Probabilistic Risk Assessment: Frontiers and Prospects

Invited Seminar
for
College of Safety and Ocean Engineering
China University of Petroleum-Beijing (CUP)

By

Prof. Mohammad Modarres
Center for Risk and Reliability
University of Maryland

November 1, 2022

Summary of the Talk

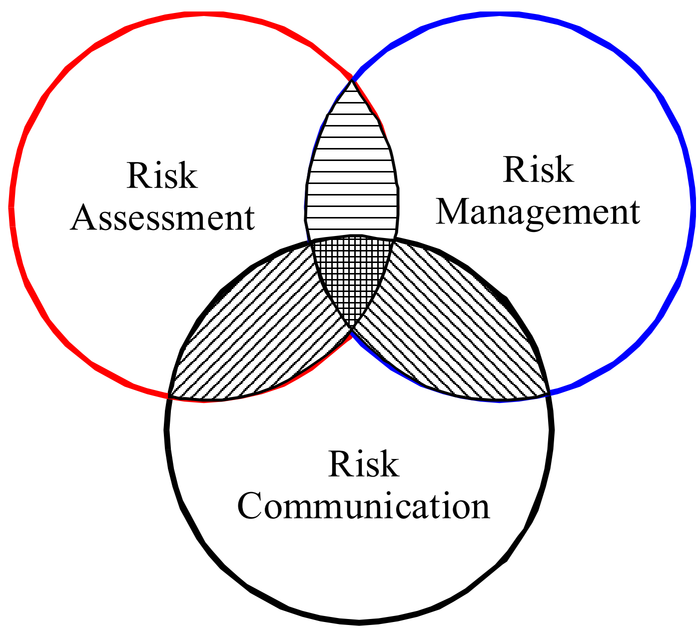
- Risk Analysis and Risk Assessment Preliminaries
- Critical Elements of Probabilistic Risk Assessment (PRA)
- Strengths of PRA
- Establishment and Uses of Risk Acceptance Levels for Risk Management
- What PRAs Tell Us?
- Frontier Research in PRA
- Future PRAs
- Conclusions
- Questions

ELEMENTS AND TYPES OF RISK ANALYSIS

- Risk analysis attempts to measure the magnitude of expected losses (consequences) associated with complex systems, including evaluation, risk reduction and control policies.

- Three types of risk analysis: Quantitative, Qualitative and a Mix of the two

- Three elements (constituents) of risk analysis are:



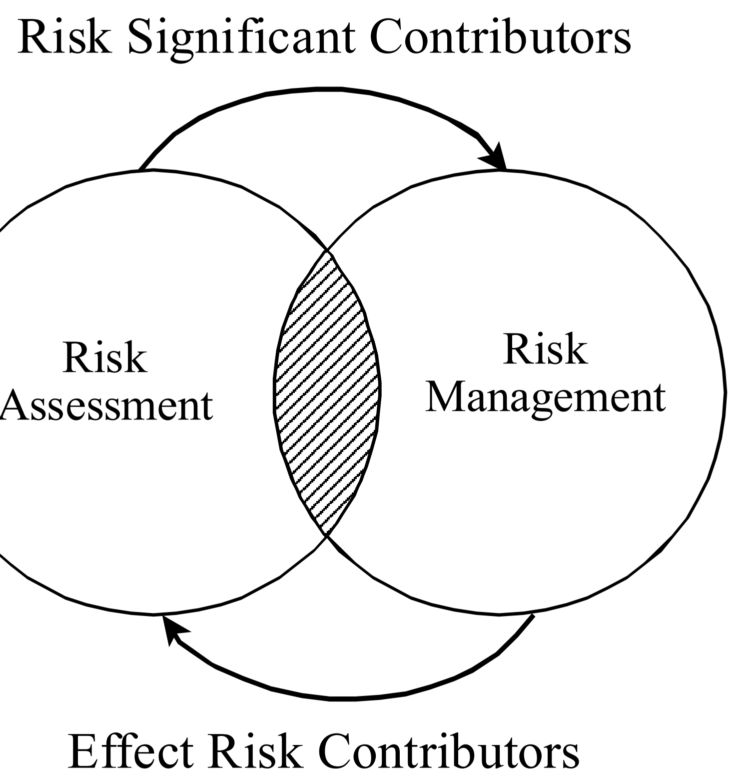
ELEMENTS OF RISK ANALYSIS

Risk assessment is the process through which the **frequency of a loss** by or to an engineering system is estimated and the **magnitude of the loss (consequence)** is calculated.

