurrent Neural Networks (RNN) for producing satisfactory reliability prediction results. Faults are discovered before they become critical in order to disrupt the normal activity of the web server (H. Madsen a, b et al., 2010). The method is based on the observation that a piece of software traverses multiple degraded states before it fails (G. Albeanu et al., 2010). These degraded states can be monitored and predicted, consequently optimal maintenance actions can be scheduled for improving reliability, under cost constraints (N. Gebraeel a et al., 2009). This paper describes a novel approach of the problem of fault prediction and also presents some results for a test case study. The approach consists of monitoring the activity of the web servers in question in order to define specific relationships. Predicting a fault for severe performance loss of a server requires the measuring of the capacity of a server at any given time. This is highly complex, if not impossible. There are several variables which we can measure on a running system, such as: CPU usage, network usage

and memory usage. For the purpose of time series

prediction, a neural network can be considered

for a general nonlinear mapping, between a sub

set of the past time and future time series values

(N. Gebraeel b et al., 2009).

Studies confirm that NN approaches perform

better than statistical autoregressive moving aver

age (ARMA) methods and in addition Recurrent

Neural Networks (RNN) perform even better for

A modal choice approach for freight transportation considering

accident risks and eco-efficiency

I.C. Leal Jr. & P.A.A. Garcia

Fluminense Federal University, Volta Redonda-RJ, Brazil

Business Administration Department, Human and Social Science Institute, Florida

M.A. D'Agosto

Federal University of Rio de Janeiro, Transport Engineering Program, COPPE/UFRJ, Brazil

ABSTRACT

The freight transportation activities have environ

mental influences and in the case of hazardous

materials these influences are improved due to

its specific characteristics. In this paper one pro

pose the application of a Modal Choice Method

(MCM) considering the risk of accident and meas

ures of eco-efficiency. The intent of the proposed MCM is to establish a priority ranking among the available transportation modes.

Theure use of eco-efficiency indicators gener ates specific measures based on the ratio value of the product or service with the environmental influence and which are represented by equation 1, according to WBCSD (2000).

Eco efficiency Valueof the product or service Environmental Infl

- = uences (1)

We considered transportation experts' opinions to determine the relevant indicators to the evalu ation of the transportation process. The indica tor related to value of service was the revenue freight received and the denominator indicators of environmental influence were: (i) total energy consumption, (ii) emission of greenhouse gases, (iii) lubricating oil discarded and (iv) Risk. After that we gathered, based on historical analysis, the accident frequencies of each transportation mode. Traditionally in Brazil this kind of analysis is not developed considering the risk associated with each transportation mode. In a common sense, direct cost is the main factor which is considered in the decision process. The transport modes have

a different probabilities, severities and risks about

accidents (Table 1).

Due to the fact that we must considers many

criteria in the analysis, a multi-criteria approach

is adopted to establish the priority ranking of the

transportation modes. The multi-criteria approach is based on grey relational analysis–GRA (Deng, 1989, Liu and Lin, 2006). We applied the MCM specifically to analyze the transport for exportation of Brazilian bio-ethanol produced from sugarcane in the country's SouthCentral region. Conuresidering the risk, the results of the priority ranking can be observed in Figure 1. The alternatives are combinations of the four modes considered and that the risk is a weighted average by the distance traveled by each mode on a particular route. Table 1. Probability, severity and risk of accidents for transport modes. Mode Probability of accidents (Accidents /t.km) Severity of accidents (US$/ 1000.t.km) Risk of accidents Pipeline 0,1000 × 10 −7 4,6152 0,4615 × 10 −7 Waterway 0,1022 × 10 −7 0,1818 0,0186 × 10 −7 Railway 0,1348 × 10 −7 0,9594 0,1293 × 10 −7 Roadway 0,5429 × 10 −7 3,5481 1,9263 × 10 −7 – 0,10 0,20 0,30 0,40 0,50 0,60 0,70 0,80 0,90 A1 A10 A7 A8 A9 A4 A3 A2 A5 A6 P e r f o r m a n c e Performance with and without inclusion of risk Without Risk With Risk Figure 1. Classification of transportation alternative.

Observe that when inserting an eco-efficiency

measure that takes into account the revenue

freight received divided by the risk of accidents,

the performance ranking of the alternatives has

changed.

The paper presented shows how a structured

approach can bring benefits to decision-makers in

the selection of transportation modes of danger

ous goods. It was observed that the inclusion of

the risk of accidents in the analysis changes the

performance of the alternatives and influence in

decision making.

The eco-efficiency measures for a modal choice

Adapting the air traffic management safety screening technique

for railways

B. Milius & N. Petrek

Institute of Railway Engineering and System Safety, Technische Universität Braunschweig, Germany

ABSTRACT

Safety is the most important aspect for about every

transportation system. Experience has shown that

all transportation sectors can learn from each

other and often ideas work as well for one system

as for another.

For railways a new EU regulation became rel

evant in 2009 which regulates the risk assessment

process. A rather new concept discusses the signifi

cance of a change as only for significant changes

of the railway system a risk assessment is neces

sary. However, there is very little guidance on how

to identify the significance of a change. The given

criteria are rather fuzzy and leave room for specu

lation. Several suggestions have been made how

the identification process could be done. There

already exist some amendments of the original process made by different groups in the railway sector like national railway agencies, train operators and manufacturers, which should fix some of the known problems.

Beside the amendment of the original process, it could also be useful to learn from rather different concepts, which are already in use in other transportation systems. Such an interesting concept is the Safety Screening Technique (SST). For system changes of the air traffic management system the SST tool was developed which helps to get a preliminary opinion on the potential implications of system changes on the overall safety performance. The method is qualitative, easy to use and rather intuitive. The results are presented in a structured and easy to interpret way.

In order to decide if the SST can be developed into a tool which can be used for the identification of significant changes in the railway sector, it is necessary to analyze the SST taking into account the information given in the EU regulation. Two different approaches are possible. One approach necessities a detailed system analysis. By comparing the results of such an analysis for air traffic man

Improving the reliability/availability of a complex system by an active monitoring based onto “augmentation concept”: Application onto a railway system

J. Gandibleux & L. Cauffriez

Université Lille Nord de France, Université de Valenciennes, Valenciennes, Nord Pas-de-Calais, France

G. Branger

BOMBARDIER Transport France, Crespin, Nord Pas-de-Calais, France

ABSTRACT

This research work deals with design for Reliability, Availability and Maintainability (RAM) in the field of railway transportation. It is a part of the SURFER project (French acronym for “railway active monitoring”), which intends to:

- anticipate the failures influencing the reliability and availability,

- help to efficiently localize failures,

- improve the traceability for a better experience feedback.

The innovative aspect of our approach is the dependability improvement of architecture based onto the “augmentation concept”, which was pro posed by TEMPO PSI team (Sallez, 2010) in the field of product manufacturing.

Let us consider a generic classical component supporting a primary function. The “augmentation concept” consists in integrating a second “non intrusive” function in this component. In our work, the goal of this second function is the active monitoring and diagnosis. The so called “augmented component will then continue carrying out the initial primary function and will be able to diagnose failures influencing the primary function’s performance.

However due to the innovative aspects and the use of new technologies like intelligent distributed control systems (Cauffriez, 2004), (Ciame, 2009) SURFER increases the complexity of train’s architecture. The achievement of reliability/availability goals is therefore more complicated. The main objectives of this our work are to:

- propose a methodology to assess the reliability/availability of the augmented system,
- compare the parameters’ value of the augmented system with the ones of the initial “non augmented” system,
- study the impact of the use of augmentation

F.J. Restel

Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Transportation processes occurring in the transportation system are not determined, however, the processes may be disrupted as a result of various problems connected with:

- vehicle unreliability,
- infrastructure unreliability (failures of rail, signalling etc.),
- random accidents occurrence (associated with environment).

All of these problems can be a cause of preventing execution of the transportation process in accordance with the timetable. First problem of the vehicle reliability analysis has been extensively researched for many decades.

On the other hand the infrastructure reliability has not been investigated and unfortunately, little attention has been given to this problem in reliability literature. Unwanted events bounded with infrastructure share more than fifty percent of whole incidents of an exemplary region. Considering the share, the question is formed, how to define the transportation system reliability level

and which measures allows to characterize and

compare reliability level by different railway lines

in different regions.

This task is strictly connected to definition of

possible hazard events and its measurable terms.

For example intensity of events defined by number

of unwanted events per year does not allow to

compare lines with different numbers of trains

launched per year.

The paper considers problem of reliability

measures of railway transportation system. Relia

bility analysis of such a complex system is compli

cated because of many factors. In the introduction

section, have been defined problems of unwanted

events and their influence to railway transporta

tion system. There is also presented how many

percent of all failures are related to infrastruc

Optimization of preventive maintenance policy based on operational

reliability analysis (Application to tramway access doors)

B. Bonnet

Engineer in the RAM Center of Excellence, Transport Information Solutions, Alstom Transport,

Saint Ouen, France

P. Dersin

RAM Methods and Tools Director, Transport Information Solutions, Alstom Transport, Saint Ouen, France

ABSTRACT

Preventive maintenance is often organized on the basis of pre-determined time-based operations. Adapting preventive maintenance periodicities to the actual reliability characteristics of an asset generally leads to higher availability (by avoiding failures) and to lower costs (by avoiding unneces sary maintenance operations).

In addition, an in-depth knowledge of reliabil ity characteristics makes availability and life-cycle cost predictions more accurate and paves the way for maintenance policy optimization. Such an approach, with application to the access doors of ALSTOM's Dublin tramway, is reported here.

Because field failure data are typically strongly censored, ALSTOM Transport Information Solu tions' RAM Center of Excellence has decided to develop its own statistics software package to proc ess field failure data, as commercial packages have not been found satisfactory in that respect. The resulting software, named RDAT® (Reliability Data Analysis Tool) has been relied upon for this study: it is especially adapted to statistical failure data analysis.

The analysis is separated in two phases.

- During the first phase, all tramway doors data are processed indistinctly (meaning that all tram ways are taken into account): this gives a global appreciation of the tramway doors behavior.
- During the second phase, tramway data for each tramway are considered separately: this gives an individual appreciation of door behavior for each individual tramway.

