Summary and Presentation Slides from: Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions

April 26, 2019

Organized by: The Center for Risk and Reliability

A.J. Clark School of Engineering University of Maryland College Park, MD

Co-sponsors: American Society of Mechanical Engineers (ASME) and Ford Motor Company

Summary

UMD Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions

We have witnessed remarkable technology advancements and competitions in autonomous and connected transportation vehicles. These include major developments of self-driving electric cars by new technology development companies such as Waymo and Tesla, and by the traditional automobile manufacturers that include the Ford Motor Company, Mercedes-Benz and Rolls-Royce.

In this rapidly changing world, cities are growing fast. With urban centers dealing with record levels of traffic and pollution, the United Nations has identified increasing urbanization as one of the defining trends of the 21st century. This growth is also causing a shift from individual vehicle ownership to the use of shared mobility options such as ride-hailing services. Most of our infrastructure was built to meet the needs of individually used vehicles. However, most of those vehicles sit idle about 95% of the time. Because of this, as much as 30% of the real estate in city centers is devoted to parking.

The Ford Motor Company, for example, sees this as an opportunity to design smart vehicles for a smart world. If applied correctly, new technologies can enable solutions to help city transportation systems improve the quality of life for everyone. That's why Ford is approaching these opportunities in a holistic way. The company recognizes that just injecting new mobility technologies and services into a city or neighborhood won't solve their existing challenges and may even make them worse.

While technology development has been the prime focus of the most recent technology innovations, the industry's advances on the issues of safety, risk and reliability has been slow. A number of accidents and near-misses have already occurred, the mean distance driven to an unsafe condition, near miss or accident has been far shorter than the conventional road vehicles.

While the public at large is extremely excited about these technologies, concerns over safety, software reliability, security, hacking/misuse, and licensing are mounting. Given some vacuum in formal safety, risk, and reliability considerations in this of rapidly evolving transportation technology, convergence of many related resources involving academia, autonomous vehicle industry, insurance and related government agencies would be desirable to identify and address the related technology, policy and regulatory developments needed.

Far more attention by the industry and research by the government would be needed to close these safety gaps. Some of the major issues identified by the workshop as examples of the safety improvement needs include:

- Need to develop more case studies.
- Building of more incentives on the part of the industry to promote, further satisfy and engage with NHTSA
- Development of clear top-down safety requirements.
- Reliance on more modern safety and risk-based analysis methods and simulations.

- Avoidance of using the old safety analysis methods practiced in the conventional level-0 and level-1 vehicle technologies, and develop new out-of-the-box safety methods.
- Investigate and optimize the use of more redundancies in the safety equipment of driverless vehicles.
- Develop approaches for better safety enforcement
- Understand, study and model the role of human behavior and intensions in fully autonomous vehicles.

PROGRAM
Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions
April 26, 2019
Kay 1-2 Boardrooms
A.J. Clark School of Engineering
University of Maryland
College Park, MD USA

8:00-8:30 Registration, Coffee and Donuts

8:30-8:45 Welcome Messages and Objectives

Prof. Mohammad Modarres, Nicole Y. Kim Eminent Professor of Engineering, University of Maryland (UMD)

Prof. Darryll J. Pines, Nariman Farvardin Professor and Dean A.J. Clark School of Engineering, University of Maryland

8:45-9:15 Sponsors Messages: ASME and Ford Motor Company Interests in Autonomous Vehicles (Dr. M. Pourgolmohamad, ASME SERAD Chair-Elect, Sr. Manager at Johnson Controls Inc., Moderator)

Dr. Said Jahanmir, President of ASME

Dr. Vasiliy Krivtsov. Director of Reliability Analytics, The Ford Motor Company

9:15 – 10:15 (Part I) Advances in Safety and Coordination Frameworks of Connected Autonomous Vehicles (Dr. Mark Fuge, Assistant Professor UMD, Moderator)

Prof. Phil Koopman, Associate Professor of Electrical and Computer Engineering, Carnegie Mellon University
Assuring Autonomous Vehicle Safety

Autonomous vehicles bring with them the promise of dramatically reduced road mishaps. However, making self-driving cars as safe as a person is more difficult than is widely acknowledged. Unimpaired human drivers, while imperfect, are actually quite impressive. While computers don't drive drunk, they do have failure modes that differ dramatically from humans, especially in the area of perception. Ensuring safe deployment of this technology will require significant augmentation to existing safety standards. In particular, we will need to find a responsible way manage uncertainty as a first class citizen, and to determine an acceptable level of risk tolerance while we wait the years it will take for the technology to mature.

Prof. Andreas A. Malikopoulos, Terri Connor Kelly and John Kelly Career Development Associate Professor, University of Delaware
A Decentralized Energy-Optimal Control Framework for Connected and Automated Vehicles

We are currently witnessing an increasing integration of energy and transportation, which, coupled with human interactions, is giving rise to a new level of complexity in the next generation of transportation systems. Connected and automated vehicles (CAVs) provide the most intriguing and promising opportunity for enabling users to better

monitor transportation network conditions and make better operating decisions to reduce energy consumption, greenhouse gas emissions, travel delays and improve safety. While several studies have shown the benefits of CAVs to alleviate traffic congestion and reduce fuel consumption in specific transportation scenarios, one key question that remains unanswered is "how much can we improve fuel consumption, if we assume that the vehicles are connected and can exchange information with each other and with infrastructure?" In this talk, I will present a decentralized optimal control framework whose closed-form solution exists under certain conditions, and which yields for each vehicle the optimal acceleration/deceleration at any time in the sense of minimizing fuel consumption. The solution allows the vehicles to cross the intersections and merging roadways without the use of traffic lights, without creating congestion, and under the hard safety constraint of collision avoidance.

10:15- 10:30 BREAK

10:30 – 12:15 (Part II) Policy, Technology and Regulatory Initiatives (Dr. Lei Zhang, Ph.D. Herbert Rabin Distinguished Professor, Director, Maryland Transportation Institute, Moderator)

Mr. Gregory Slater, Administrator, Maryland Department of Transportation
Maryland Cybersecurity Initiatives in a Connected and Autonomous World.

The rise of new technologies has and will continue to increase mobility choices that test the State's transportation resiliency. Maryland Department of Transportation State Highway Administration's (MDOT SHA) Administrator Mr. Gregory Slater will provide a brief overview of MDOT SHA's initiatives in the digital infrastructure world, how we plan to support public needs and shape a safe and efficient transportation network.

Ms. Dee Williams, Deputy Associate Administrator for Vehicle Safety Research, National Highway Traffic Safety Administration (NHTSA), U.S. Department of Transportation
NHTSA's FMVSS Considerations for Vehicles with Automated Driving Systems

The presentation will cover NHTSA's policy, research, and regulatory efforts under consideration at the Agency for vehicles equipped with Automated Driving Systems (SAE L3-L5).

Ms. Marjory S. Blumenthal, Director, Science, Technology, and Policy Program
RAND Corporation, Washington, DC Office
Measuring Automated Vehicle Safety: Building Better Outcomes and Policy

Public trust—and the public interest—in automated vehicles demands understanding of how safe they are, especially once they operate on public roads. Today, the race to develop working and, ultimately, commercially deployed AVs is characterized by idiosyncratic approaches. Not only do developers make different choices for their essential technologies, they approach testing in different ways and they report testing results both selectively and in developer-specific ways, even when seeming to use the same measure. Recently completed research shows how it is possible to have a framework for measuring AV safety that is technology- and company-neutral. Using such a framework would foster both comparability across companies and vehicles and broader understanding of the safety performance of AVs as they progress through development to deployment. Such a framework could be complemented by additional steps to foster transparency and comparability. Public policy provides the backdrop and shapes the incentives for progress that also involves collective action by industry.

Prof. Mohammad Modarres, Director Center for Risk and Reliability (CRR)
What we can learn from risk-informed approach to regulating nuclear power plants?

This presentation offers an overview of the way risk of accidents has been addressed in design and operation of nuclear power plants by the nuclear industry in the U.S. It draws a parallel between the early stages of the nuclear energy development and the current trends in the autonomous vehicle development. The presentation points to

nuclear industry's efforts to restore and manage safety over its 60 years history. On the basis, conclusions will be drawn about the relevance of the formal probabilistic risk assessment and risk-informed decision making to autonomous vehicles design and policy development.

12:15-1:45 LUNCH Speaker: Dr. Roger McCarthy, P.E., McCarthy Engineering (Welcome and introduction by Dr. Bala Balachandran, Minta Martin Professor of Engineering and Chair, Department of Mechanical Engineering)

No vehicle technology has caused more excitement, investment than potential vehicle "autonomy" (SAE or NHSTA level 4 & 5). Since the "critical pre-crash event" of ~94% of US traffic accidents is a "driver critical reason(s)," vehicles driven by a fast-autonomous agent that does not blink, sleep, drink, etc. spawn "predictions" of unprecedented safety impact. Autonomous vehicle potential to revolutionize western economies is inestimable. The 8% utilization of current automobiles could increase 10X as autonomous cabs. The vast tracts of real estate now dedicated to road side parking, driveways, and garages could be reclaimed.
Unfortunately, the "hype" surrounding all US self-driving vehicles, even though they are using somewhat different technologies, significantly overstates the current capabilities of the technology, and the foreseeable improvements in the next few years to operate on normal road interacting with human drivers. This is apart from autonomous vehicles having no demonstrated ability in snow or rain, which accounts for the overwhelming testing miles in sunny states. The early overall crash rates for self-driving prototype vehicles under ideal conditions has been less than promising, even though virtually always the fault of the other driver. The actual safety record of Tesla's "autopilot," while less than true autonomy, is not a cause for optimism.
Because of these challenges, and issues of lability, security and privacy, the most significant active accident prevention will increasingly result from the deployment of automatic "backup" systems that monitor the driver, automatically intervene to prevent crashes, but don't actively drive. An example is 99% of new vehicles in the US Market by 2022 will have an automatic emergency braking (AEB) system.