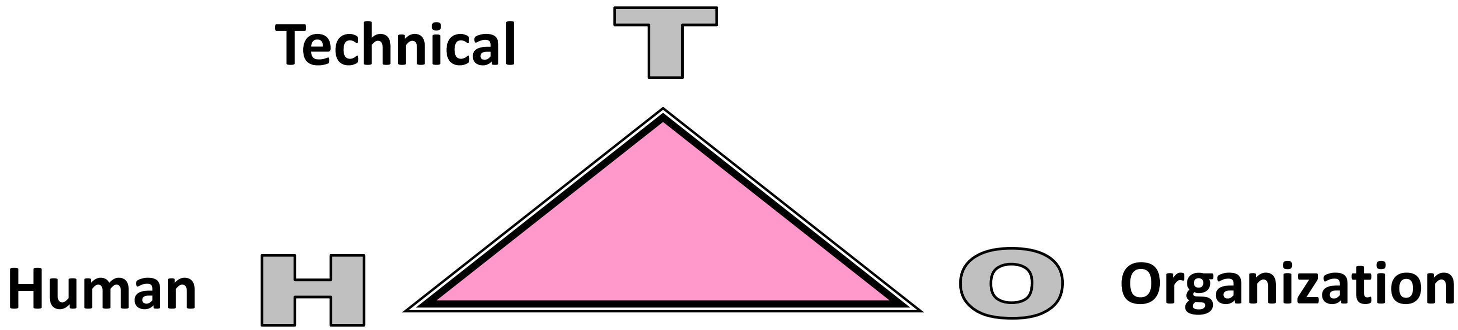
Risk management is the process through which **magnitude and contributors to risk** are estimated, evaluated, minimized, and controlled.

Risk communication is the process through which information about the nature of risk (expected loss) and consequences, risk assessment approach and risk management options are exchanged, shared and discussed between the decision makers and other stakeholders.