For each analysis level (global and individual analysis), a wear-out phenomenon (or an increase in failure rate over time) is confirmed for tramway doors. Indeed, at every analysis level (first failure or all failures considered), the reliability law is

RAMS processes in railway-substructure engineering for improved project quality

E. Okstad

SINTEF Technology and Society, Safety Research, Trondheim, Norway

ABSTRACT

System RAMS, as seen in the context of the European standard EN50126 is a combination of reliability, availability, maintainability and safety. Railway RAMS is thus a characteristic of the rail way systems' long term operation and is achieved by application of different engineering concepts,

methods, tools and techniques from the early plan
ning phases of, and all the way into the operation
phases of the system. Current experiences from
railway RAMS implementations in Norway are
that RAMS to a certain degree is an activity for
the “experts”, a bit on site of the main business
value-chain.

The main objective of this paper is to suggest
improvements of the RAMS process as it is con
ducted in railway engineering projects. The main
problem is to make the railway-RAMS processes
more cost effective and streamlined in a way that
satisfies requirements of main stakeholders. Sub
objectives of the paper are:

- To give en overview of current practice based on
available literature and open sources to indus
trial practices.
- To suggest improvements of the RAMS process,
including the RAMS analyses and implementa
tion of risk reducing measures.

The suggested approach is illustrated below.
The figure shows the main RAMS activities in
relation to the value chain. The core engineering

A)

B) Railway building and operation

C) RAMS coordination, two times a year Engineering, HAZID
RAMS coordination, once a month Engineering, RAMS review
Hazard register

Figure 1. RAMS process and activities in engineering.

Risk analysis applied to discrete transportation systems

D. Caban & T. Walkowiak

Wroclaw University of Technology, Wroclaw, Poland

ABSTRACT

Risk analysis is used to ascertain the consequences of making a decision, when these cannot be a pri ori determined. The analysis ensures that the risks are identified, likelihood of their occurrence is established and the consequences are evaluated. We consider the operational risks connected with managing a Discrete Transportation System (DTS), i.e., a transportation system in which goods are transported by a fleet of vehicles of limited capacity. The vehicles operate according to fixed schedules, carrying goods between destinations. The considered operational risks are connected with unexpected, grave distortions of the system operation—massive vehicle breakdowns, epidemic illness, strikes, other concerted actions that cause periodic inoperability or inefficiency of the system. Inoperability or reduced efficiency of the system can cause serious backlog of goods requiring trans

portation. Thus, on resuming normal operation, it

may be impossible to mitigate the consequences of

inoperability or it may take excessively long time.

This causes high risk of liability for transportation

delay or loss of goods.

The proposed risk analysis is based on the

assessment of system operation using Monte Carlo

simulation. A custom designed simulator has been

developed to support this approach. The consid

ered risks are modeled in the simulator, which can

then estimate their impact on the system. The qual

ity of service realized by the system is characterized

by the percentage of shipping assignments that are

delivered on time (before a fixed deadline):

A E N N r i pd i i pin i d i i in i

( ) (,) (N) (,) (N) , τ τ τ ⎡ ⌊ | ⌉ ⌋ | 1 (1)

where

N pd (τ i , τ i+1), N d (τ i , τ i+1) denote numbers of assign

ments realized in the reporting period (τ i , τ i+1), on

time and overall,

N pin (τ i), N in (τ i)—numbers of in progress

assignments at the end of the reporting period, on

Risk assessment and improvement of resilience of critical

communication infrastructure

S.O. Johnsen

Norwegian University of Science and Technology (NTNU),
SINTEF, Trondheim, Norway

M. Veen

Norwegian National Rail Administration, Trondheim, Norway

ABSTRACT

This paper discusses the significant findings of a risk assessment of the infrastructure used in emergency communication in railways in Norway, the Global System for Mobile Communications in Railways (GSM-R) system.

The risk assessment was based on a socio technical approach, which considers technical, organizational and human factors, called MTO as explored by Rollenhagen (2007). Action research was used as a part of the risk assessment, to improve the quality and the impact of the assess ment, as mentioned in Johnsen (2009). To improve continuity and reliability, resilience of the infra structure and organization was included in the risk assessment. Resilience was defined as “the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances, so that it can sustain operations even after a major mishap or in the presence of continuous stress”, from Hollnagel (2006).

The mitigating actions prioritized by the risk assessment wereimproved resilience, such as redundancy in technology and organizational capabilities.

The key risks were documented in a risk matrix, and discussed and improved in an open search conference, with participants from key stakehold ers from management and the workforce. Mitigat ing actions were enhanced and prioritized by the participants in the search conference.

In addition, we have performed a survey of safety and security culture in 2009 and 2010 in order to assess development of knowledge and aware ness of key issues related to safety and security. This approach was based on correlation between attitude factors such as the operators morale and motivation and the actual incident/accident rate of train operations, from Itoh (2004). Based on the correlation of the past, it is suggested to use sur veys in addition to incident/accident data to iden tify possible high risk or low risk units or areas.

We have reviewed the results in 2010, docu

Statistical analysis of railway safety performance in the European

Union

J. Braband

Siemens AG, Braunschweig, Germany

H. Schäbe

TÜV Rheinland, Köln, Germany

ABSTRACT

The European Railway Agency (ERA) has published their first report “Railway Safety Performance in the European Union 2008” (ERA 2008), presenting statistical data from the member states from the period 2005-2006. An intermediate update has been published 2009 (ERA 2009a), reporting data from 2007.

Albeit the ERA has several caveats spread throughout the report (ERA 2008), such as

- “It must be remembered that data are now submitted by the national bodies for the first time and it is obvious that all of them have not had the possibility or time to put in place efficient quality assurance systems to provide consistent and accurately validated data.”
- “We issue a strong warning against drawing too far reaching conclusions on comparisons of data between EU member states.”

ERA already draws some careful conclusions from the data, e.g.

• “The data show a great variation between differ

ent countries. … As a matter of fact the differ

ence between the countries with the lowest and

the highest risk is greater than a factor of 20.”

Methodologically the ERA report contains only

raw data and mean values, but no treatment of sta

tistical uncertainty, which is always present in field

data. Thus this paper examines the data carefully

and explores what conclusions can be drawn using

statistical methodology. As it seems that also the

regulation on “Common Safety Targets” (European

Commission 2009), by which the safety performance

of the member states shall be assessed in the future,

does not take into account statistical uncertainty,

the findings of this paper may have also an impact

in this field. It should also be noted that in 2010 ()

European Commission 2010a) a first set of refer

ence values based on the accident statistics was pub

lished, which are based on data from 2004–2007.

It has been shown in this paper that the qual

Audit to a specific study scenario according to a reference framework

for the improvement of the warranty management

V. González Díaz, C. Parra Márquez, J.F. Gómez Fernández & A. Crespo Márquez

Department of Industrial Management, School of Engineering, University of Seville, Spain

ABSTRACT

This study is intended to present to the reader a classification of different engineering tools, focused on the improvement of the warranty man agement and product reliability, showing all this by its application on a practical case. For that pur pose, a first goal in this paper will be to describe a case study of warranty assistances, analyzing its management in the framework of a manufactur ing company which provides deliverables during a specific period of time and following a certain scheduled distribution. Several different types of warranties are suited for different products (consumer, commercial and industrial; standard versus custom built ...). From these, the kind of product that the paper will deal with is a custom built product. Once depicted the working pro cedure and the connections set between sections inside a generic company, a reference framework will be proposed in order to manage the warranty assistance, using specific and previously-developed engineering techniques found in the literature on similar processes. They will be gathered in four sequential stages, where the different techniques will play a crucial role. Following this scheme, a

framework is presented as a sequence of activities

in order to support the management of a warranty

program. This proposed reference framework

will be focused in the improvement not only of

the product reliability, but also in the relationship

between manufacturer and customer, offering a

practical vision of the set of actions which com

pose each organizational block. By reengineering

of management processes and by the application

of a correct warranty organization it is possible

to influence the product design and manufactur

ing among others features, increasing its quality

and reliability by enhancing the information flow

concerning product defects and their sources.

After presenting the case study and the proposed

management framework, they will be compared

Exact formulation of (R,S) and (s-1,1) inventory policies with poisson

demand. Application to spare parts stock optimisation

J. Lonchampt

EDF R&D Division, Chatou, France

ABSTRACT

Spare parts management is a crucial stake for

industries, as badly sized inventories may generate

important losses, such as storing or holding costs

if a stock is oversized or unavailability if it's under sized. An inventory may be characterized by its complete cost made of the spares costs, the stock ing costs including storage and maintenance of the spares, and the cost of the unavailability due to empty stock.

Several models exist to evaluate complete cost of a given stock, depending on wether the underly ing components suffer ageing or not (Lonchampt, 2007) or on the kind of results a decision maker wants to obtain, mean values or enhanced risk indicators (standard deviation as in Lonchampt, 2008). The policy considered in this paper is a (R,S) periodic review policy, where R stands for the periodicity of review and S is the target number of spares at each review, that is to say every R the gap between the actual stock size and S is purchased. This model is described for the need of power plants components, the customers arriv als of the inventory theory are then here failures of components and the customer waiting time are downtime of plants.

The indicators we need to calculate to valuate a given policy, consisting in a choice of a periodic ity and a target number of spares are:

• Mean Inventory Level (IL) used to calculate the

holding cost which is proportional to the number

of spares in stock.

• Mean Unavailability (U) used to calculate the

cost of forced outages.

• Initial supply used to calculate the investment

cost at the constitution of the stock.

• Mean supply all over the lifetime of the

inventory.

All these indicators are calculated with the mean

dates of the inventory variation, which are the

mean dates of failures.

The mean date of the kth failure knowing n have

been observed is given in (Eq. 1).

τ k t k n

ICT application on the warranty management process.

The “e-Warranty” concept

V. González Díaz, L. Barberá Martínez, J.F. Gómez Fernández
& A. Crespo Márquez

Department of Industrial Management, Escuela Superior de
Ingenieros de Sevilla, Spain

ABSTRACT

This document is focused on one of the steps

included in a reference framework, proposed by

the authors in former works and developed for

the improvement of the warranty management.