1:45 – 3:00 (Part III) Experiences and Advances in Safety of Autonomous Marine Vehicles (Dr. Katrina Groth, Assistant Professor UMD, Moderator)

Prof. Ali Mosleh, NAE, Distinguished Professor and Evelyn Knight Chair in Engineering, University of California, Los Angeles (UCLA).
Highlights of the First International Workshop on Autonomous Systems Safety, Reliability, and Security

The First International Workshop on Autonomous Systems Safety (IWASS-1) was recently held in Trondheim Norway, co-sponsored by UCLA and Norwegian University of Science and Technology (NTNU). The objective of the workshop was to identify common challenges related to safety, reliability and security (SRS) of autonomous systems, and propose possible solutions for those challenges. A white paper distributed to the attending 40 experts from academia, industry, and governmental agencies, proposed the following topics as the focus of the workshop: How to make the case for autonomous system SRS; (b) Approaches to modeling and analysis of autonomous systems SRS; (c) Risks and benefits of human being in the loop; and (4) Issues in establishing safety standards, oversight, regulations, and liability. Two and half days of plenary presentations and discussions by four breakout groups on these subjects resulted in preliminary conclusions presented at the end of the workshop. This talk will summarize the key findings of IWASS-1 and provide a personal perspective on the challenges in assuring Safety, Reliability, and Security of autonomous system.

Dr. Jeevith Hegde, Postdoctoral Fellow, Department of Marine Technology, Norwegian University of Science and Technology, Norway.
Development of Safety Envelopes for Underwater Vehicles

This talk presents the implementation of dynamic safety envelopes for Autonomous Remotely Operated Vehicles (AROVs). A safety envelope is defined as a three-dimensional spatial area around the AROV, which forms a virtual

protective barrier against collision with known and unknown obstacles in the subsea environment. The Octree method is used to setup the cuboidal shape of the proposed safety envelope. A Fuzzy Inference System (FIS) is modeled to derive the size of the dynamic safety envelope. The three inputs of the proposed FIS are vehicle velocity, probability of acoustic sensor failure and time to collision risk indicator. A user interface allows for verification and visualization of the resulting dynamic safety envelope during live laboratory tests. The results show that similar to vehicular envelopes in other industries, dynamic safety envelopes can be implemented on AROVs. Dynamic safety envelopes may also be used to model the behavior of AROVs when confronted with different collision scenarios.

Dr. Mario Brito, Associate Professor in Risk Analysis and Risk Management, University of Southampton, UK
From autonomous underwater vehicles to unmanned marine surface vehicles: Reflections on risk models and expert judgment elicitations

Over the years, risk models have been developed to manage different types of hazards for marine autonomous systems. In this talk I will present a review of different models, discuss their effectiveness and limitations.
The risk model can be informed by historical failure data, subjective expert judgments or by a combination of these two sources of assessments.

When we attempted to combine historical data with expert subjective judgments, we realised that a new type of survival models was required. I will discuss this model and how this has been used to support actual decision making of marine autonomous systems operations in extreme environments. I will also discuss extensions to this model to capture other types of hazards.

3:00-3:15 BREAK

3:15 – 4:15 (Part IV) Autonomous Vehicle Traffic Safety and Trajectory Planning Research (Dr. Jeffrey Herrmann, Professor of Mechanical Engineering and Institute for Systems Research, UMD, Moderator)

Prof. John Baras, Lockheed Martin Chair in Systems Engineering and Distinguished University Professor, Electrical and Computer Engineering, University of Maryland
Assured and Composable Safety in Connected Autonomous Vehicles

Prof. Gang-Len Chang, Director, Traffic Safety and Operations Lab., Department of Civil Engineering, University of Maryland.
Managing AV flows under different levels of highway congestion: A case study of MD100 congestion management

Recognizing the need for responsible highway agencies to effectively manage emerging AV flows in contending with daily recurrent congestion, this study has presented a systematic procedure for understanding the AV flows' impacts on the traffic conditions under different AV behavioral mechanisms (i.e., car-following and lane-changing), penetration rates.. Our research results have indicated that the presence of AV flows, depending on their adopted behavioral mechanisms, may have significant (either positive or negative) impacts on the overall traffic conditions. Hence, it is essential for responsible highway agencies to have proper operational guidelines to manage and coordinate with AV flows. To demonstrate the proposed methodology, this study has further conducted simulation experiments using a congested segment of MD-100 network under various AV penetration rates and behavioral mechanisms. The collected MOEs highlight that at each AV penetration level there exists a set of optimal behavioral mechanisms for the AV flows to coordinate with non-AV flows via the V2I or V2V infrastructure so as to maximize the roadway capacity and minimize the resulting highway congestion.

4:15-4:30 BREAK

4:30 – 5:30 OPEN DISCUSSION

5:30: ADJOURN

Autonomous Vehicles: Issues and Future Directions

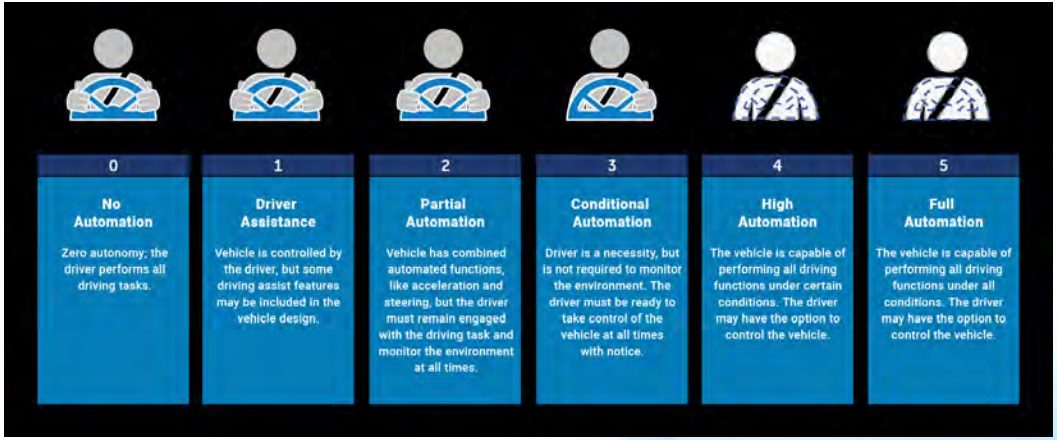
SAID JAHANMIR, PH.D.

ASME PRESIDENT

26 APRIL 2019

Road to Automation

- Safety
- Economics
- Mobility
- Efficiency and Convenience
- Levels of driver assistance technology to full automation



NHTSA

Future of Mobility, New Ecosystem

» Smart & Reliable Infrastructure

» Broadband & Cybersecurity

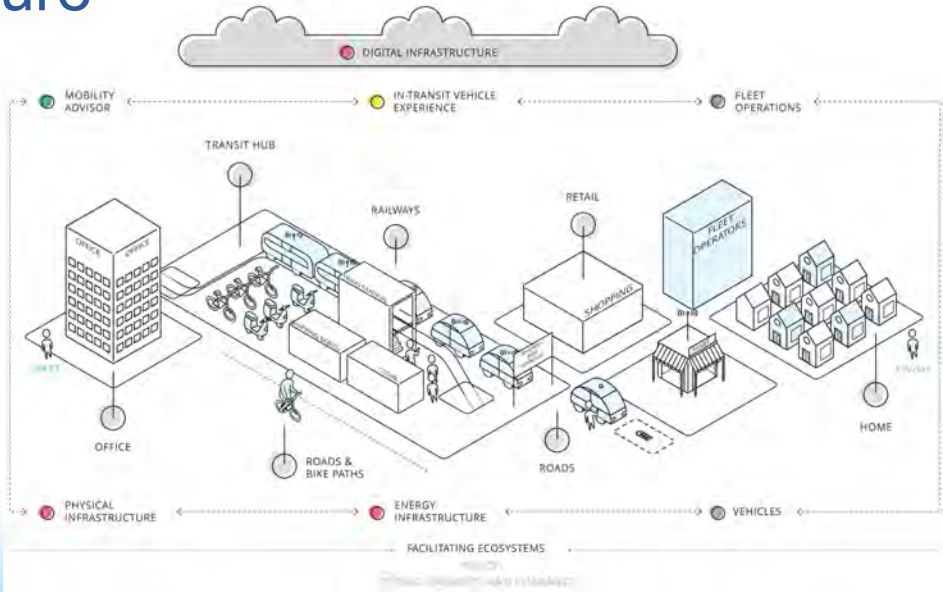
» Vehicle Technology

» Sensors & Software

» Standards

» Regulations

» Education



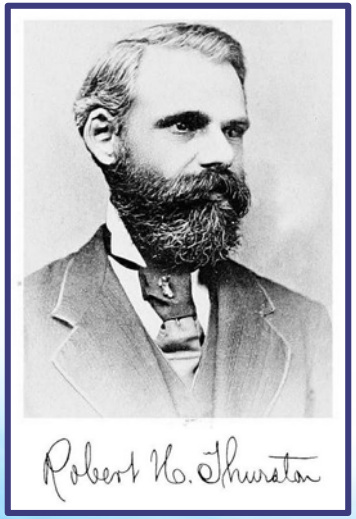
Role of Engineering Societies

- The engineering community focused on design, safety, reliability and efficiency.
- Forum for technology discussions and dissemination
- Educating the public for acceptance
- Advocacy to legislative/regulatory bodies
- Development and dissemination of standards