Risk Assessment Preliminaries: Risk Assessment vs. Risk Management



Risk Assessment Preliminaries: Complex Systems



6

Risk Assessment Preliminaries: Risk Triplets

- Risk assessment answers three basic questions known as Risk Triplets [Kaplan & Garrick, 1981]:

  1. What can go wrong?
  2. How likely is it?
  3. What are the losses (consequences)?

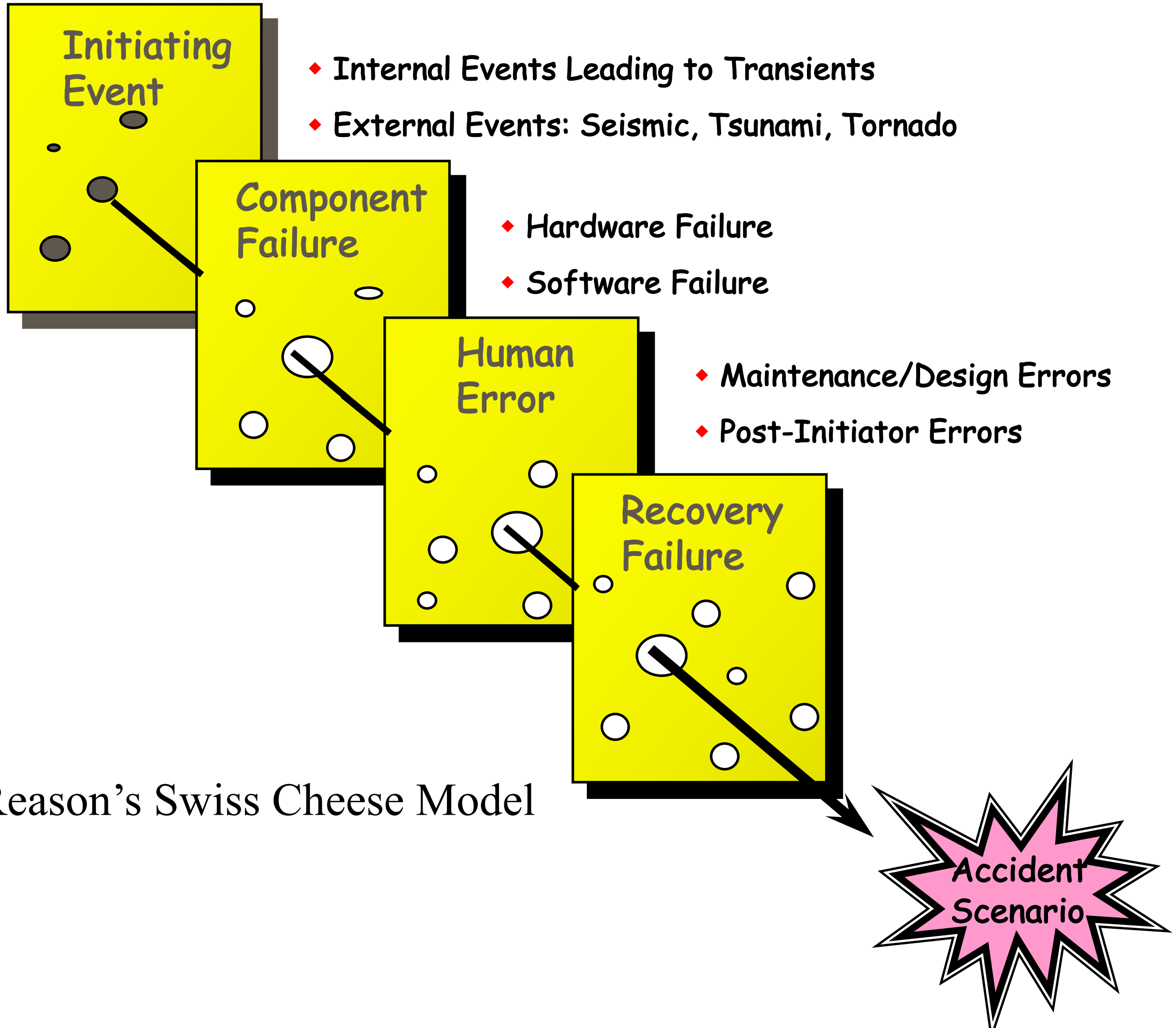
- Answering these questions require significant amount of expertise, analyses and probabilistic modeling.