Particularly, the referred stage tries to apply the new Information and Communications Technolo gies (ICT) in the improvement of the after-sales service organization, where such technologies may help and make easier the decision-making related to different aspects in the context of warranty man agement as, for instance, the possibility to foresee eventual complains from the customer. For that purpose, the paper starts with an introduction to the current notion on warranty, describing briefly all those steps included in the refer ence framework proposal. Hence the reader can locate the stage to be developed along the paper, inside a context of tools and methodologies. Then, the concept of ICT and its specific application on the maintenance area is defined in order to apply it later on and in similar terms to the case of a product, which is already launched to the market. This product shall be, logically, assisted under warranty when the user communicates a claim about some defect or failure during a specific period of time. This particular application of the ICTs to the warranty manage ment, called “e-warranty” by the authors, allows us to determine qualitatively its influence inside the proposed reference framework and its interaction

with the rest of stages which configure it, needed for a proper and right technical assistance to the customer. Finally, some conclusions derived from the study are exposed and future researches on this

Institutional design of product recall based on multi-agent simulation

K. Mitsudo, T. Kanno & K. Furuta

Department of Systems Innovation, The University of Tokyo, Tokyo, Japan

ABSTRACT

As people’s demands for safety have increased recently, a high level of quality assurance is now required for suppliers of industrial products. Generation of defective products is not completely avoidable, however, even though producers are fully making efforts to avoid it. Product recall, which is to be executed by self-judgment of product pro ducers, is a social scheme for protecting consumers from unanticipated damage due to defective prod ucts. Meanwhile the media repetitively report late recall judgment by car makers, deceptive original indications of foods, organizational cover-up of information on defective products, and so on, and these cases often attract social attention. The con sequence of such infamous acts is not only that the producer will lose reputation and benefit, but also

that deteriorated consumers' trust on the market may lead to economical damages for the society as a whole. It is required therefore socially as well as administratively to establish an effective and trustworthy scheme for product recall.

Consistent institutional design of product recall is not an easy task, because a very wide variety of products can be the targets of product recall. For example, the Quality-of-Life Policy Bureau, Cabi net Office of Japan published the general product recall guideline as a framework for promoting product recall fast and appropriate from a view point of consumers in preparation for establishing the Consumer Affairs Agency in 2009 (Quality of-Life Policy Bureau 2009). Well-founded dis cussions have not yet been made, however, how a concrete scheme of product recall can be designed for achieving the final goal of the guideline, and some method for doing it is desired.

This study proposes a method of social simula tion based on a multi-agent model for application to product recall. The model consists of three types of agents: producers, consumers, and news media. Producers manufacture and sell products to gain benefit, consumers buy products to enjoy product utility, and news media report product failure and product recall

to consumers. By observing interacting behaviors of agents in a virtual society, it is possible to search for the conditions where the designated goals of product recall are achievable. As a result of test simulation, it was demonstrated that four society types could represent different characteristic behaviours of the artificial society: seller's market, buyer's market, mind-oriented market, and ability-oriented market (Figure 1). Some insights also have been obtained on the conditions that enhance producers' motivation toward product recall. Consequently, it was demonstrated that the proposed simulation is a useful mean for institutional design of product recall. REFERENCE Quality-of-Life Policy Bureau, Cabinet Office. 2009. General product recall guideline – framework for promoting product recall fast and appropriate from a viewpoint of consumers –, http://www.caa.go.jp/ safety/pdf/ 090901safety_6. pdf (in Japanese). Product quality Failure rate High High R e c a l l r a t e H i g h H i g h Good Able Unable Mind oriented Buyer's market Ability oriented Seller's market R e c a l l t h r e s h o l d Bad Figure 1. Qualitative relation between model parameters for producers and consumer's assessment.

Integrated model of control chart and maintenance management with

costs of production losses

F. Costantino, M. De Minicis & G. Di Gravio

Department of Mechanical and Aerospace Engineering, University of Rome "La Sapienza", Rome, Italy

ABSTRACT

According to many authors (Cassady et al., 2000,

McKone et al., 2001, Kuo 2006) the role of main

tenance management in improving production

quality is particularly important. Adequate main

tenance certainly contributes to keep equipment

efficiency thus avoiding the production of scraps.

In literature, this issue has been discussed mainly

considering the adoption of Statistical Process Control as a way to prevent out-of-control production. In particular, the most important contributions are related to the optimization of the design of control charts when planned maintenance is carried out (Duncan 1956, Alexander et al., 1995, Cassady et al., 2000, Linderman et al., 2005, etc.). The literature review revealed that the integration of statistical process control with preventive maintenance activities can be effective to reduce maintenance cost per hour. Nevertheless, most methodologies are characterized by the optimization of maintenance cycle costs without considering the consequences that out-of-control processes have on production cycles. When a quality shift occurs, defective products must be reworked or worked from scratch. In this case, an additional cost must be added to take into account time spent producing scraps.On these considerations, starting from the model presented by Linderman et al. (2005), the paper presents an integrated quality and maintenance model in which costs of production losses are considered. First of all, proposed formulation has been compared to the Linderman's one proving to be suitable to all those circumstances in which production losses are substantial and maintenance costs can be considered negligible if compared to them. Then, the methodology has been applied to a case study in a pharmaceutical plant,

which represents an innovative context of application. In particular, the problem of powder filling in a bottling line has been addressed. In this environment, costs related to scraps are sensibly high due to the presence of active principles in the powder. Proposed model has been applied to a real case in a pharmaceutical plant. Maintenance cycle cost of the coordinated model has been compared to the ones obtained by adopting exclusively planned maintenance strategies or statistical process control. The analysis was meant to determine if the adoption of a coordinated monitoring-maintenance model (MM) was effective in terms of total costs over time, that is considering system degradation. Moreover, the situation was tested even considering a reduction of maintenance costs and a decrease in the number of failures. According to obtained results, the adoption of a MM model to the power filling line appears effective to reduce total hourly costs. By the way, in case of acquisition of new equipment or the arrangement of mitigation actions to reduce penalty costs, results from the model could change in favor of a different maintenance strategy.

Intelligent supervisory system for availability estimation of automated

material handling system

J. Smoczek & J. Szpytko

AGH University of Science and Technology, Krakow, Poland

ABSTRACT

The paper presents fuzzy logic approach to

estimate the operating time OT f f ∧ ( )T T ∈TBF

(Time Between Failure) of exploitation systems

equipments based on the operating conditions. The

model of prediction of the failure time is based on

the assumption that it is possible to specify the X

vector of parameters which changes monitored

from the time of the last failure occurred in the

system (denoted T f-1) can be used to characterize the system exploitation state at the actual time t. Consequently the input variables X describe how the exploitation state of the monitored system has changes in the period of time t-T f-1 . Those input variables of the fuzzy model (Fig. 1) are used in fuzzy relations IF-THEN to estimate output vari able denoted POT (T f -T f-1)—the predicted operat ing time of the considered system between the last failure T f-1 and the next (predicted) failure at the time T f .

The relations between the exploitation states of the considered system and the predicted operating time between the last and next failure is expressed in the form of N implications specified in the knowledge base of fuzzy model:

IF x 1 is MF k (x 1) and x 2 is MF k (x 2) … and x n is MF k (x n) THEN POT k (T f-1) (1)

The FIS parameters (crisp output values POT k (T f-1) of fuzzy singletons) are improved in on-line learning process by using Recursive Least Squares (RLS) algorithm.

Figure 1. Fuzzy inference system (FIS) to predict

Key performance indicators—a necessary tool for managing improvement processes?

O. Meland

SINTEF Technology and Society, Trondheim, Norway

ABSTRACT

European companies having their main niche within manufacturing are experiencing several challenges surviving on today's markets among a continuously increasing number of competitors from the eastern part of the world. Traditionally, these competitors were mainly manufacturing cheaper versions of already existing products. How ever, during the last decades, they have increased their competence, enabling them to begin monitor ing and improving their manufacturing processes in a new and innovative way.

In order for the European manufacturing companies to stay competitive, they have to strug gle towards leading their production departments to the optimum level of efficiency and effectiveness. Simultaneously, it is important to focus on finding the right areas for minimizing the company`s costs. Finding the right balance between all these elements might become an expensive exercise for the companies.

The paper highlights and discusses challenges within improvement processes and performance

measurement. All issues are related to a large project and case study performed in collaboration with a Norwegian manufacturing company producing different products with potatoes as raw material. All activities were performed over a time period of four years and received financial support from the Norwegian Research Council.

Based upon a lack of continuity and reliability in several production departments, the potato company in 2006 decided to sketch a project with an objective of improving the efficiency and effectiveness in their production departments. Simultaneously the company wanted to focus on mapping areas with potential for cost reductions. Within the Norwegian convenience chains there is a growing trend related to developing private label products. By offering these products at lower prices, the convenience chains aim towards capturing larger market shares. An increasing number of new brands on the market contributed to reinforce the potato company's demand and need for a project with these objectives. In 2006 there was an ongoing trend within Norwegian manufacturing companies. Almost every company was performing some kind of effort trying to implement the LEAN concept. The LEAN concept was initially developed out of Toyota's Production System and focuses on converting an organization into only performing value creating activities. Instead of starting a project for the potato company only focusing on implementing the LEAN

concept, it was decided to start the project by implementing Total Productive Maintenance (TPM). Without having implemented TPM, it will be challenging to convert an organization heavily dependent from its machines, into a LEAN organization. Instead of pointing out a complete process as object for the analysis, TPM only focuses on a specific work area within a production process with main objective on visualizing and eliminating the losses. The first step when implementing TPM is to establish an improvement model which objective is to describe the containment and sequence of the activities in the project. The intention of the model is to serve as a road map describing the road or terrain which has to be crossed for the company to be able to achieve its objectives within TPM. Additionally the road map is going to illustrate the chronology of the activities, starting with the foundation stones. Initially, the potato company wanted to start measuring performance to enable improvement processes. Early in the work package of establishing a balanced system for performance measurement, the company realized that only measuring performance as number of produced product per time unit was insufficient when wanting to capture the totality in the company. The vision of the potato company is world class cost-effective production. To be able to concretize this vision and visualize the effect on the steps towards fulfilling it, an assumption is to establish a balanced system for performance measurement.

Logistic support for the improvement of the warranty management

V. González Díaz & A. Crespo Márquez

Department of Industrial Management, School of Engineering, University of Seville, Spain

F. Pérès

Laboratoire Génie de Production, ENIT–INPT Université de Toulouse, France

M. De Minicis & M. Tronci

Department of Mechanical and Aerospace Engineering, University of Rome, “La Sapienza”

ABSTRACT

As a result of the increasing customer expectations,

product performances and characteristics are no longer the sole aspects to consider in a competitive global market. Nowadays, products must perform satisfactorily over their useful life to reach buyers satisfaction. In this context, the role of post-sale services, particularly during warranty period, becomes crucial so that an efficient warranty program represents a competitive weapon.