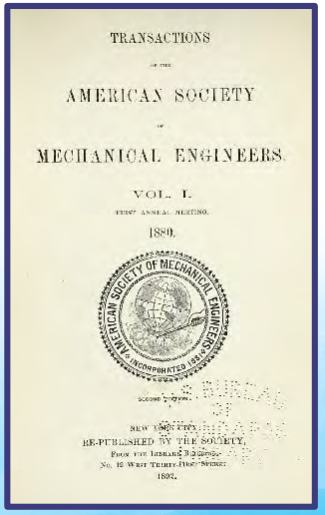
ASME
SETTING THE STANDARD

History of ASME

Creating, recording & sharing the activities of a Society
"founded on a vision of a world served by mutual cooperation and aimed at mutual welfare"



- **Discipline of Mechanical Engineering established in 1870 at Stevens Institute of Technology**
- **ASME Charter, 1880 "to meet and associate together to read and discuss professional papers, and to circulate by means of publication among its members"**
- **Annual *Transactions* documented vibrant early years of professional meetings and published papers**
- **President Robert H. Thurston provided guiding philosophy for Society's aim: "Care of self, of family, of friends, of fellow-citizens and of mankind."**


TRANSACTIONS
OF THE
AMERICAN SOCIETY
OF
MECHANICAL ENGINEERS.
VOL. I.
FIRST ANNUAL MEETING.
1880.
AMERICAN SOCIETY OF MECHANICAL ENGINEERS INCORPORATED 1880
SECOND EDITION.
RE-PUBLISHED BY THE SOCIETY,
1892.

ASME
SETTING THE STANDARD

The ASME Family

Members – Volunteers – Staff – Customers

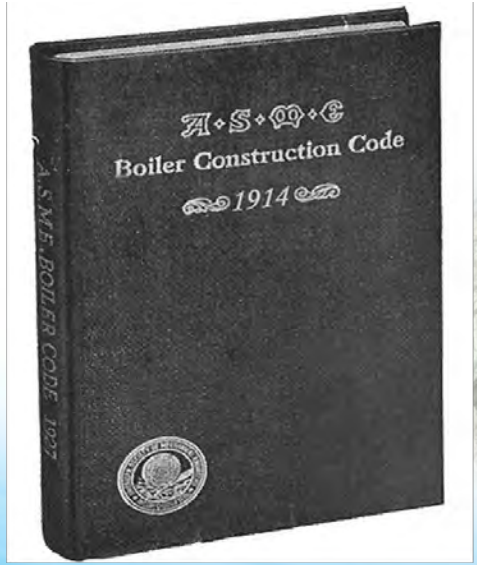
- 100,000+ Members
- 35,000+ Volunteers
- 28,000+ Students
- 1,000+ Sections & Student Sections
- 36 Technical Divisions
- 700 Code Committees (500+ Standards)
- 570,000+ Social Media Followers

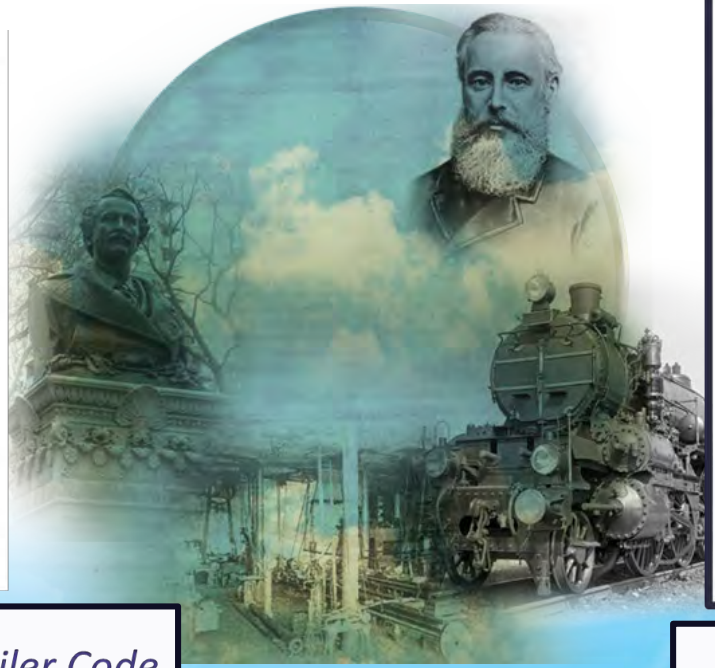
All Working Together Toward One Objective

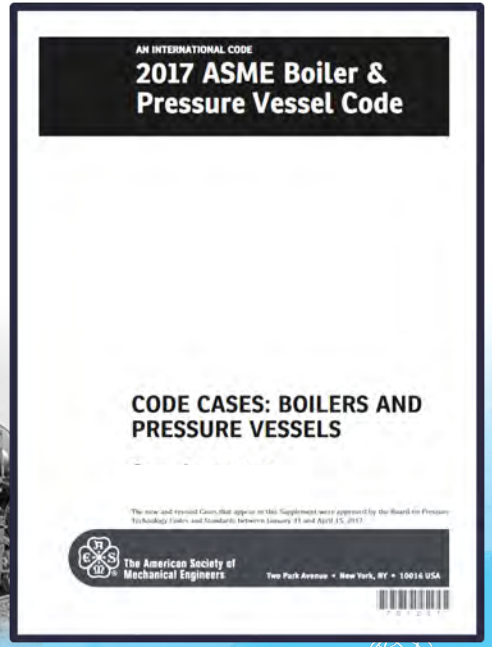
ASME
SETTING THE STANDARD

History of ASME

Setting the Standard since 1880







Inaugural Edition of the ASME Boiler Code

The Tradition Continues

ASME's Interest in AVs

- Autonomous Land, Aircraft and Ocean Vehicles
- Automation that Reshapes the Future of Cities
- Robotics to Provide Safety and Protection to Human Life
- Safety of Complex Systems that Engage Human Interaction
- Understand Both the Benefits and Risks of Autonomous Technologies

ASME
SETTING THE STANDARD

Related ASME Activities

- Journals/Books/Conferences
- Technical Divisions (Safety Engineering and Risk/Reliability Analysis Division, Design Engineering Division, ED, Computers & Information Systems, Micro/Nano Systems, and others)
- Standards Committee, Mobile Unmanned Systems (MUS)
- Unmanned Aerial Systems (UAS), crawlers/ground robotics, and submersibles

ASME
SETTING THE STANDARD

Thank you

SERAD, Ford Motor Co. & University of Maryland

SAID JAHANMIR, PH.D.

ASME PRESIDENT

JAHANMIRS@ASME.ORG

26 APRIL 2019

Reliability Aspects of Connected and Autonomous Vehicles

Vasiliy Krivtsov, PhD

Director of Reliability Analytics
The Ford Motor Company
vkrivtso@ford.com

Adjunct Professor of Reliability
The University of Maryland
krivtsov@umd.edu

University of Maryland
26 April 2019

FORD ANALYTICS
Global Data Insight & Analytics

Why Transportation Needs to Evolve

In this rapidly changing world, cities are growing fast. With urban centers dealing with record levels of traffic and pollution, the United Nations has identified increasing urbanization as one of the defining trends of the 21st century.

This growth is also causing a shift from individual vehicle ownership to the use of shared mobility options such as ride-hailing services. Most of our infrastructure was built to meet the needs of individually used vehicles. However, most of those vehicles sit idle about 95% of the time. As a result of this, as much as 30% of the real estate in city centers is devoted to parking.[1]

At Ford, we see this as an opportunity to design smart vehicles for a smart world. If applied correctly, new technologies can enable solutions to help city transportation systems improve the quality of life for everyone. That's why we're approaching these opportunities in a holistic way. We recognize that just injecting new mobility technologies and services into a city or neighborhood won't solve their existing challenges and may even make them worse.

Therefore, we created a City Solutions team dedicated to working closely with cities and communities to address these challenges. We're learning how each city works, what its needs are and how our technology can adapt and support each city's unique transportation system. We're developing a portfolio of solutions that can help a city improve its transportation system through better orchestration of traffic, transit and the ever-growing mobility options emerging every day.

Self-driving vehicles are one of the solutions to help enable this future. Ford is designing them to operate as a productive, safe and valuable part of a city transportation system to help make people's lives better.