Risk Assessment Preliminaries: Risk Triplets (Cont.)

What can go wrong? Develop Scenarios	How likely is it? Determine probability or frequency of scenarios	What are the losses? Estimate losses to humans, environment, other living species and other asset
S_1 S_2 S_3 . . . S_N	f_1 f_2 f_3 . . . f_N	C_1 C_2 C_3 . . . C_N

$$\text{RISK} = \langle S_i, f_i, C_i \rangle$$

Probabilistic Risk Assessment Process: Scenario Development



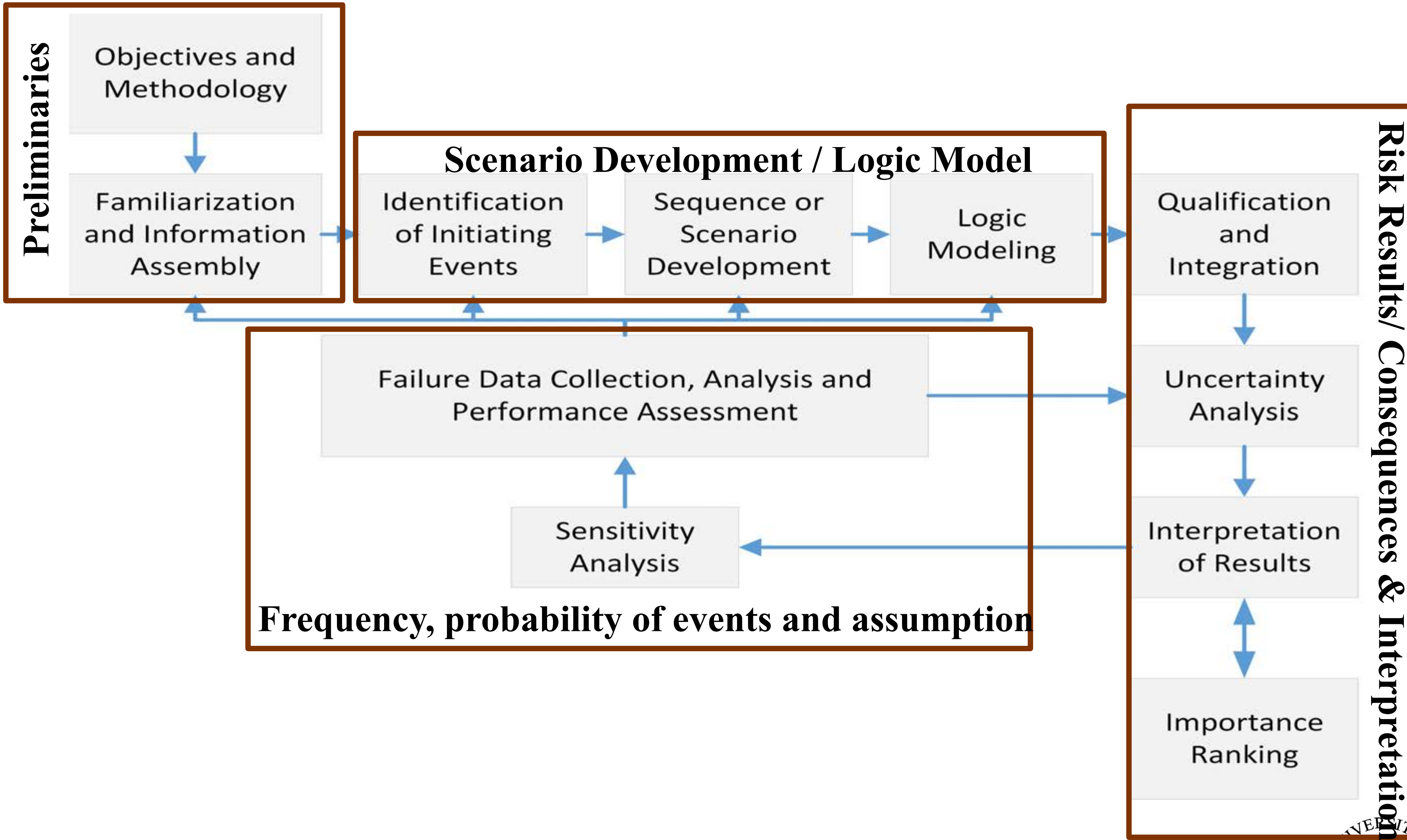
- Internal Events Leading to Transients
- External Events: Seismic, Tsunami, Tornado