The management of warranty is not a simple issue as it combines technical, administrative and managerial actions. Literature review reveals important interactions between warranty and other disciplines, such as outsourcing, quality, costs and maintenance. Considering the above mentioned aspects, main problems in warranty management efficiency seem to be correlated to logistic issues (for example spare partsinventory levels an warehouse logistics).

On these considerations, the paper addresses the problem of warranty management efficiency, in particular for complex system such as a custom built product, where multitude components and conditions must be taken into account. More in details, the adoption of logistic support principles to the definition of strategically important

warranty issues is proposed. After presenting most important issues of warranty management and proposing a framework for its management, the paper analyzes the logistic support applied to complex products and how this support can be focused to facilitate and improve the decision-making process.In particular, the paper presents a reference model to guide the decision making process concerning the following critical aspects: - classification of critical components of the product which, due to their significance according to different factors, deserve to be specially analyzed for the warranty management; - choice of repair levels, which are those maintenance levels that are more effective to take the proper actions during the development of a warranty program; - tasks definition which refers to those methods that define the maintenance and warranty tasks when a component, in a specific product, fails; - required spare parts and allocation. The presented framework is referred to the military industry in which logistic support strategies are widely applied. Despite this, proposed methodology can be considered universally valid and easily applicable to different contexts.

Near-miss management system design in a lean manufacturing process

S. Andriulo & M.G. Gnoni

Department of Innovation Engeneering, University of Salento, Lecce, Italy

P. Nardone & G. Maggio

Bosch Diesel Technology and Brake Systems S.p.A., Bari, Italy

ABSTRACT

One critical component of a Safety Management

System (SMS) is the near-miss management activity.

An effective Near-miss Management System (NMS)

aims to recognize signals from the operational fields

in order to apply more effective prevention strategies.

These systems are widespread in industrial contexts

characterized by high level of risk, i.e., major hazard and hospital sectors; few examples could be found in manufacturing processes which are characterized by different operational conditions and risks (i.e., occupational risks). Few applications are develop ing in other industrial sectors: they are usually infre quent in the manufacturing process. On the other hand, lean thinking strategy currently represents a competitive tool for facing with current market dynamic. Thus, when lean manufacturing principles are applied, the near-miss management system must be designed according to this issue differently from its traditional fields of application (e.g., chemical sectors). Moreover, the effectiveness of a near-miss management system represents a complex issue: sev eral parameters—such as safety climate, high number of data, etc.—could influence its design and appli cation. The present paper proposes the design of a near-miss management system in a lean manufactur ing process of an automotive supplier: lean concepts have been applied in order to integrate traditional features characterizing near-miss management sys tem with basic ideas of lean manufacturing.

Thus, the design of a NMS in a lean manufac turing environment has to be in accordance to lean

principles.

The goal is to design a NMS according to Lean Manufacturing concepts as this system has to be fully integrated in the BPS. The first activity is to define events the NMS have to deal with. Thus, three types of events have been defined: Unsafe Act:, Unsafe Situation, Near Miss event. After near-miss event definition, the information flow for managing event in the NMS has been evaluated aiming to integrate effectively this system according to lean principles. Next, operational procedures of the proposed NMS have been designed. As defined in the scenario

Optimal controller for manufacturing systems by decentralized

approach

A. Philippot & V. Carré-Ménétrier

CReSTIC—University of Reims Champagne-Ardenne (URCA), Reims, France

A. Tajer

ENSA, University of Ibn Zohr, Agadir, Marocco

ABSTRACT

Elaboration of controller’s programs for the manufacturing systems in a Programmable Logic Controller (PLC) requests a good knowledge of the normalized languages (IEC 61131-3, 1993) but also of the plant behavior. However, with the increase

of the systems complexity, the designer needs to take into account some constraints of safety, live ness and dependability. Manufacturing systems can be represented as Discrete Event Systems (DES), i.e., dynamical systems with discrete state spaces and event-driven transitions (Cassandra and Lafor tune, 2002). To help the designer in this task, two approaches are possible: (i) control Validation and Verification (V&V) and (ii) Supervisory Control Theory (SCT) based on synthesis controller. However, the main problem to performing V&V or SCT is the combinatorial explosion due to the synchronous product state space. To overcome these problems, decentralized or hierarchical approaches have been recently exploited in the literature. However, the major problem is how to ensure implementation in the Programmable Logic Controller.

This work proposes a decentralized approach of SCT using a synthesis algorithm and based on a modular modeling of the plant. The proposed approach consists in restricting the system behavior within a desired specification expressed by logical local and global constraints. There are two types of constraints to model: safety constraints (what you

should not make) and liveness constraints (what it

is necessary to make). To insert constraints con

sists in inhibiting some actions and/or ranking the

execution of actions to send to the plant.

The proposed approach is composed of 5 steps

(Fig. 1):

- Firstly, plant is modularly modeled according

to mechanical characteristics. Local models are

called Plant Elements (PEs).

- The second step consists into define safety and

The management of a warranty assistances program: A suggestion as

reference framework

V. González Díaz, L. Barberá Martínez, J.F. Gómez Fernández & A. Crespo Márquez

Department of Industrial Management, School of Engineering, University of Seville, Spain

ABSTRACT

The objective here is to propose a reference

framework for the management of warranty assist

ances, using certain engineering techniques for

similar processes, and according to a process-based

quality management system. Therefore, regard

ing the warranty management process, a generic

framework is presented integrating management

models already developed and found in the litera

ture. They will be gathered in four sequential steps or managerial blocks, where the different techniques will play a crucial role. As a first step, it is considered the Warranty Program Effectiveness in order to avoid strategical contradictions between the warranty program and the overall business management as well as how crucial a client's complaint can be and its consequences to the business. As a second step, it is considered the Warranty Program Efficiency in order to attend warranties with minimum waste, expense, or unnecessary effort. As a third step, it is considered the Warranty Program Assessment where studies related to Reliability, Availability, Maintainability and Safety as well as the Life Cycle Cost Analysis takes its importance. As a fourth step, it is considered the Warranty Program Improvement where it is included the implementation of new technologies, the Customer Relationship Management as well as the Six Sigma methodology which integrates the human factor with statistical tools in order to engage the complex mechanisms inside a company. Following this scheme, the framework is defined as a support for the management of a warranty program, offering together a practical vision of

the set of activities which compose each manage

rial block, and focused on the improvement of the

relationship between manufacturer and user. By reengineering of managerial processes and by the application of a correct warranty management is possible (among others features) to influence in the product design and/or manufacturing, increasing its quality by the enhancement of the information flow about product defects and their sources. The result of the study is in few words a classification of different engineering tools, focused mainly on the improvement of the warranty program and product management, enhancing in parallel maintenance and manufacturing aspects, and discussing briefly the proper use of each tool or technique according to the data or information available. Step 1: EFFECTIVENESS Balance Score Card Criticality Analysis Failure Root Cause Analysis S t e p 2 : E F F I C I E N C Y RA & MDT adapted to Warranty Warranty Policy Risk-CostBenefit Analysis S t e p 4 : I M P R O V E M E N T Six sigma E-Technologies (E-Warranty) Customer Relationship Management Step 3: ASSESSMENT Life Cycle Cost Analysis Reliability, Availability, Maintenability and Safety Figure 1. Proposed framework for warranty management.

The reverse logistics model of single-component product recovery

M. Plewa & A. Jodejko-Pietruczuk

Wrocław University of Technology, Wroclaw, Poland

ABSTRACT

Until recently logistics systems supported only

processes carried out in classical material flow

from producer to final user. Recently it has been

a striking growth of interest in optimizing logis

tics processes that supports recapturing value

from used goods. The process of planning, imple

menting, and controlling the efficient, cost effec

tive flow of raw materials, in-process inventory,

finished goods and related information from the point of consumption to the point of origin for the purpose of recapturing value or proper disposal is called reverse logistics. In reverse logistics systems demand can be partially satisfied with new items manufacture or procurement and returned prod ucts value recovery. Reuse of products can bring direct advantages because company uses recycled materials instead of expensive raw materials. The first part of the article contains literature survey, which is a summary of work that has been done around the theme of research, allowed to set out this article aims and objectives. In literature the field of reverse logistics is usually subdivided into three areas: inventory control, production, recovery and distribution planning. The model presented in this paper is a inventory control model and hence the literature survey refers to this area. Presented review allows to summarize the cur rent state of knowledge. Most authors assume that demand and returns are independent Poisson random variables. Few authors examine the relationship between the demand, and the number of returns but there are no inventory models in reverse logistics that use reliability theory to assess

the number of returns. There are few models that use the reliability to assess the reusability of components. In real reverse logistics systems products that fail in a short time after the purchase by the final user are withdrawn from the market. In most cases these products are returned to the manufacturer. Recovery of such products or components is not labor-intensive, because undamaged components have not been exposed to the aging process and are suitable for direct reuse. The goal of this paper is to create a inventory control model in which products are recoverable if they are withdrawn because of failure before a specified time from the start of the operation process. Article contains forecasting model which explains the process of moving goods from maintenance system to recovery system. In presented model there is an assumption that there is a relationship between demand for new products and the number of returns. There is also an assumption that every product that fail before acceptable time to failure can be recovered and used again. After recovery process products are as good as new ones. Demand for new products can be fulfilled by production or by recovery of used (failed) products. This article deals with single-item products. This paper objectives are achieved by creating the mathematical model that describe analyzed processes. Some objectives can't be achieved without creating a simulation model, which make possible to describe analyzed processes with various probability distributions. The next step is a sensitivity analysis of created model. The article ends with conclusions and directions for further research. Maritime transportation This page intentionally left blank

A proposed Fuzzy Bayesian Network (FBN) model for measuring

seafarers' reliability

R. Riahi, I. Jenkinson, S. Bonsall & J. Wang

Liverpool John Moores University, UK

ABSTRACT

The UK Marine Accident Investigation Branch

(MAIB, 1999) stated that one factor; human error

still dominates the majority of marine accidents.

The most common human factor causes were

error of judgement and improper look out or watch keeping, followed by failure to comply with regulations (Hetherington, et al., 2006). Risk factors in maritime transportation were analysed and researched by many researchers. After analysing many accident reports and by taking the vessels' flag, ownership, type, age, type of cargo, and location of accident into account human factors were found to be the prevalent causes.