[1] Keeping the Nation Moving: Facts on Parking, RAC Foundation, 2012, www.racfoundation.org/assets/rac_foundation/content/downloadables/keeping_the_nation_moving-parking_fact_sheet.pdf

Delivery Services of the Future

What do people think about getting their pizza delivered by a self-driving car? We partnered with Domino's Pizza to understand the role self-driving vehicles can play in food delivery.

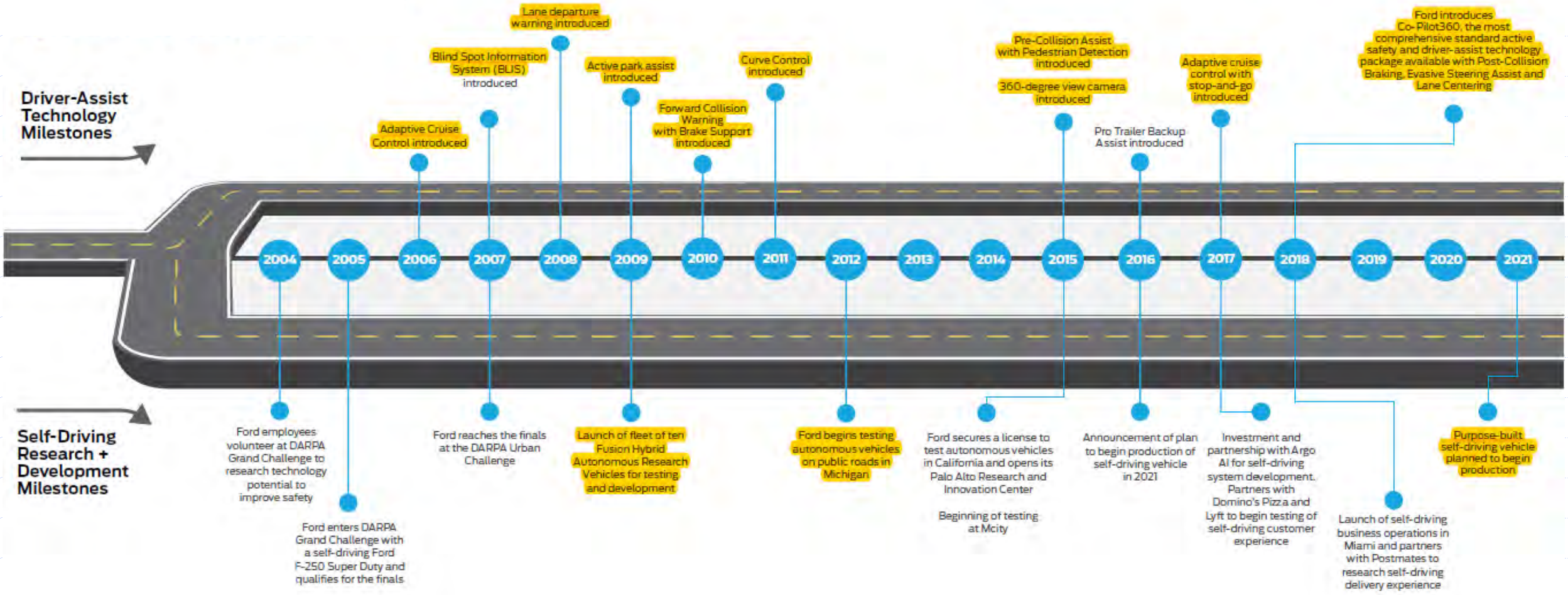
The focus of our research is what's sometimes referred to as "the last mile" or in this specific case "the last 50 feet," which is the transfer of the pizza to the customer. What that means is we will be looking at how customers respond to this new experience, which will require them to interact with the self-driving car instead of a delivery person — walking out to the vehicle instead of just walking to answer their front door.

We conducted an observational study, looking at how people respond to and interact with a self-driving vehicle when it arrives with their pizza. Will they be willing to walk out to the curb, or do we need to park in their driveway? Will people be able to determine on which side of the vehicle they should collect their pizza? How should they be notified upon arrival since there won't be a delivery person knocking on their door? What's the best way to guide people through the process of getting their pizza?

Some of the initial findings were promising. We found significant interest from customers as a vast majority opted-in for self-driving delivery when offered. Post-delivery interviews revealed that customers enjoyed the spoken instructions played from external speakers that explained how to get their pizza out of the vehicle. In fact, as the car "talked" to them, many people talked back and even said "Bye!" as the car drove away. We also identified opportunities to overcome such as the difficulty of finding curbside parking spots in dense urban areas as self-driving vehicles won't be programmed to double park.

We are developing solutions to these questions and concerns in ways that are customer-friendly and easy-to-use.

Ford's Autonomous Driving Systems Milestones



FORD ANALYTICS
Global Data Insight & Analytics

Connected Vehicles Technology

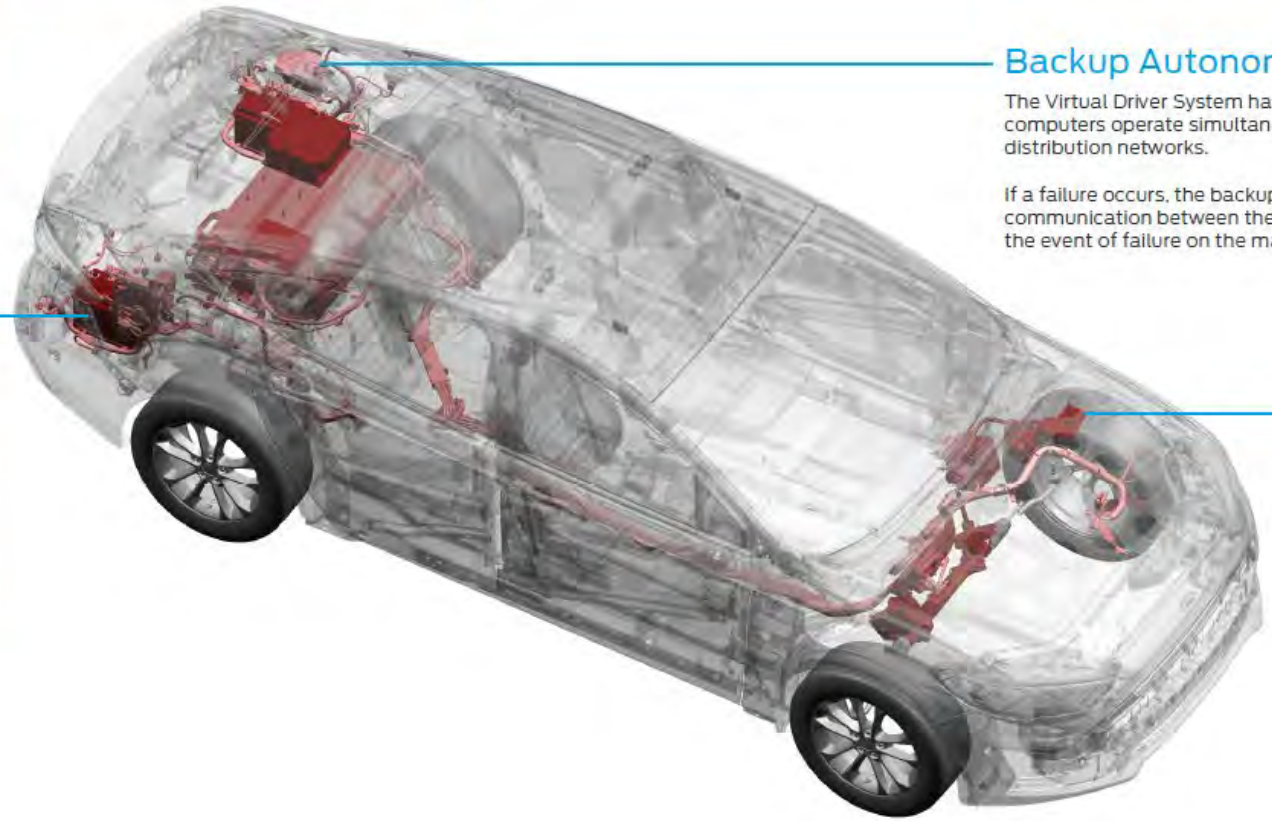
- **V2I "Vehicle to Infrastructure"** The technology captures data generated by the vehicle and provides information about the infrastructure to the driver. The V2I technology communicates information about safety, mobility or environment-related conditions.
- **V2V "Vehicle to Vehicle"** The technology communicates information about speed and position of surrounding vehicles through a wireless exchange of information. The goal is to avoid accidents, ease traffic congestions and have a positive impact on the environment.
- **V2C "Vehicle to Cloud"** The technology exchanges information about and for applications of the vehicle with a cloud system. This allows the vehicle to use information from other, though the cloud connected industries like energy, transportation and smart homes and make use of IoT.
- **V2P "Vehicle to Pedestrian"** The technology senses information about its environment and communicates it to other vehicles, infrastructure and personal mobile devices. This enables the vehicle to communicate with pedestrians and is intended to improve safety and mobility on the road.
- **V2X "Vehicle to Everything"** The technology interconnects all types of vehicles and infrastructure systems with another. This connectivity includes cars, highways, ships, trains and airplanes.

Ensuring Reliability through Redundancy

Diagnostics and Vehicle Health Monitoring

A sophisticated vehicle health monitoring strategy employs diagnostics integrated across multiple systems within the vehicle to determine vehicle health and perform fallback maneuvers when needed.