- Hardware Failure
- Software Failure

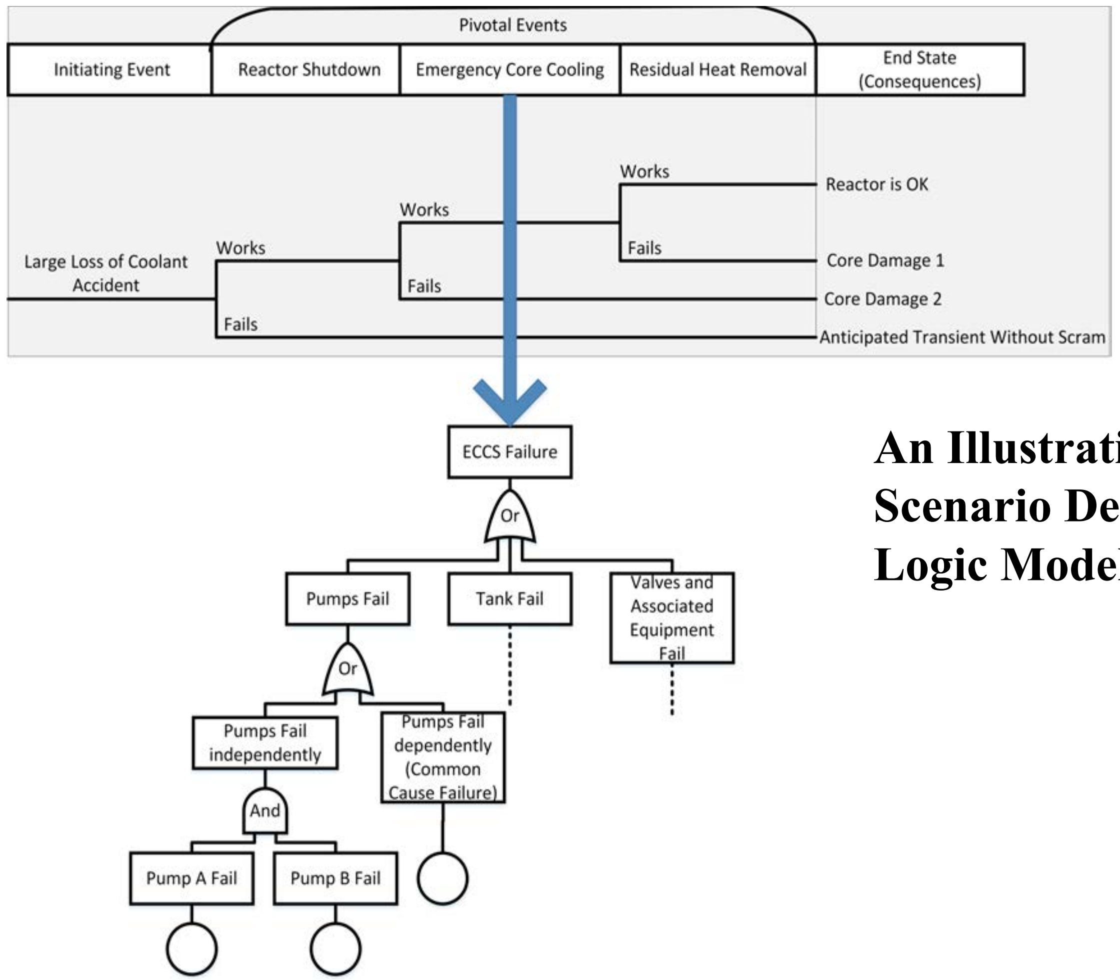
- Maintenance/Design Errors
- Post-Initiator Errors

J. Reason's Swiss Cheese Model

Probabilistic Risk Assessment Process (Cont.)