Root causes for human error can be segregated into two categories, which are described as preventable (e.g., a ship's design & habitability, a ship's design & layout) and inevitable (e.g., sea conditions). Throughout the preparation of a specification for new building of a vessel and during its design and fabrication stages, preventable factors can be diminished by the appropriate strategies. The seafarers' motivations, fatigue, and rest hours are highly dependent on a ship owner's strategies. The frequency of accidents and the severity of their consequences, as a result of a ship owner's correct strategies and by improving the seafarers' reliability, can be reduced and accordingly seafarers' performance can be enhanced.

Measurement of reliability of human behaviour

in a human-machine system has been a source of interest since 1963. Given that human reliability is normally expressed in both quantitative and quali tative terms, decision makers may often carry out their judgments based on both quantitative data and experiential subjective assessments. Thus, a proposed mathematical model for measuring the human reliability should be capable of processing

A study of the implementation of maritime safety regulations by a ship operator

H. Karahalios, Z.L. Yang & J. Wang

Liverpool John Moores University, Liverpool, UK

ABSTRACT

Many maritime regulations are not adequately implemented worldwide. As a result, the stake holders within the shipping industry have often found themselves in an uncomfortable position in developing their business. A methodology involv ing a System of Hierarchical Scorecards (SHS) has been developed to facilitate the implementation of a newly introduced or an existing maritime regula tion in the shipping industry. The SHS includes a cost and benefit analysis capable of assessing the burden that is generated to the shipping industry from the implementation of a maritime regulation.

A ship operator is chosen as an example to demon
strate the proposed methodology

Every maritime regulation introduced by the IMO aims to enhance safety at sea and/or to protect the environment. Any failure to effectively implement a maritime regulation may have adverse effects in terms of safety, pollution and business damage for the violated parties. Therefore, a stake holder should monitor his performance while implementing a regulation since partial imple mentation may generate grounds for accidents.

A stakeholder needs a tool that will allow him to monitor the regulatory implementation process at all levels within his organisation. To meet the above steps/objectives a SHS tool generated by combin ing a set of techniques such as the Balanced Score card (BSC), Analytical Hierarchy Process (AHP) and fuzzy set theory is proposed as an appropriate methodology of measuring maritime regulation implementation. The BSC provides the strategic framework that can be followed to obtain a desired result by producing scorecards. However each perspective or each measure from the produced scorecards is ranked by using fuzzy set modelling and AHP in order to determine the weight of each

scorecard element in the implementation process.

A framework for evaluating a regulation per

formance can be set by using the following steps:

1. Set the hypothesis that will be tested.

2. Identify the divisions of a stakeholder’s

An integrated Life Cycle Assessment model to facilitate ship ecodesign

E. Vanem, L.E. Mangset & G. Psarros

DNV Research & Innovation, Det Norske Veritas, Høvik, Norway

R. Skjong

International Affairs, Det Norske Veritas, Høvik, Norway

ABSTRACT

The methodology of Life Cycle Assessment (LCA)

has recently gained widespread support as a way of

estimating the environmental and societal impact

over the life-time of a ship. The output from such

an LCA will normally be a set of indicators which

depict individual performance of each variable

included in the analysis. Increasingly, it is a demand

for the inclusion of indicators not conventionally

included in an LCA such as safety and economics.

An integrated analysis demands that all indi

cators provided by the LCA are weighted, with

respect to their relative importance to other indi

cators and with respect to the difference they

may have towards different stakeholders, i.e., in a multi-criteria decision process. However, comparison is not possible in an effective manner without a common denominator. In order to facilitate integration of ecodesign (design process where the environmental footprint is used to environmentally optimize the design) with risk based design (ship design optimized with regards to safety and accidental costs), this paper proposes a way of monetizing the various indicators related to the environmental footprint, the social external impact and safety. Hence, an integrated model for assessing the safety and environmental performance of a ship in monetary terms is presented.

The outcome of a performance evaluation will be a set of indicators, for example presented by spider diagrams (see Figure 1 for an example). This is important decision support in the design process, but it would be preferable to derive a common denominator for all impact variables. This paper proposes monetized values as such a common denominator and proceeds with suggesting actual values for the most relevant externalities. The paper will identify the dimensioning indicators and provide monetized values for those, e.g., related to

- Safety: cost of statistical lives and injuries
- Health: cost of health impacts
- Environmental risk: cost of release of environ

mentally harmful substances, e.g., oil spill, air

Analysis of near collisions in the Gulf of Finland

Floris Goerlandt, Jakub Montewka, Heikki Lammi & Pentti Kujala

Aalto University, School of Science and Technology, Department of Applied Mechanics, Espoo, Finland

ABSTRACT

Ship traffic poses various risks in terms of human

casualty, damage to the environment and eco

nomic loss. In a busy and ecologically vulnerable

sea area such as the Gulf of Finland, the risks are

considerable.

Various approaches can be taken towards under

standing and measuring the safety performance of

the maritime traffic system. This paper approaches

maritime safety from the viewpoint of near misses.

Inoue et al. (2007) indicate that near misses in the

complex maritime system are much more com

mon than accidents. Analysis of these can provide

a statistically more significant understanding of

the system safety than accident analysis, while still

based exclusively on observations.

The paper uses the concept of a ship domain

along with available data from the Automatic Identification System (AIS) to detect vessels which present a possible near miss. The applied domain, originally proposed by Fujii (1971), corresponds to the area around the vessel which a navigator wants to keep clear of other traffic. As the Fujii domain is the smallest domain proposed in the literature (Wang et al., 2009), it is used to detect possible near misses. The possible near misses according to the Fujii domain are detected from AIS data using a computational algorithm which scans the data for violations of the domain by other nearby ships. The analysis has been performed for the Gulf of Finland, using data for the period 01.04.2007-31.10.2007.

Results of the analysis indicate that possibly dangerous close encounters occur frequently in the Gulf of Finland. In Figure 1, the possible near col lisions in crossing encounters are shown.

Analysis of these incidents indicate that ships sailing under certain flags are more frequently involved in such encounters then ships under other flags. There is also a significant difference between ship types.

While the method provides some knowledge

about possible near misses, it is important to

understand its limitations. The AIS data sampling

rate and the definition and applicability of the

ship domain are discussed. In finding the actual

How incomplete statistical accident data affects the validation

of risk analysis models

M. Hassel

Safetec Nordic AS, Trondheim, Norway

B.E. Asbjørnslett & E.K. Ombler

Norwegian University of science and Technology, NTNU, Trondheim, Norway

ABSTRACT

Validation of risk assessment models are often

conducted by comparing model estimations with

historical and statistical accident data. Qualitatively

assured input data is also a requirement for proac

tive risk management, based on risk assessment and

analysis of the effect of risk control measures. This

is also true for maritime transport systems as they

rely on a historical basis of vessel accident data to

provide validation to risk assessment models.

This paper presents a fairway traffic risk assess

ment study in the Oslofjord area in 2010, where

statistical data was used to validate the risk assess

ment model used in the study. Historical statisti

cal accident data have been found and compared with the risk model used in the Oslofjord study. Statistical accident data for the Oslofjord area was collected from the Norwegian Maritime Authorities and IHS Fairplay Sea-Web, for the period from 01.01.1981 to 01.07.2010. Using a capture recapture method, an estimation of the specific level of underreporting for this location during this timeframe has been uncovered.

The paper suggests that statistical data used to validate risk assessment models should first be checked for underreporting and validated, for instance through the use of capture-recapture methods. Then, the subsequent use of correction factors should be evaluated. The degree of safety margin applied for the data used in the risk assessment, and the relation between the risk assessment result and the risk acceptance criteria should be given consideration in evaluating use of correction factors. Hence, a sensitivity analysis of the input data's effect on the risk assessment result versus the risk acceptance criteria could be an alternative to correction factors. Depending on the timeframe and geographical area of interest, correction factors should be made specifically for the scenario which is to be investigated,

to ensure maximum accuracy. The appropriate

methodology to develop specific correction factor

or alternative approaches to cope with lack of trust

Integrated risk management in an industrial port

P.A. Bragatto & A. Pirone

INAIL Italian Workers' Compensation Authority—Dipia ex Ispesl—Monte Porzio Catone Rome, Italy

ABSTRACT

The main goal of the present paper is to transfer

the recent findings in occupational risk quanti

fication, such as Ale (2008) into the question of

industrial ports. Even though the basic problem

is common to other industries, in chemical ports

there are a few specific issues, which include vessel

vulnerability, navigation risks and security issues.

Furthermore the method is required to be simple

and easy to use in order to be shared by all stake

holders. This paper is aiming to propose a semi

quantitative method, based on bowtie approach,

which has been developed for the assessment of the

personnel risk at an Italian industrial port.

The case study is a pier, featuring three berths

for gases and petrol transfer. The personnel at the

pier includes the gangs at the berths for mooring

and transfer operations, the squads for mainte

nance and fire fighting services, the engineers at the

control room, the guards at the security check. The (un)loaded materials include flammable liquids, such as gasoline or naphtha, and flammable lique fied gases (both pressurized and cryogenic). In the on-shore facilities Seveso legislation is enforced. An integrated Safety Report is present, as drawn up by all companies in the site. There are 15 top events and a possible domino scenario.

The basic idea is that both major accident haz ards and occupational risks could be evaluated by taking into account job descriptions, workers' number into a potential damage area, probabil ity of occurrence of the initiating event, workers' capability to mitigate consequences, as well as inspections results. The potential users should be the safety managers of the industrial port.

For each type of risk, for each worker, in each unit, the risk has been quantified as the combi nation of event probability, exposure to dam age, capability to mitigate consequences, levels of consequences.

The performance ranking for both preventive and protective barriers has been deducted from

two ships

J. Ahn, J. Kwak & D. Chang

Division of Ocean Systems Engineering, KAIST, Daejeon, Republic of Korea

ABSTRACT

This study proposed the procedure to determine the optimal redundancy level for the automatic docking system which was supposed to connect two ships at open sea. The docking system had a dozen of vacuum pads. The number of the functioning pads for successful docking was deter mined by the sea state. The system availability varies according to a sea state. Since the bare sys tem containing no redundant component showed a significantly low reliability, the optimum level of the redundant items was determined on the basis of a cost-benefit analysis. Adding the redundant items following the critical importance improved the total system reliability.