In addition to diagnostics, we also monitor the vehicle to determine its readiness, such as if all doors are closed.



Backup Autonomous Driving System

The Virtual Driver System has both main and backup computing systems. These two computers operate simultaneously while sharing information yet are on separate power distribution networks.

If a failure occurs, the backup system will bring the vehicle to a controlled stop. In addition, communication between the sensors, computers, and actuators have an alternate path in the event of failure on the main system.

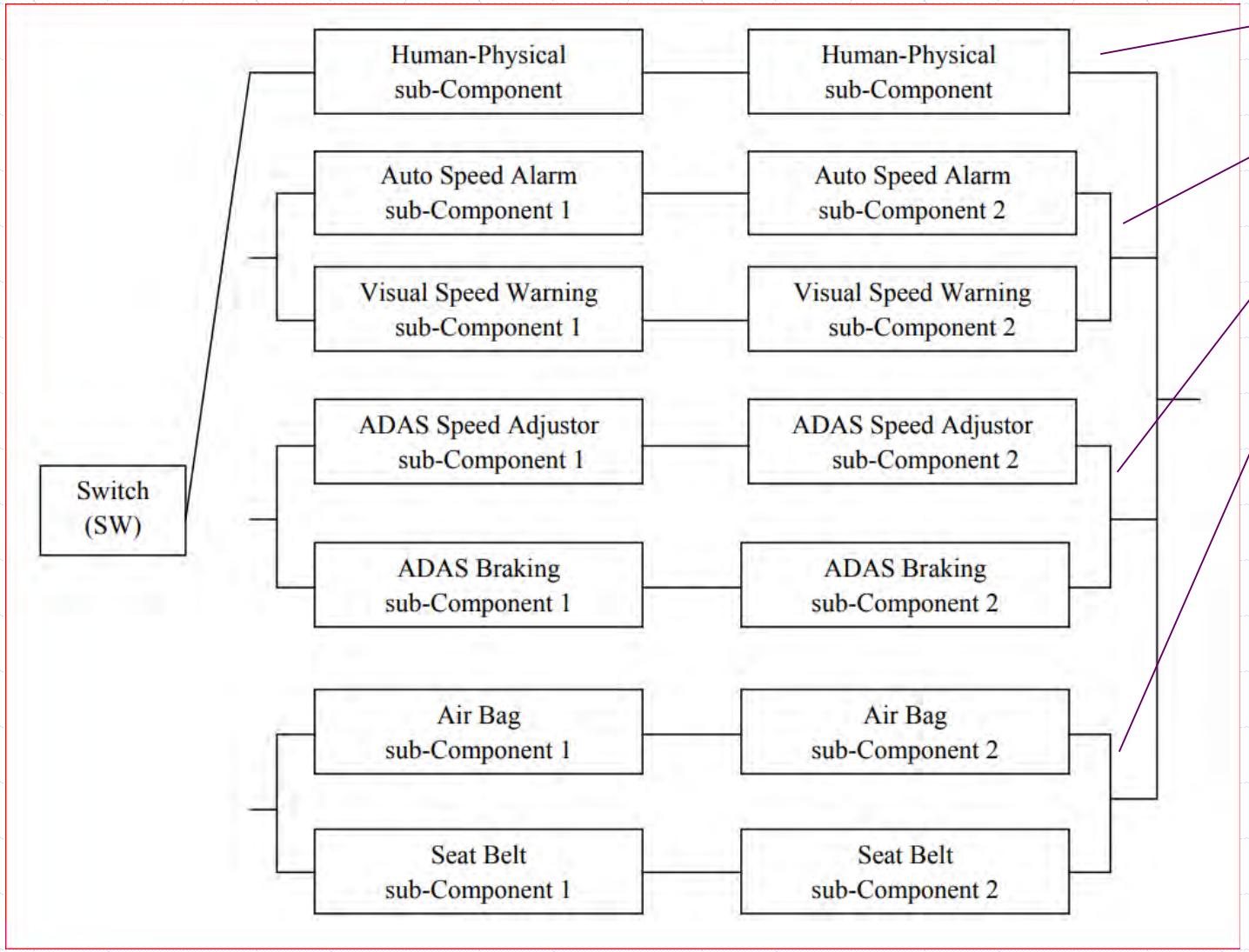
Electrical Power Systems

While main power to the vehicle is provided from the high voltage battery, there are backup electrical power sources and distribution to several critical components. In the case of a power failure, the backup powernets are able to provide low voltage power to the computers, sensors, braking and steering systems to bring the vehicle to a controlled stop.

Redundant Braking and Steering Systems

Backup braking and steering systems exist on separate power distribution networks. This redundancy allows the system to bring the vehicle to a controlled stop if a system fails.

ADAS Redundancy Modelling | Classical RBD Representation



Human Component (A)

ADAS Warning Systems (B)

ADAS Crash Avoidance (C)

Passive Safety Systems (D)

System Reliability Model:

$$R_S(t) = R_{SWA\to B} R_A(t)$$
$$+\int_0^t f_A(x_A) R_{SWA\to B} R_B(t-x_A)\,dx_A$$
$$+\int_0^t f_A(x_A) \int_{x_A}^t \begin{matrix} f_B(x_B) R_{SWB\to C} \\ R_B(t-x_A-x_B)\,dx_B \end{matrix} dx_A$$
$$+\int_0^t f_A(x_A) f_B(x_B) \int_{x_B}^t \begin{matrix} f_C(x_C) R_{SWC\to D} \\ R_D(t-x_A-x_B-x_B)\,dx_C dx_B \end{matrix} dx_A$$

Reference: K Hojjati-Emami, BS Dhillon , K Jenab (2012) “Reliability prediction for the vehicles equipped with advanced driver assistance systems and passive safety systems” Int. J of Industrial Eng Computations s 3 (2012) 731–742.

Design Life Implications

- Usage rate of average conventional passenger cars is 5%
- This translates into 72 mins in 24 hrs
- In a mixed, primarily urban duty cycle, with 30 MPH average speed, this further translates into ~13,140 miles/year
- Current design life target: 10YIS|150K (90th percentile)

- Usage rate of ride sharing and autonomous cars is expected to be (at least) 75%
- This translates into 1,080 mins in 24 hrs
- In a mixed, primarily urban duty cycle, with 30 MPH average speed, this further translates into 197,100 miles/year
- What should be design life target then?

Reference: JW Wasiloff (2018) “How Ride Sharing and Autonomous Vehicles impact Customer Usage and Reliability”, Automotive Excellence, No. 1-2018, 4-7.

Reliability Demonstration Implications

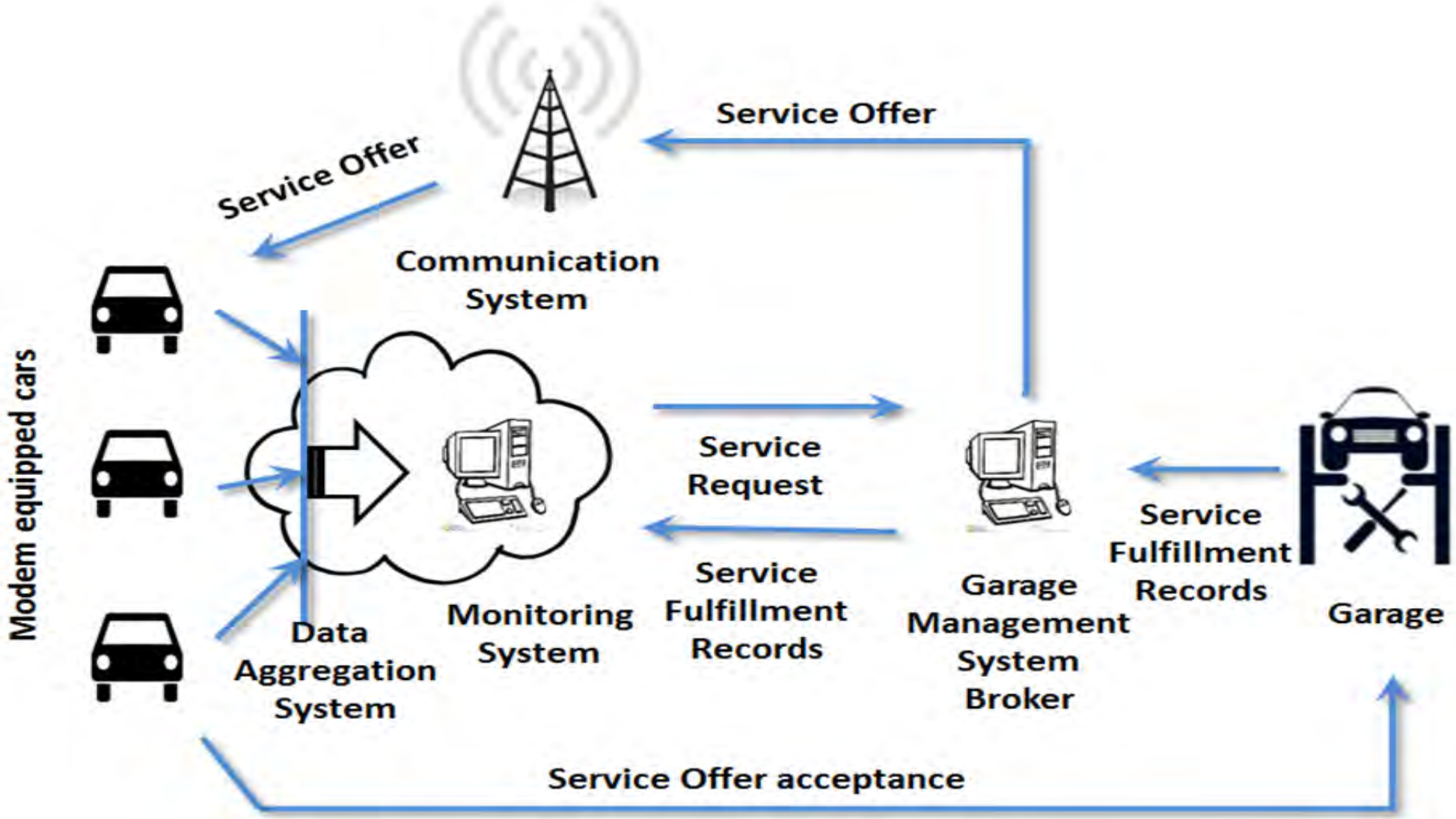
	How many miles (years[a]) would autonomous vehicles have to be driven...	Benchmark failure rate		
		(A) 1.09 fatalities per 100 million miles?	(B) 77 reported injuries per 100 million miles?	(C) 190 reported crashes per 100 million miles?
Statistical question	(1) without failure to demonstrate with 95% confidence that their failure rate is at most...	275 million miles (12.5 years)	3.9 million miles (2 months)	1.6 million (1 month)
	(2) to demonstrate with 95% confidence their failure rate to within 20% of the true rate of...	8.8 billion (400 years)	125 million (5.7 years)	51 million (2.3 years)
	(3) to demonstrate with 95% confidence and 80% power that their failure rate is 20% better than the human driver failure rate of...	11 billion (500 years)	161 million (7.3 years)	65 million (3 years)