Probabilistic Risk Assessment Process (Cont.)

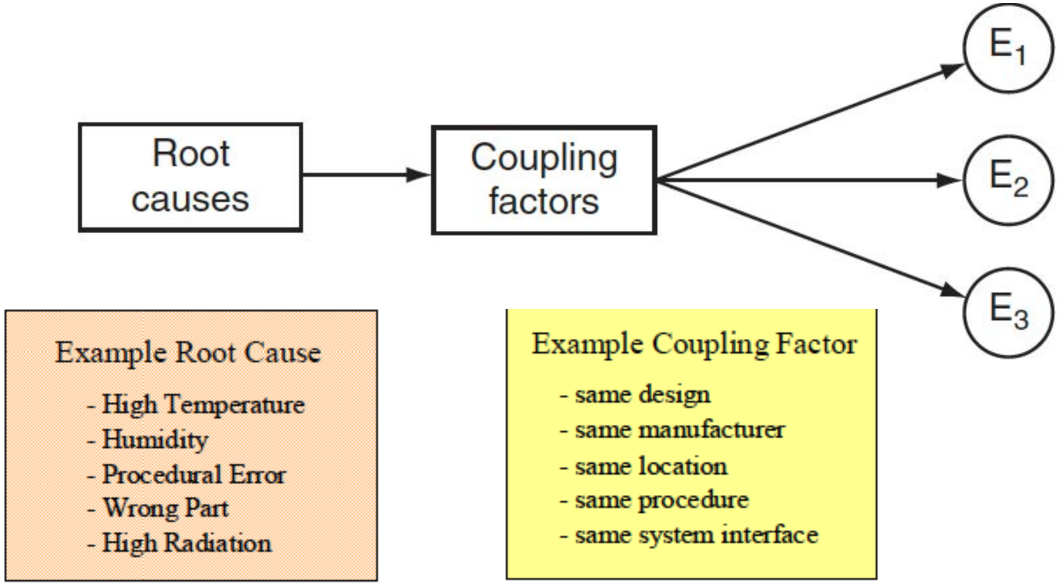


An Illustration of the Scenario Development / Logic Model Part of the PRA

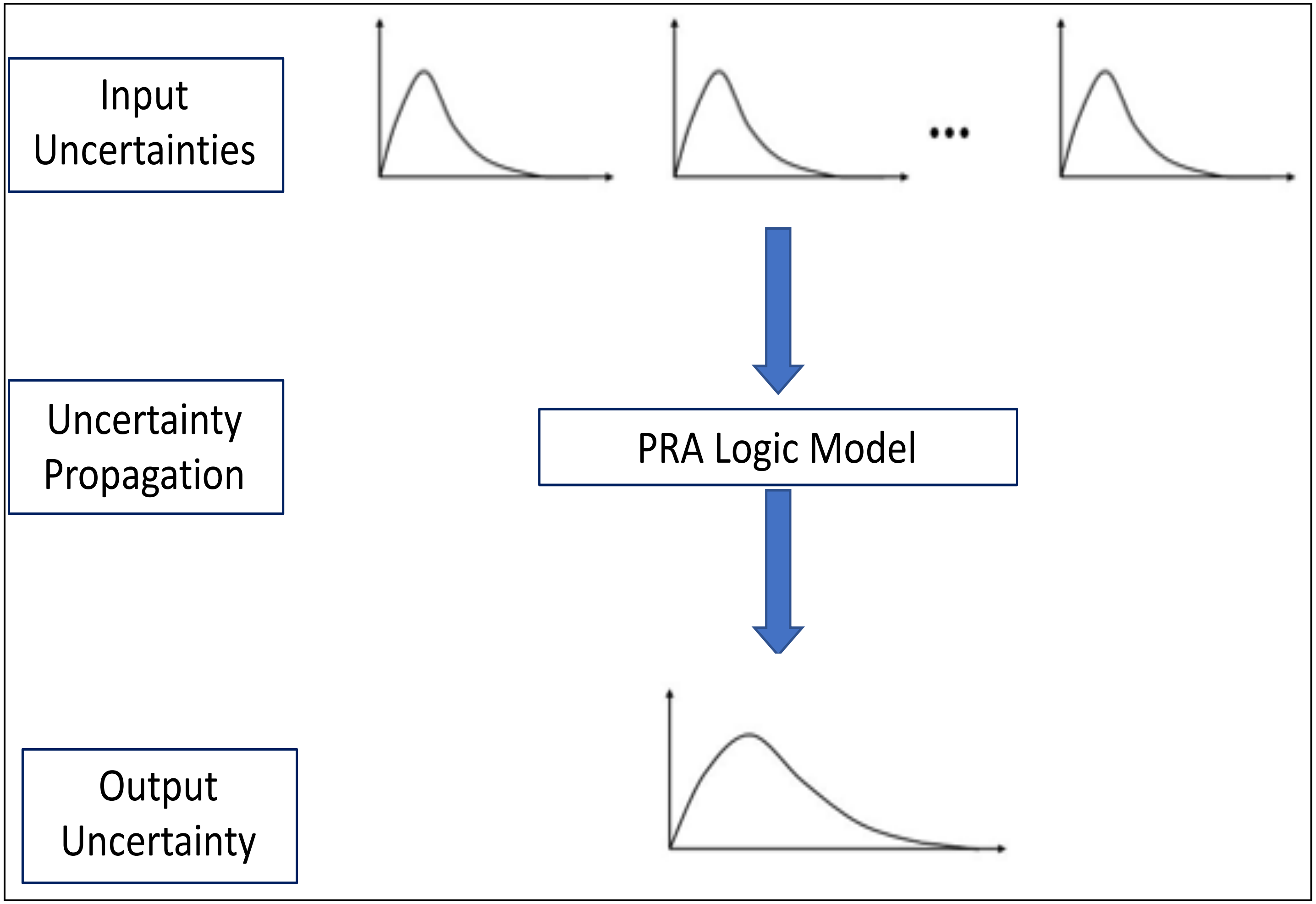
Critical Element of PRA: Common Cause Failures