The optimum level of the redundant items was determined on the basis of a cost-benefit analysis where the cost was given by the added redundant items with the benefit given by the improved sys

Figure 1. Procedure for optimal redundancy strategy.

The possible impact of different watch keeping regimes at sea on sleep,

fatigue, and safety

T. Kongsvik & K. Størkersen

Studio Apertura, NTNU Social Research, Trondheim, Norway

J.H. Hansen

SINTEF Technology and Society, Trondheim, Norway

ABSTRACT

Fatigue has been an important contributing fac
tor for several major accidents and environmental
catastrophes at sea. It can be defined as a general
degradation in human performance (the Inter
national Maritime Association 2001). Sleep dep
rivation is an important contributor to fatigue
(Akerstedt et al., 2002, 2004). Different watch
keeping regimes provides different possibilities for
sleep. One of the most common regimes involves
6 hours on duty and 6 hours' rest (the 6-6 regime).
Another watch keeping system divides the day into
8 hours on duty, 8 hours' rest, 4 hours on duty, and
4 hours' rest (the 8-8-4-4 regime).

The following model illustrates possible relation
ships between watch keeping regimes and levels of
sleep, fatigue, and safety.

Different watch keeping system can prevent or
cause sleep deprivation leading to fatigue (involving
reduced cognitive performance), which can lead to

accidents (Akerstedt et al., 2002, 2004). Our research question is: Are there differences between different watch keeping regimes regarding sleep, fatigue, safety perceptions, and accident/near miss involvement?

The crews included in our study use one of two different watch keeping regimes during their four week duty period—either the 6-6 regime or the 8-8-4-4 regime.

Both objective measurements and subjective evaluations have been applied to shed light on the differences between watch keeping regimes regard ing sleep, fatigue, safety perceptions, and accident/ near miss involvement: 1) Cognitive and physi ological testing of 43 seafarers and 2) survey ques

Figure 1. Possible relationships between watch keeping regime, sleep, fatigue, and safety. Fatigue Safety Sleep Watch keeping regime Natural hazards This page intentionally left blank

A probabilistic framework for managing blowout risk during access to subglacial Antarctic Lakes

M.P. Brito, G. Griffiths & M. Mowlem

National Oceanography Centre, Southampton, UK

ABSTRACT

The planning for exploring Antarctic subglacial

lake has been on the making since they were first discovered, nearly 20 years ago (Siegert et al., 2007), (Mowlem et al., 2010). An important topic in planning for entry into a lake is the likely gas concentration and the potential risk for blowout. Depending on hydrological setting, subglacial lakes may contain large amounts of dissolved gas or gas trapped within clathrates. Consequently, access can be potentially dangerous due to the risk of blowout from the sudden release of pressure. We present a structured approach to assess the blowout risk in subglacial lake exploration. The approach integrates a generic event tree, applicable to open and closed hydrological systems, with site specific expert judgment incorporating rigorous probabilistic formulations. We apply the method ology to assess the risk of blowout during access to the subglacial Lake Ellsworth. Formally elicited judgments were provided by five experts with a combined 80 years experience in glaciology and ice drilling. Expert judgments' were aggregated to form two schools of thought, the optimists and the pessimists. The optimistic model was used for estimating the blowout risk during access to Lake Ellsworth, which gave a median risk of blowout of

1 in 12014 with a lower quartile of 1 in 17065 and an upper quartile of 1 in 9796. Following this initial assessment we explain how the efficiency of differ ent risk mitigation strategies can be quantified. The paper gives a background about Ellsworth subglacial lake and how the team is planning to gain access to the lake. The paper then presents the risk model used for estimating the blowout risk. Details of a formal expert judgment elicita tion process are also given. Results of the blowout risk analysis are discussed. The quantitative assess ment of potential risk mitigation strategies is also provided. Figure 1 presents the cumulative prob ability of blowout in light of three risk mitigation

Active environment as a potential source of risk of major accident

K. Sikorova & A. Bernatik

Faculty of Safety Engineering, VSB Technical University of Ostrava, Czech Republic

ABSTRACT

Since 1997, hit the Czech Republic a series of different sized floods—from two years to five hundred years waters. It was not a repetition of one particular situation. Each flood has been inter esting for its diversity.

From the perspective of major accident pre

vention, the flood is a significant source of risk, which can seriously endanger or damage the facility with a dangerous substance and cause considerable damage not only to property but also to the environment. An example of floods, which were leading to a major release of more than 80 tons of chlorine into the air and water were summer floods in Spolana chemical plant in 2002.

It is the environment in which we live and which is also an assumption for our further development. Given the increasing frequency of floods in the world, due to the increasing amount of dangerous substances to which they are traded, of course, increases the risk of negative impact. Therefore, we should in the coming years, through the “Research & Development Activities” to focus primarily on prevention, early prediction and pre paredness for these events in order to minimize the impacts to the lowest possible level.

For future, an important need is the interconnec tion of both two prediction systems of major acci dents and floods. Also important is the consistency of cooperation between experts responsible for certain part in this wide issue (the meteorologist,

hydrologist, safety engineer, technologist, environ

mentalist, etc.)

A part of this work was written in the frame

work of dealing with the grant project of Tech

nology Agency of the Czech Republic under the

Hydraulic modelling of the flood prone area in a basin with a historical report of urban inundation: The Arunca River case (Central Portugal)

P.P. Santos & A.O. Tavares

Centre for Social Studies and Department of Earth Sciences, University of Coimbra, Portugal

A.I.A.S.S. Andrade

Centro de Geofísica, Department of Earth Sciences, University of Coimbra, Portugal

ABSTRACT

Floods, considered major hazardous processes

due to the rising number of events with high

socio-economic impacts causing widespread dis

turbance, are frequent in the Arunca River drain

age basin (Central Portugal) as a result of climatic,

morphological, geological, hydrological and

anthropogenic factors. The vulnerability of the

area has increased in recent decades, mainly due to

the disturbances introduced by man (e.g., channel

artificialisation and a reduction in the infiltration

capacity of the floodplain and cover in urban

areas).

This paper describes how the 1-D hydraulic model HEC-RAS, using a higher resolution topographic surface including hydrogeomorphological details and other features influencing hydraulics, was applied to 4 reaches/sections spanning the upper, middle and lower basin of the Arunca River as well as urban and rural areas, in order to determine the flood prone areas for a return period of 100 years. The results were then compared with the existing flood prone areas.

The analysis made possible a new cartographic representation of the flood prone areas in four sections, which represent the most hazardous areas of the basin due to urban occupation (the large concentration of residential, industrial and commercial areas) and communications infrastructures (national and regional roads and national railway).

The comparison of the previous flood prone areas represented in the River Mondego Hydrological Basin Plan maps with the new cartographic representation stresses the great variations in the upstream sections (over 20%), due to more significant anthropogenic changes, in contrast with the

downstream sections (under 4%).

The results of the water height maps (Table 1)

emphasize that in the downstream sections meas

urements of over 2 meters are dominant; 93 ha of

Section D, the section furthest downstream, has a

water column height of over 4 meters. Table 1. Water height for the flood prone areas in the sections. Section A Section B Section C Section D Total area 4.1 ha 102,8 ha 193,4 ha 706,7 ha Height Area 1 m 79.81 66.51 9.54 9.37 1-2 m 13.14 26.48 17.45 19.30 2-3 m 5.11 1.81 33.58 26.83 3-4 m 1.70 0.95 34.10 31.32 > 4 0.24 4.25 5.33 13.19 An analysis of the elements exposed to flooding (Table 2) reveals a total of 391 residential buildings, essentially located in the two major towns (Pombal and Soure). In the downstream sections, the flooded area affects mainly farmland and its corresponding infrastructures. It is also significant to note that in all the modelled sections it is not possible to cross the floodplain area in the event of Table 2. Exposed elements in the modeled sections. Exposed element Section A B C D Residential buildings 8 208 156 19 Warehouses, commercial and industrial buildings 1 67 7 3 Social, health and educational facilities 0 3 4 0 Sports and leisure facilities 0 3 1 Transport, sanitation and energy infrastructures 0 7 2 0 Bridges 1 4 3 1 Farm buildings 0 2 15 9 Regional and municipal roads 1 2 3 3 Cemetery 0 0 1 1

flooding. These disruptions would have a serious

effect on regional and municipal socio-economic

flows and connections.

The hydrologic-hydraulic modeling, with new

relevant data and a detailed DTM, in association

with the incorporation of hydraulic and block

structures, and anthropogenic morphological and land use changes, has enabled new flood prone areas to be defined and the water height to be mapped for a 100-year return period. This study can serve as a support element in planning updates, including the Master Plans for the Soure

and Pombal municipalities and the Mondego Hydrographical Basin Plan.

Industrial hazards associated with the eruption of Etna

M.F. Milazzo & G. Ancione

University of Messina, Messina, Italy

A. Basco & E. Salzano

Istituto di Ricerche sulla Combustione, CNR, Napoli, Italy

G. Maschio

University of Padova, Padova, Italy

ABSTRACT

The recent event of Icelandic volcano has focused worldwide attention on the effects of ash fallout in areas prone to this kind of natural phenomenon. In Italy, in the period 2001–2004, Mt. Etna volcano has manifested many times eruptions with great emission of ash (Andronico et al., 2008; Scollo, 2006). As a consequence, significant problems for the resident population, road/rail and air traf fic and production activities have occurred. This paper describes the main objectives of a research project aimed at defining the potentially critical scenarios on industrial installations and infrastruc tures due to eruptions of Mt. Etna. The presence of the industrial area of Catania and the industrial site of Augusta-Priolo, close to the volcano, has evidenced the necessity of a specific risk analysis

related to the industrial hazards associated with volcanoes. The activities presented in this work have been addressed to the analysis of the structural effects, service interruption and malfunction associated with the fallout of ash on industrial installations and infrastructure.

This combination of risk related to the interaction of natural and technological disasters is generally defined as Na-Tech risk. The analysis of volcanic Na-Tech risks related to the eruptions of Etna aims at the definition of vulnerability maps for structures, infrastructure and industrial installations located in potentially affected areas. A methodology for the construction of vulnerability maps may defined as in the following scheme:

1. Selection of representative eruptive scenarios

The analysis of historical data related to eruptions allows to define the representative scenarios in terms of eruption hazard, emission rate and duration.