[a] We assess the time it would take to complete the requisite miles with a fleet of 100 autonomous vehicles (larger than any known existing fleet) driving 24 h a day, 365 days a year, at an average speed of 25 miles per hour.

Reference: N Kalra & SM Paddock (2016) "Driving to safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?" — Transportation Research Part A: Policy and Practice, Elsevier.

These findings support the **need for alternative methods** to supplement real-world testing in order to assess autonomous vehicle safety. These methods may include but are not limited to **accelerated testing** (Nelson, 2009), **virtual testing & simulations** (Chen and Chen, 2010; Khastgir et al., 2015; Olivares et al., 2015); **maximal admissible safe interval simulations** (Kianfar et al., 2013); **scenario & behavior testing** (California Department of Motor Vehicles, 2015; Sivak and Schoettle, 2015); and **special pilot studies** (ANWB, 2015), as well as **extensive testing of hardware and software systems**."

Advanced Diagnostics & Vehicle Health Monitoring



Censoring Implications

Nonparametric Estimation of Marginal Failure Distributions from Dually Censored Automotive Data

Vasiliy Krivtsov; Ford Motor Company, Dearborn
Michael Frankstein; Ford Motor Company, Dearborn

Key Words: censoring, hazard function, warranty data, marginal estimates

SUMMARY & CONCLUSIONS

It is not uncommon that a component's reliability characteristics depend on two usage variables. As an example, for automotive components such variables are time in service and accumulated mileage. For certain airplane chassis components, these variables are accumulated flight hours and the number of landings. The problem of failure time distribution estimation from dually censored (at warranty limits) automotive data has been addressed by many authors. However, most of published work is focused on estimating *marginal in time* failure distributions or (less frequently) joint failure distributions. This paper focuses on nonparametric estimation of the *marginal in mileage* failure distributions, since for the majority of the automotive components mileage is considered a more relevant survival variable than time in service.

1. *INTRODUCTION*

Statistical analysis of automotive warranty data has been addressed by many authors. A general review of statistical methods for warranty data analysis can be found in Lawless and Kalbfleisch (Ref. 7), as well as in Blischke and Murthy (Ref. 1). The work of Suzuki (Ref. 10) followed by Lawless, Hu, and Cao (Ref. 6) and Hu, Lawless and Suzuki (Ref. 3) address the issues of incomplete records, bivariate censoring, and other complications related specifically to automotive warranty data. Wu and Meeker (Ref. 11) discuss some statistical procedures for early identification of reliability problems based on warranty data. In his recent paper, Majeske (Ref. 9) proposes a general mixture model framework for automobile warranty data that includes parameters for product field performance, the manufacturing and assembly process, and dealer preparation process.

Most of the above papers are focused on either parametric estimation of the joint failure distributions or nonparametric and parametric estimation of *marginal in time* failure distributions – see Figure 1. The latter is, often, due to: a) difficulties associated with mileage accumulation (Majeske, Ref. 9), and/or b) the necessity to report (project) warranty performance as a function of calendar time.

We would like to argue that for the majority of automotive components, mileage-to-failure (MTF) is often a more appropriate survival variable (i.e., the one "driving" failures), while time-to-failure (TTF) is a usage variable (i.e., just reflecting the time age of the component). When you buy a used car (say, 2-5 years in service), what is a more important consideration in your decision-making: the time age of the car or its mileage?

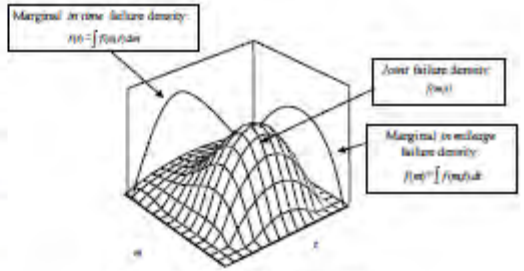


Figure 1. Graphical Interpretation of Joint and Marginal Probability Densities.

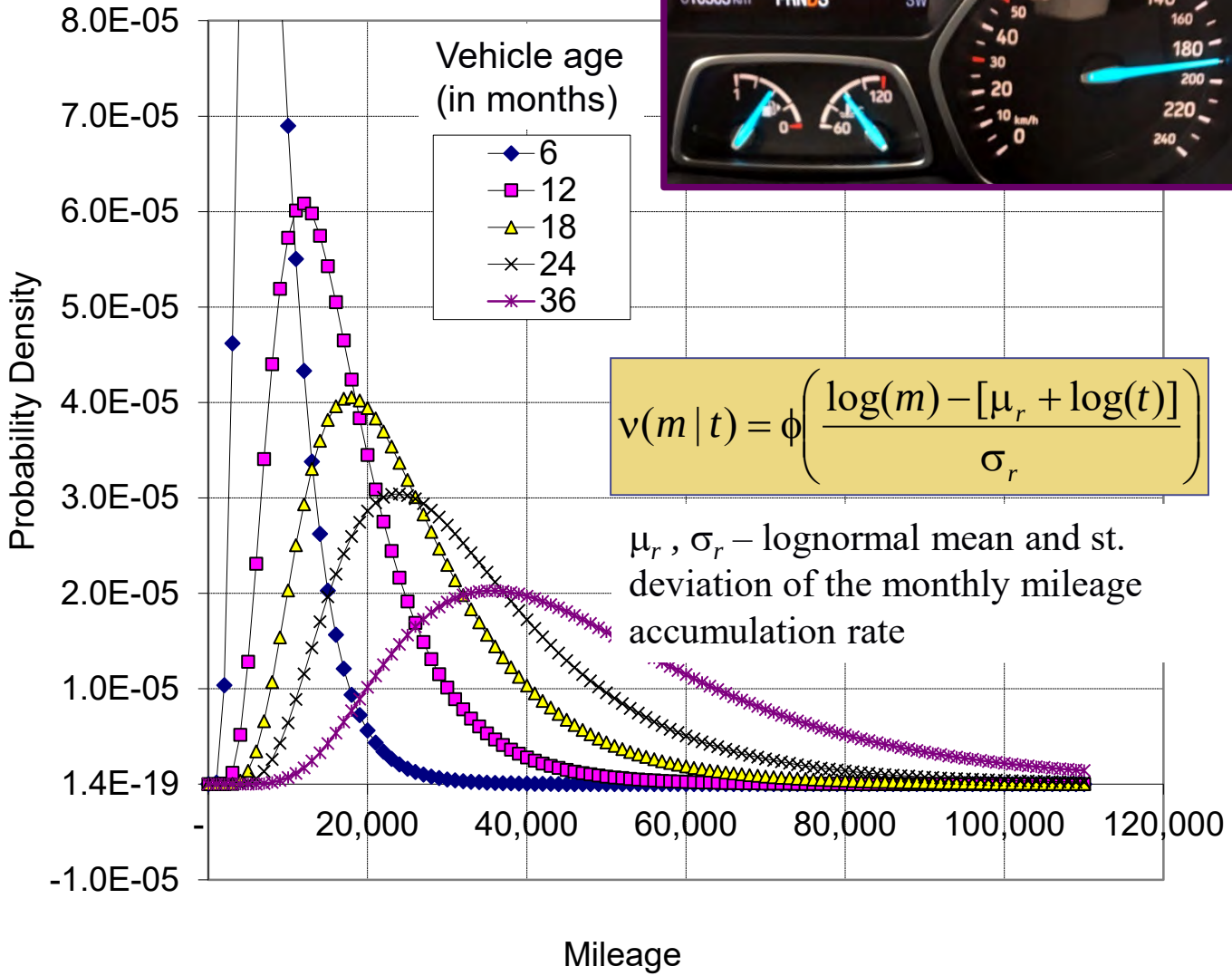
Consider brake pad wear as the failure mode in question. Obviously, mileage is a much more dominant stressor in this case than time in service. So, the reliability function estimated in mileage domain would better reflect the true failure distribution, while the time domain would represent the distribution of brake pad ages "accompanying" respective mileages.