A common cause failure (CCF) is an implicit dependent failure where:

1. Two or more items fail within a specified time leading to system failure, loss of redundancy or degradation.
2. Item failures result from a single shared cause and coupling factor (or mechanism)



Critical Element of PRA: Uncertainty Analysis



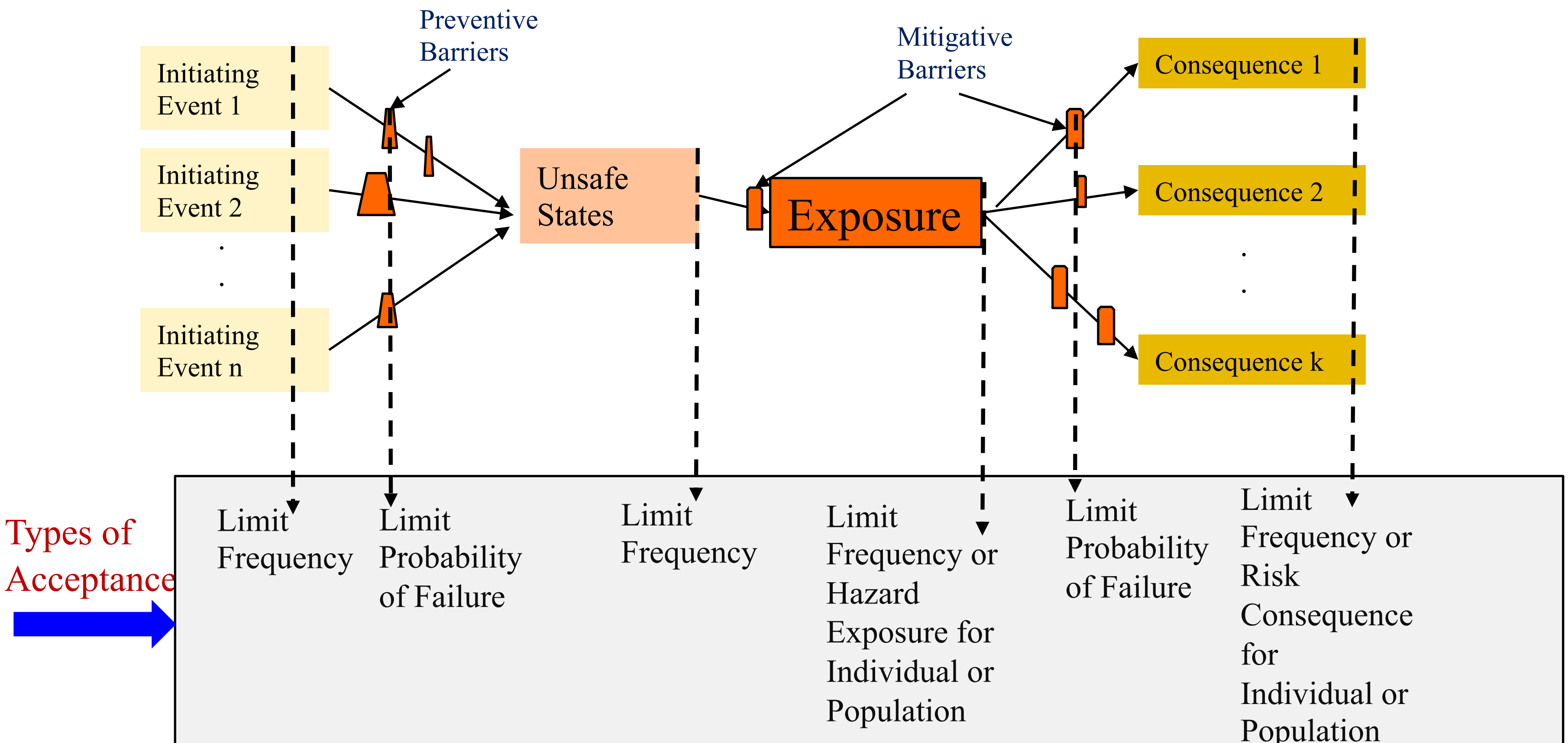
Strength of PRA

1. Integrated and systematic examination of most design and operational features of a complex system.
2. Include interactions and human-system interfaces.
3. A model to formally incorporate operating experiences.
4. Explicit consideration of uncertainties.
5. Analyzes competing risks (e.g., list of risk-significant elements).
6. Analysis of assumptions and data issues via sensitivity studies.
7. Provides a measure of the absolute or relative importance of human, hardware & software components in a system.
8. Provides a quantitative measure of the overall level of health and safety for the engineered system.

What to Learn From Past Risk Assessments

- Formal PRA models can provide important realistic static and dynamic scenarios and contributors to operational and accidental risks in design and operation of systems
- The PRA models can be updated through streams of sensor data, sentimental conditions, temporal state of the facility
- PRAs may serve in support of risk management and policy decision making to predict, avoid and mitigate accidents
- PRA can learn by updating its risk models with near-miss events and specialize itself to a specific facility, operator and environment
- Analysis of significant risk scenarios provide an organizational learning resource

Establishment and Uses of Risk Acceptance Levels for Risk Management



Classes of Frontier Research in PRA

Automating Everything

- Computers take on mundane tasks
- Maximum use of AI
- Real-time risk values
- Integration with risk management and instant risk-informed decision making
- Proactive risk management vs. reactive risk-management

Integrating Human and Organizational Behaviors

- Organizational impact on risk values
- Ability to detect risky behaviors / errors
- Just-in-time training and education
- Monitoring workforce attitudes and risky behaviors (safety culture)
- Best practices and standards developments

Classes of Frontier Research in PRA (Cont.)

- Collecting 24/7 Risk Information and Data
  - Condition monitoring and prognosis and health management
  - Innovative monitoring, processing and learning from performance data
  - Advance computational capabilities to use and fuse big data
  - Advance IoT concepts in risk and performance collection data
- Learning from Incidents
  - AI use in understanding incident and near-miss reports and mapping to PRA
  - Automate "what-if" scenarios
  - Develop and understanding of and monitor emerging threats
  - Establish adequate system resilience
  - Mitigative measures, especially for natural hazards

Classes of Frontier Research in PRA (Cont.)