2. Meteorological modelling

The meteorological model must be built using a

subjected to probabilistic earthquake hazards

Isaac Hernandez-Fajardo & Leonardo Dueñas-Osorio

Department of Civil Engineering, Rice University, Houston, TX, US

ABSTRACT

Physical and functional interdependence between urban distributed systems characterize modern societies. A major drawback of interdependence is intersystemic fragility propagation triggered by external perturbation. This possibility demands accounting of interdependence effects on systemic fragility. Previous research (Hernandez-Fajardo and Dueñas-Osorio, 2011) developed method ologies for including interdependence uncertainty and displayed interdependence consequences in systemic fragility for earthquake scenarios. This paper proposes a new strategy to arriveto fully probabilistic descriptions of interdependent sys temic fragility accounting for the stochastic nature of earthquake hazard. For this purpose, a strategy for probabilistic seismic hazard description pro posed by Adachi and Ellingwood (2008) is inte grated in the proposed methodology. Systemic performance is evaluated using Monte Carlo simu lation by comparing the capacity of interdepend ent systems before and after earthquake action.

Interdependent links act as instruments of damage transmission from a master node in one system to a slave node in another. The failure of a master node in one system induces the failure of a subordinated node in an external system according to a proba bilistic parameter called interdependence strength (Istr) (Dueñas-Osorio et al., 2007) used as uncer tainty accounting tool for the dependence rela tionship. The proposed methodology is applied to a test case of two interdependent real power and water systems in Shelby County, TN, USA. Figure 1 presents partial results on the evaluation of the test case for extreme values of Istr. The comparison of systemic performance for the extreme conditions of systemic isolation and full interdependent operation confirms that interde pendence presence noticeably increases the proba bilistic fragility of the distributed systems involved.

Management of hurricane risk in Florida

J.-P. Pinelli, T. Johnson & G.L. Pita
Florida Institute of Technology, FL, US
K. Gurley
University of Florida, FL, US
S. Hamid
Florida International University, FL, US

ABSTRACT

Florida, due to its geographic location, and the ever increasing population on its coastline, is subject to potentially devastating hurricane damage. The failure of econometric models to predict the insured building losses produced by hurricane Andrew, which hit Florida in 1992, led to the adoption of computer-based catastrophe models, and increased regulation at the State level, including the creation of the Florida Commission on Hurricane Loss Projection Methodology (FCHLPM), as part of an aggressive program of mitigation which includes predicting and evaluating the risk. The Florida Public Hurricane Loss Model (FPHLM) is part of that change in paradigm providing a state-of-the-art loss projection model with a transparent rationale opened to public scrutiny.

The first module of the FPHLM focused on single-family residential homes and has been consistently certified every year by the FCHLPM since 2006. This module was introduced at the 2004 ESREL conference. In subsequent ESREL conferences, the authors showed validation results (2006), and they presented mitigation cost effectiveness studies (2007). A new module

of the FPHLM focuses on projecting losses of commercial-residential multi-family buildings, either condominiums or rental apartments. In addition, the commercial residential module is divided into two almost independent sub-modules: one for low-rise buildings and one for mid/highrise buildings (4 stories or more). This latest module was presented at the 2008 ESREL conference. All three modules contain a meteorology model which defines the hazard, i.e., hurricanes, an engineering or vulnerability model which defines the damage to the structures due to the hazard, and, an actuarial model which converts the damage into monetary losses. In addition, a computer platform integrates the three models into one functioning program. This paper presents an integrated view of all key elements of the vulnerability Model. The paper shows how the FPHLM is part of an overall risk management strategy in Florida, and how the Florida experience might be extended to other areas. In particular the paper deals with the problem of treatment of incomplete or missing data in insurance portfolio files, and the problem of models distribution of time and the capture of information regarding the evolution of building codes and construction practices.

The significance of regulatory framework on safety climate

R.J. Bye & J. Røyrvik

NTNU social research, Trondheim, Norway

G.M. Lamvik

SINTEF, Trondheim, Norway

ABSTRACT

Several studies regarding risk and safety in

marine industry have drawn the attentions

towards a relationship between nationality/

ethnicity of the crew and safety level on board

(Hansen et al., 2002, Håvold 2003, Lamvik & Bye

2004, Håvold 2005, Hetherington et al., 2006,

Hansen et al., 2008, Håvold 2010).

In this paper we show that although there are significant differences in safety climate measures between crew members of different nationality, one can not necessarily conclude that this is due to cultural differences.

The data used in this paper was collected as a part of an explorative study of operational practice on board cargo vessels operating in costal water of Norway. The methods used are a safety climate survey, interviews and observations. The inter views and observations were carried out by three researchers on ten different boats and shipping companies, including 74 crewmembers and 63 peo ple interviewed through 35 structured interviews.

The survey data used in this paper shows an overall poor standard in terms of safety climate. Further, it shows significant differences between (1) Scandinavian speaking, (2) Russian speaking and (3) Filipinos, indicating that safety climate are determined by different nationality/ethnicity. However, observations and interviews shows that working conditions and the formal work contexts vary for people of different nationalities even though they all sail on cargo vessels, own by Norwegian companies, and operating only on the

Norwegian coast.

An apparent difference in the work context of

the different nationalities was the length of the

contract period. The length of contract period due

to i.a. conditions given by flag state/register, may

differ from 1 month to 6 months. The Scandinavians

works normally for 1 month, whereas the Russian

speaking works between 4 and 5 months. The

length of the Filipinos contract period is normally

The use of risk and vulnerability analysis in climate change adaptation

Jens Laugesen

Det Norske Veritas, Høvik, Norway

Bodil Aamnes Mostue

SINTEF Technology and Society, Trondheim, Norway

Ingrid Bouwer Utne

Department of Marine Technology, Norwegian University of Science and Technology (NTNU),

Trondheim, Norway

Jørn Vatn

Department of Production and Quality Engineering, NTNU, Trondheim, Norway

ABSTRACT

A wide range of Risk and Vulnerability Analysis

(RVA) methods exist in the literature and are also

used in relation to climate changes. A traditional

approach to RVA might be sufficient to assess risks and vulnerabilities on a superior level, but for climate change adaption more detailed analyses are often necessary to improve the results. For flooding this involves detailed mathematical and probabilistic modeling of hydrology, surface absorption capacities, snow melting, and failure or breakdown of critical components or system. The challenge is to link the identified threats and vulnerabilities to the risk picture taking physical models and climate projections explicitly into account. The objective of the paper is therefore to extend current RVA methods to combine physical models with results from climate projections. In the paper, a typical approach to RVA is applied to a flooding event and challenges associated with the method and the results of the analysis are discussed as basis for evaluating the need for extensions of the traditional RVA. We propose a seven steps method that integrate the dose-response analysis related to flooding into RVA:

1. Scope and limitations of the study. It is importance to clarify which decisions the risk analyses shall support.
2. Screening. The main objective is to identify

relevant land areas for which, e.g., flooding is

regarded as an important risk element.

3. Physical response model/drainage analysis. The

objective of this step is to establish the neces

sary physical models describing the flooding

situations under various strains (doses).

4. Dose scenarios identification. The purpose

DSB, 1994. Guidelines for community risk and

vulnerability analyses (in Norwegian: Veileder for

kommunale risiko- og sårbarhetsanalyser). Tønsberg:

Directorate for Civil Protection and Emergency Plan

ning (DSB).

Hanssen-Bauer, I., Drange, H., Førland, E.J., Roald, L.A.,

Børsheim, K.Y., Hisdal, H., Lawrence, D, Nesje, A., Sandven, S., Sorteberg, A., Sundby, S., Vasskog, K. & Ådlandsvik, B. 2009. Climate in Norway 2100. Background information to NOU Climate adaptation (In Norwegian: Klima i Norge 2100. Bakgrunnsmateriale til NOU Klimatilplassing), Oslo: Norsk klimasenter.

Total suspended particulate from mobile sources in an Italian opencast

quarry: A proposal to improve US EPA ISC3 model

Guido Alfaro Degan, Dario Lippiello & Mario Pinzari

Dipartimento di Ingegneria Meccanica e Industriale, Facoltà di Ingegneria, Università degli studi Roma Tre,

Rome, Italy

ABSTRACT

In Italy, according to the Goverment Decree

n°152/2006, both air quality standards and quanti

fication of emission rate from pollutant sources, are required to estabilish industrial activities. Among these, quarrying activities, tend to release huge amount of dust and the most common pollutant is represented by Total Suspended Particulate (TSP). The Industrial Source Complex (ISC3) model, cre ated by the United States Environmental Protection Agency (U.S. EPA), is the most diffused model for predicting dispersion of pollutants from industrial facilities and it can be used also in predicting TSP concentration due to opencast quarrying activities. Moreover it defines emission factors and prediction type equations for many quarry dust sources (US EPA, 1998) but past studies, referred only to PM10 fraction, showed that this model tends to over pre dict dust concentration because it does not allow to model mobile source in the proper way such as haul trucks that many studies defined to represent an important fraction of the amount of dust from these activities. So in recent years, an evolution of the US EPA ISC3 model called DCP (Dynamic Component Program) was realized and tested in US opencast quarries. In the present investiga tion the DCP model, set for PM10 dispersion from mobile sources, is developed for TSP fraction and

tested according to field studies and samples real

ized in an Italian opencast quarry extracting basalt.

Moreover the most common emission factors from

haul trucks are tested and once the amount of dust

from mobile sources is defined, the impact on

air quality is assessed according to the developed

DCP model. So, the aim of the present research

can be summarized in two different steps: the first

is represented by the phase of testing TSP emission

EPA, 1998 and Jacko, 1983) for unpaved roads in

an Italian basalt quarry in order to test their accu

racy for the proposed case study. In the second way

a proposal to improve the ISC3 model is developed

in order to suggest a clear procedure to define TSP

Reed, W.R. 2004. An Improved Model for Prediction of

PM10 from Surface Mining Operations, Theoretical

and Experimental Studies. Ph.D. Thesis March 21,

2003, Virginia.

U.S. EPA 1995. User’s guide for the industrial source

complex (ISC3) dispersion models. Vol. I. User

instructions. Research Triangle Park, NC: U.S.

Environmental Protection Agency, Office of Air

Quality Planning and Standards, EPA publication No.