Below, we first discuss a nonparametric procedure for estimating hazard and reliability functions in time domain and then follow with that in mileage domain.

2. *NONPARAMETRIC ESTIMATION OF MARGINAL HAZARD FUNCTIONS*

Reliability analysis of warranty data requires a few assumptions. First, every warranty repair corresponds to a respective failure, i.e., data collection errors due to misdiagnosis, "trouble not identified", mis-binning, etc. are neglected. Second, the time/mileage to repair is equated with the time/mileage to failure, which holds true for hard failures (component performance ceases) but may be false for soft ones (component performance degrades). Finally, time and mileage to failure are, strictly speaking, continuous variables.

Daily odometer readings completely resolve(!) the problem of censoring estimation

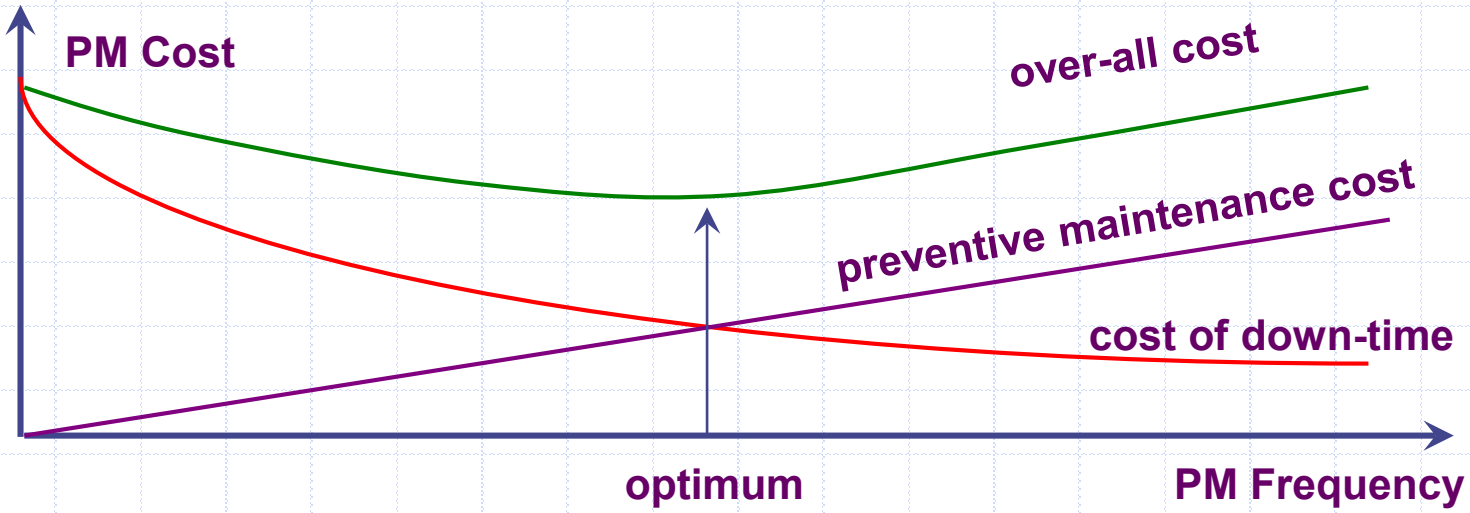


$$\nu(m \mid t) = \phi\left(\frac{\log(m) - [\mu_r + \log(t)]}{\sigma_r}\right)$$

μ_r , σ_r – lognormal mean and st. deviation of the monthly mileage accumulation rate

Reliability Based Maintenance Optimization

- Complex technical systems during their operational life, are subject to **preventive maintenance** (PM), which is necessary to meet these systems' reliability and availability (readiness) requirements.



- The question is what should be the **optimal schedule** of such actions? Optimal in the sense that high frequency of these actions increases the cost of maintaining system's operation but reduces the cost due to the system's downtime, while low frequency – decreases the cost of maintaining system's operation but increases the cost due to the system's downtime.

Optimal Replacement for Non-repairable Components

- Problem Statement
  - A component is replaced upon a failure or at a predetermined time, whichever occurs first.
  - What **is** that predetermined time, T, which minimizes the overall maintenance cost?
- Maintenance Cycle Length:

$$T_C = \int_0^T t \cdot f(t)\,dt + T \cdot R(T) = \int_0^T R(t)\,dt$$

replacements upon a failure

replacements at a predetermined time

- Maintenance Cost Model

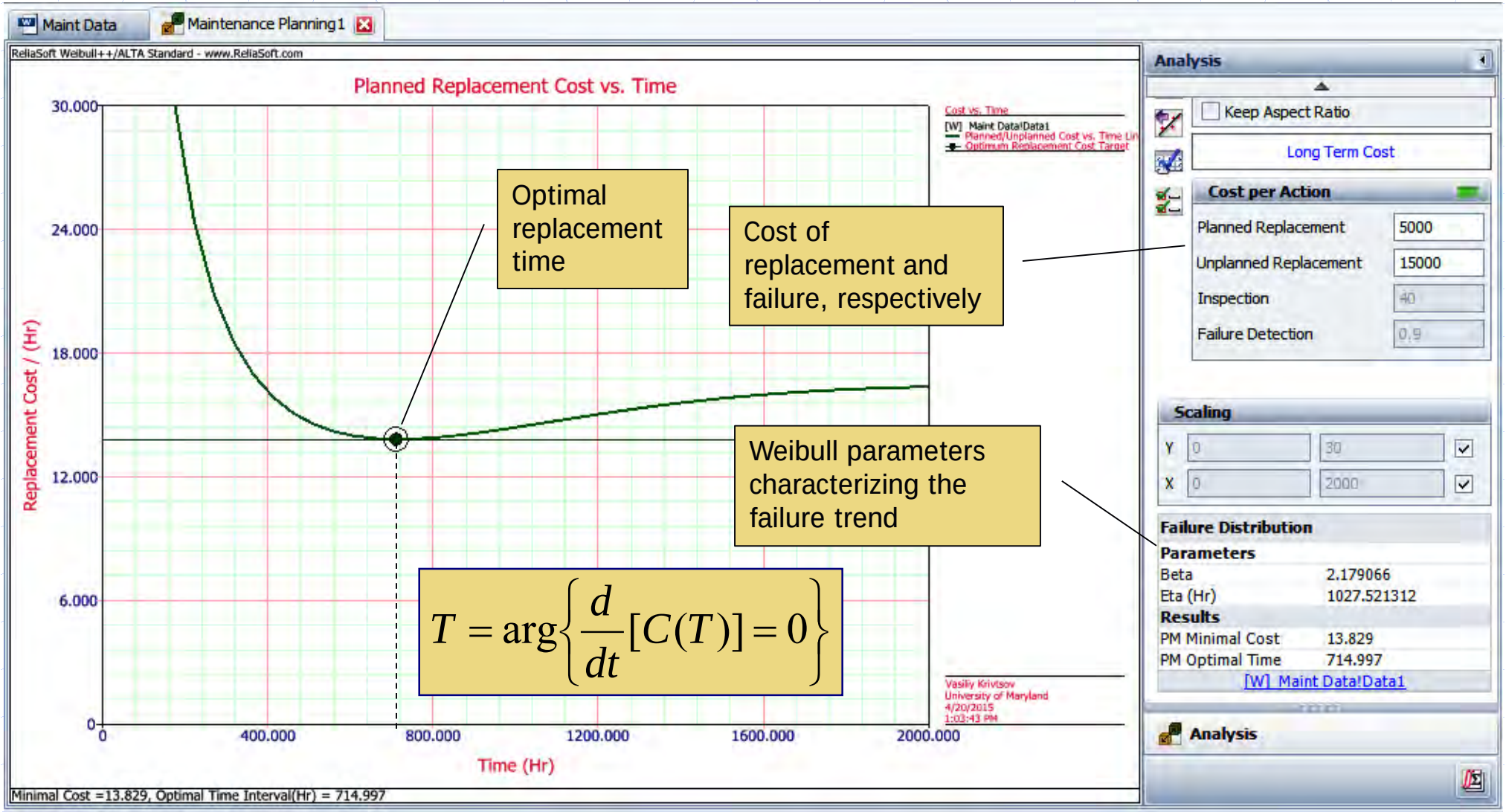
$$C(T) = \frac{C_f F(T) + C_r R(T)}{T_C} = \frac{C_f F(T) + C_r R(T)}{\int_0^T R(t)\,dt} \rightarrow \min$$

$C(T)$ = overall cost of maintenance per unit time | C_f = cost of failure | C_r = cost of replacement

$R(T)$ = reliability function of the underlying failure time distribution (e.g. Weibull)

$F(T)$ = unreliability function (CDF) of the underlying failure time distribution

Optimal Replacement Time for Non-repairable Components



Condition Based Maintenance | Brake Pads Example

techworld Trending: How to ... troubleshoot OSPF

Ford brakes the mould with car maintenance prediction algorithm

Ford has developed an algorithm using readily available car data to predict when its brakes need maintaining – and will send a text to the driver to let them know.