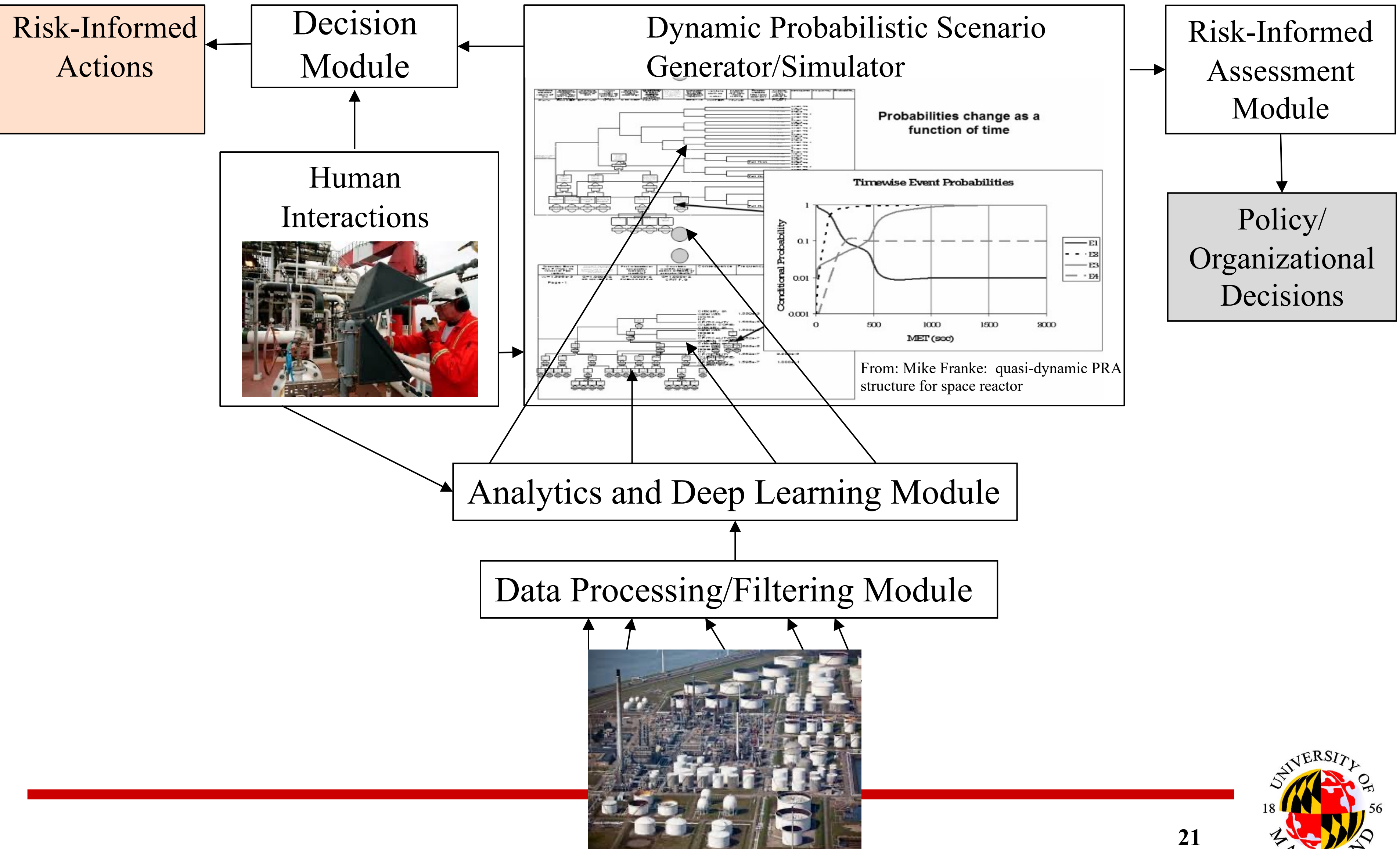
- Establishing risk acceptance and risk tolerance (how much risk is enough or how safe is safe enough)
  - How to establish an absolute and relative risk limit to show time varying risk margins
  - Where and how to move forward safely within a set risk tolerance

- Integrating / Aggregating Risks from Diverse Sources
  - Integrate risks of various hazards into a single risk metric to compare against risks acceptance levels
  - Uncertainty analysis
  - Modeling consequences of hazard exposures

Key Areas of Research Applications

- **Infrastructure Safety-Security-Resilience (SSR)**
  - Electronic Information Flow Embedded in Nearly Every Aspect of Life
  - Integrity of Complex Systems and Networks: Cyber-Human-Software-Physical (CHSP) Systems
  - Highly Connected Infrastructure Networks: Electricity, Gas, and Water Pose Major Societal Risks Through Cyberspace Attacks
  - Societal Disruption, Health, Safety and Resilience Goals
- **Life-Cycle Risks of Advanced Energy Systems**
  - Renewable Systems (Building, Environmental, Internal and External)
  - Nuclear Energy (Fission and Fusion)
  - Climate Change Risks of Disruptions in Sustained Energy Supply
  - Pipeline safety
- **Simulation-Based Dynamic Probabilistic Risk Assessment**
  - High Power Computing Leading to Less Inductive Risk Models
  - More Deductive Computer-Assisted Risk Scenario Generation

Future of Real-Time Risk Assessments & Management



Conclusions

- PRA forms the basis for risk-informed decision making
- Supports test and maintenance planning and optimization
- Supports safety upgrades
- Significant development experiences and standards in developing and proper uses of PRA models exist
- Used to develop and show adherence to acceptable risk levels
- Supports compliance to regulatory requirements
- Old methods of safety analysis are insufficient for complex technologies
- Major accidents could prove disastrous to the vitality of an industry
- Risk-informed approaches characterize uncertainties and risk contributors
- Several exciting research activities are ongoing to mix PRA with AI & modern machine learning methods and technologies

Thank you!

Questions?