EPA-454/B-95-003a. U.S. EPA 1998. Compilation of Air
Pollutant Emission Factors, Volume I: Stationary Point and
Area Sources, fifth edition AP-42, Revision of Emission

Factors for AP-42 Section 11.9 Western Surface Coal Mining. Research Triangle Park, NC: U.S.EPA, Office of Air Quality Planning and Standards, Emission Factor and Inventory Group, 1998. Nuclear industry This page intentionally left blank

A Fokker-Planck model of pitting corrosion in underground pipelines

to support risk-informed decision making

E.N. Camacho

Risco Ambiental Engenharia, Rio de Janeiro, Brasil

P.F. Frutuoso e Melo

COPPE/UFRJ—Nuclear, Rio de Janeiro, Brasil

P.L.C. Saldanha

CNEN-CGRC, Rio de Janeiro, Brasil

UBM- Campus CICUTA, Barra Mansa, Brasil

E.P. da Silva

Department of Physics, UFRRJ, Rio de Janeiro, Brasil

ABSTRACT

The stochastic nature of pitting corrosion has been recognized since the 1930s. It has been learned that this damage retains no memory of its past. Instead, the future state is determined only by the knowledge of its present state. This Markovian property that underlines the stochas tic process governing pitting corrosion has been explored as a discrete Markovian process by many authors since the beginning of the 1990s for underground pipelines of nuclear power plants.

Corrosion is a genuine continuous time and space state Markovian process, so to model it as a discrete time and/or state space is an approximation to the problem. Recent approaches involving Markovian discrete processes have overcome those difficulties but, on the other hand, a large number of soil and pipe stochastic variables have to be known. We propose a continuous time and space state approach to the evolution of pit corrosion depths in underground pipelines of a nuclear power plant.

The process is modeled by a Fokker-Planck equation which describes the space-time evolution of the transition probabilities among different states. The Fokker-Planck equation is completely determined by the knowledge of two functions known as the drift and diffusion coefficients (Gardiner 1983, Risken, 1984, van Kampen, 2007). In this work we also show that those functions can be estimated from corrosion depths data from in line inspections.

The proposed approach provides a precise and easy way in which the distribution of pit depths and corrosion rate can be obtained, which is criti

Gardiner, C.W. 1983. Handbook of stochastic methods

for physics, chemistry and the natural sciences, Spring

Verlag, Spring Series in Synergetics.13.

Risken, H. 1984. The Fokker-Planck equation, methods of

solution and applications. Berlin: Springer-Verlag. Van Kampen, N.G. 2007. Stochastic Process in Physics and Chemistry, 3 ed. Amsterdam: Elsevier Science & Technology Books.

A review of different approaches for developing process safety

indicators

G.P. Monteiro & P.F. Frutuoso e Melo

COPPE / UFRJ—Nuclear Engineering Program, Rio de Janeiro, Brazil

ABSTRACT

The BP Texas City refinery accident, in 2005, raised

a discussion about the need for process safety indi

cators which could be used as early warnings of

major accidents. The Deepwater Horizon accident

in 2010, which has caused an oil spill of national

significance in the Gulf of Mexico has reinforced

the need for such metrics (BP 2010). Although it is

impossible to prevent accidents from happening in

an absolute sense (Hollnagel 2004), safety metrics

could help preventing as many as possible from

taking place, especially the serious ones.

The research in this field has achieved some

improvement and different dimensions of safety

indicators have been distinguished, such as: personal versus process safety; safety versus risk based; leading versus lagging. The Swiss-cheese model has been used as a frame of reference for establishing indicators in most of the recent publications about these metrics, such as the guide issued by HSE (2006), followed by CCPS (2008) and more recently, API (2010).

However, when evaluating the chain of events involved in an accident it is possible to raise not only technical failures but also human and organizational causes. Although organizational aspects have been included in retrospective analyses, at least since the TMI accident, in 1979, for predictive purposes (such as risk assessment), they have only more recently been included or attempted to be included (Oien et al., 2010). According to these authors, the organizational factors' effect on safety/risk is by no means well understood. The difficulty in defining human and organizational measurable factors which could be logically linked to safety performance has been a common limitation of all recent initiatives regarding process safety metrics. This limitation is tightly coupled with the accident model type adopted. Due to its relevance

when defining indicators, this paper presents a sec

tion dedicated to the discussion about the role of

accident models.

Resilience engineering is an alternative to

Are organizational audits of safety that different from organizational

investigation of accidents?

N. Dechy & J.-M. Rousseau

IRSN, Safety Reactors Division, Human Factors Study Department, Fontenay-aux-Roses, France

M. Llory

Senior Scientist

ABSTRACT

The aim of this article is to discuss the issues that

specialists of human and organizational factors are

facing when conducting safety audits and accident

investigations in high-risk industries. Practically

speaking, what are the differences and similarities

of such inquiries being before the event or after the

event? In particular, is the hindsight bias chang

ing dramatically the conduct (data collection,

judgment, …) and the findings we can expect from

such organizational diagnosis? What are the theo

retical consequences?

At first glance, most of the human factors

and organizational factors competencies used are

similar. The basic processes with data collection, analysis, interpretation and recommendation are similar. So basically we can expect that the fundamentals of organizational analysis (Rousseau and Largier, 2008, Llory and Dien 2010) will be the same in the two configurations. At first glance too, the position to the major event is fundamentally different. This may have critical consequences on the interpretation of decisions and actions which may be judged under the famous hindsight bias when investigators know the end of the story. The discussion will go further than the first glance, and will address some key issues where variations are expected. In particular, the data collection is impacted at levels of documentations and people interviewing. For example, the interviews may not happen in the same social context before and after. Another key issue lies in the conduct of the inquiry which is not relying on a chain of events when auditing. The role of incidents is therefore discussed. The judgment will be affected by evidence available before and after. The way the analysis can be validated and received by target groups is another parameter where variations are occurring. The conditions of assessment and judg

ment are discussed towards the hindsight bias, the

complex phenomena that have to be interpreted

Integrated approach to optimize CAREM 25 nuclear power plant

J.E. Núñez Mc Leod & S.S. Rivera

Engineering Faculty, Cuyo National University, Argentina

ABSTRACT

This paper describe an integrated approach

based on Probabilistic Safety Assessments (PSA)

(Fullwood 2000), operations, tests and mainte

nance schedules for the CAREM 25 NPP. The

focus is on risk regulations and the availability of

the plant when the all issues are considered. In this

way the human factor is a main issue for the use

ful of the results. When we take into account the

human factor, the availability may be strongly pen

alty for the human error, because the safety sys

tems are independently from human intervention.

The implemented model takes into account a

number of specific aspects. These are for example

the factor of aging of components, which reflects

the actions of the time, wear, the environment, etc.,

on the components. Testing intervals and frequency

of maintenance of each component directly affect

ing both the availability and reliability. Also the

implemented model took into account the impor

tance of the shortcomings of common cause in the redundant components and the impact of human error in the reliability of systems.

On the other hand the systems, subsystems and components that does not include in the PSA need taken into account in some way. In this paper we propose that they include from an availability analy-sis.

For this work was developed an Evolutionary Algorithm (Goldberg 1989) specially designed to handle a huge search space, and it handles specifi cally different kinds of restrictions (e.g., restrictions with integer for redundancies and binary values for the inclusion of supervision tasks) Núñez Mc Leod 2007. A new method for the sampling of larger search space was developed by Núñez Mc Leod 2005 significantly to improve the performance of

Reliability analysis of Residual Heat Removal System (RHRS) in nuclear power plant by the GO-FLOW methodology

Chu Yongyue & Yang Ming

“111 Project” Nuclear Power Safety and Simulation, Harbin Engineering University, China

ABSTRACT

In recent years, risk and reliability techniques have been increasingly used to optimize deterministic requirements and to improve the operational safety

of nuclear power plant. Fault Tree (FT) and/or Event Tree (ET) analysis has been most widely used in the tasks of Reliability Analysis (RA) and Probabilistic Safety Assessment (PSA) in large and complex modern industrial systems for evaluating and improving their operation safety, reliability and usability. However, FT and/or ET technolo gies are also criticized for their limitations in deal ing with dynamic characteristics.

GO-FLOW originally invented by Prof. Matsuoka in 1980s is a success-oriented system reliability analysis methodology that can deal with time-related issues. GO-FLOW can not only describe the complex operation time sequences and the system with multiple operating states, but also can calculate the probabilities of system at each time point through a graphical analysis software. However, the applications of GO-FLOW for large and complex industry systems, such as nuclear power plant, are rarely reported.

This paper takes Residual Heat Removal System (RHRS), one of the engineered safeguard systems which play an important role in nuclear safety for restricting the development of post-accident and reducing the accident consequence, as the target

system, and applies GO-FLOW methodology

for analyzing the reliability of RHRS in different

operational stages. The purpose of this paper is to

Semi-quantitative methods in railway signaling—a viable model

for nuclear applications?

H.-P. Berg

Federal Office for Radiation Protection Salzgitter, Germany

S. Griebel

Siemens AG, Brunswick, Germany

ABSTRACT

Faced with the challenge of deriving trustworthy

safety requirements based on accurate input data

and rigorous models, many industries have resorted

to semi-quantitative methods for risk analysis.

These provide an intermediary level between the

textual evaluation of qualitative risk assessment

and the numerical evaluation of quantitative risk

assessment, by evaluating risks. Fault tree and

event tree analysis can be performed on a semi

quantitative level. Mostly, risk matrices are used or

the “bow-tie approach” combining cause and con

sequence analyses in a single diagram.

For the railway signaling industry, a national

pre-standard has been developed which establishes

clear requirements for the construction and appli
cation of such methods. Together with an explicit
risk acceptance criterion from the European
Railway Agency, it enables the user to construct a
rigorous semi-quantitative model.

The nuclear industry is also confronted with the
search for risk acceptance criteria on the basis of
which safety requirements for nuclear power plants
can be derived. As of now, deterministic analyses
and complementing Probabilistic Risk Assessments
(PRA) are performed. PRA is seen as a very pow
erful tool to assess the plant safety level and to pri
oritize necessary improvements to enhance safety.
However, this comprehensive method requires
credible data for reliability concerning failures of
structures, systems and components; otherwise the
uncertainty of results strongly increases. Therefore,
a semi-quantitative assessment might be a viable
approach for specific aspects, e.g., the treatment
of specific human actions. At present, a semi
quantitative approach is used This paper aims at
presenting the current status of the application of
semi-quantitative methods both in theory and in
practice. It highlights the characteristics of cur
rently used methods and deals briefly with some