By Margi Murphy | Jun 22, 2015

Share

Ford has developed an algorithm using readily available car data to predict when its brakes need maintaining – and will send a text to the driver to let them know.

The manufacturer has begun trialling brake maintenance alerts as part of a wider 'conditioned based maintenance project' by closely monitoring 25 different vehicle signals in a prototype fleet of 25 Ford Transits. Using an algorithm developed internally it said it can send drivers more accurate notifications than current brake-replacement alerts based on mileage alone.

Ford has a range of new tech like car sharing, car apps and is working on its driverless tech. Image: Ford

techworld Trending: How to ... troubleshoot OSPF

Vasilly Krivtsov, technical specialist on the project told Techworld: "The idea is to now collect the data and analyse the data statistically in order to evaluate the needs for maintenance for every single vehicle. For example, depending on how you drive, we would recommend how soon you change your brake pads. If you imagine the difference between a taxi driver in contrast to a retired citizen driver - we can recommend personalised oil change notifications for two very different types of drivers."

It can crunch data relating to how heavy a driver pushes on the pedals and other traits specific to the driver, to predict car part wear and tear.

"This is more than just embedding specialised sensors that tell you if something has gone wrong. It's like the difference between a heart monitor that tells you that you are having a heart attack, and having a system in place that monitors how you are using your body so it can predict that heart attack", Arun Chopra, a technical specialist on the project told

U.S. patent application (Ford) No. 14/563101

Google

how soon should i replace my brake pads?

All Shopping News Videos Images More Settings Tools

About 6,600,000 results (1.28 seconds)

Generally, **brake pads** need to be **replaced** after about 50,000 miles. Some need to be **replaced** after 25,000, while others can last for 70,000 miles – **it** all depends on **the** factors listed above. To get a more accurate number for your car's specific needs, consult **the** owner's manual. Nov 30, 2015

How Often Should Brakes Be Replaced? | YourMechanic Advice
https://www.yourmechanic.com/article/how-often-should-brakes-be-replaced

About this result Feedback

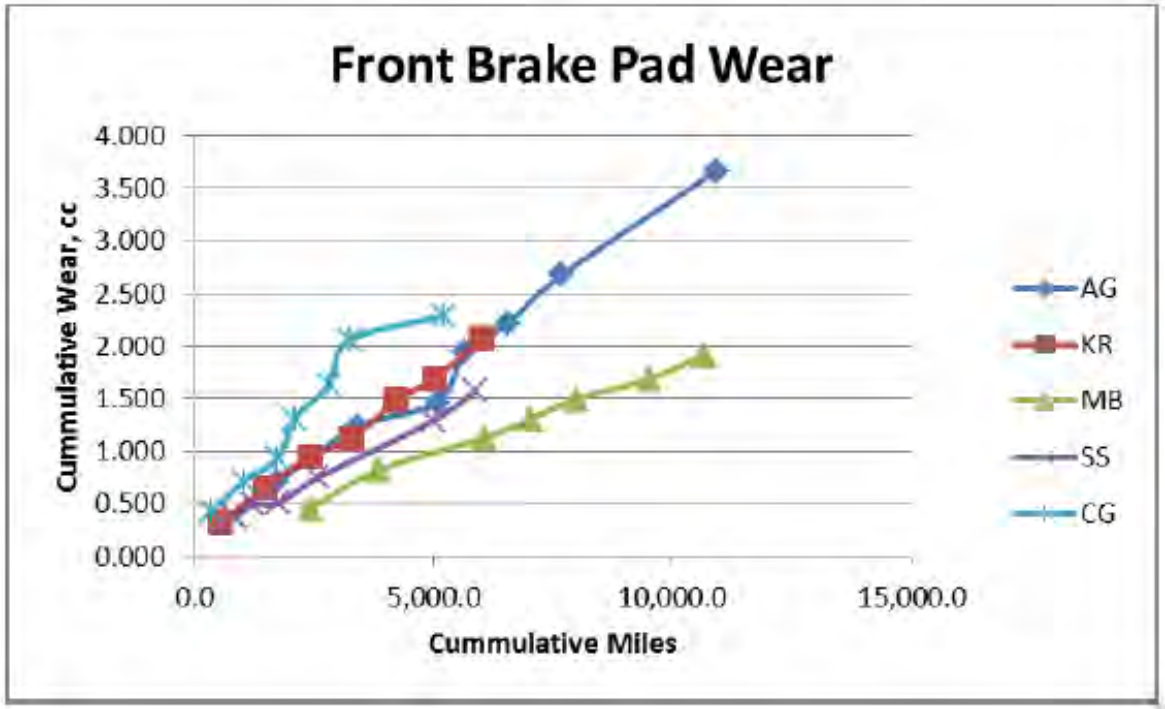
A Virtual Sensor for Brake Pad Thickness

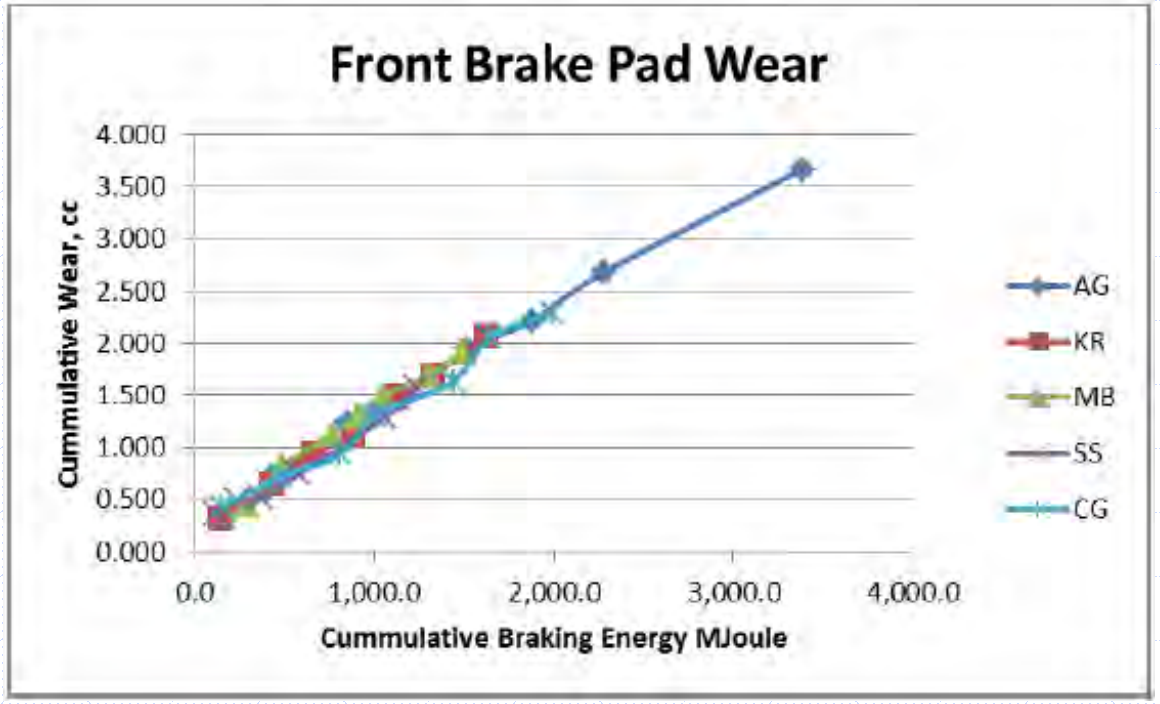
Brake pad wear is proportional to the consumed kinetic energy during a breaking event

$$\Delta W \propto \frac{m\left(V_1^2 - V_2^2\right)}{2}$$

m = vehicle mass

V_1, V_2 = vehicle speed before and after breaking, respectively





Survival Regression with Kinetic Energy as a Covariate

$$R(w,x) = 1 - \Phi\left(\frac{[\log]w - \mu_w(x)}{\sigma_w}\right)$$

$$\mu_t(x) = \gamma_0 + \sum_i \gamma_i x_i$$

where:

w is **brake pad wear**; $\Phi()$ the standard normal CDF for normal and lognormal distributions and the smallest extreme value CDF for the Weibull distribution; μ, σ are the location and scale parameters of the wear distribution, respectively.

x is the **vector of explanatory variables** such as **consumed energy** (kinetic + potential), **temperature**, **humidity**, etc.

Regression with Life Data: Wear versus Energy
Response Variable: Wear

Censoring Information	Count
Uncensored value	24
Right censored value	76

Estimation Method: Maximum Likelihood
Distribution: Normal
Relationship with accelerating variable(s): Linear

Regression Table

Predictor	Coef	Standard Error	Z	P
Intercept	0.558543	0.0970237	5.76	0.000
Energy	0.0000494	0.0000009	52.68	0.000
Scale	0.0689371	0.0109218		

Log-Likelihood = 17.528

Anderson-Darling (adjusted) Goodness-of-Fit

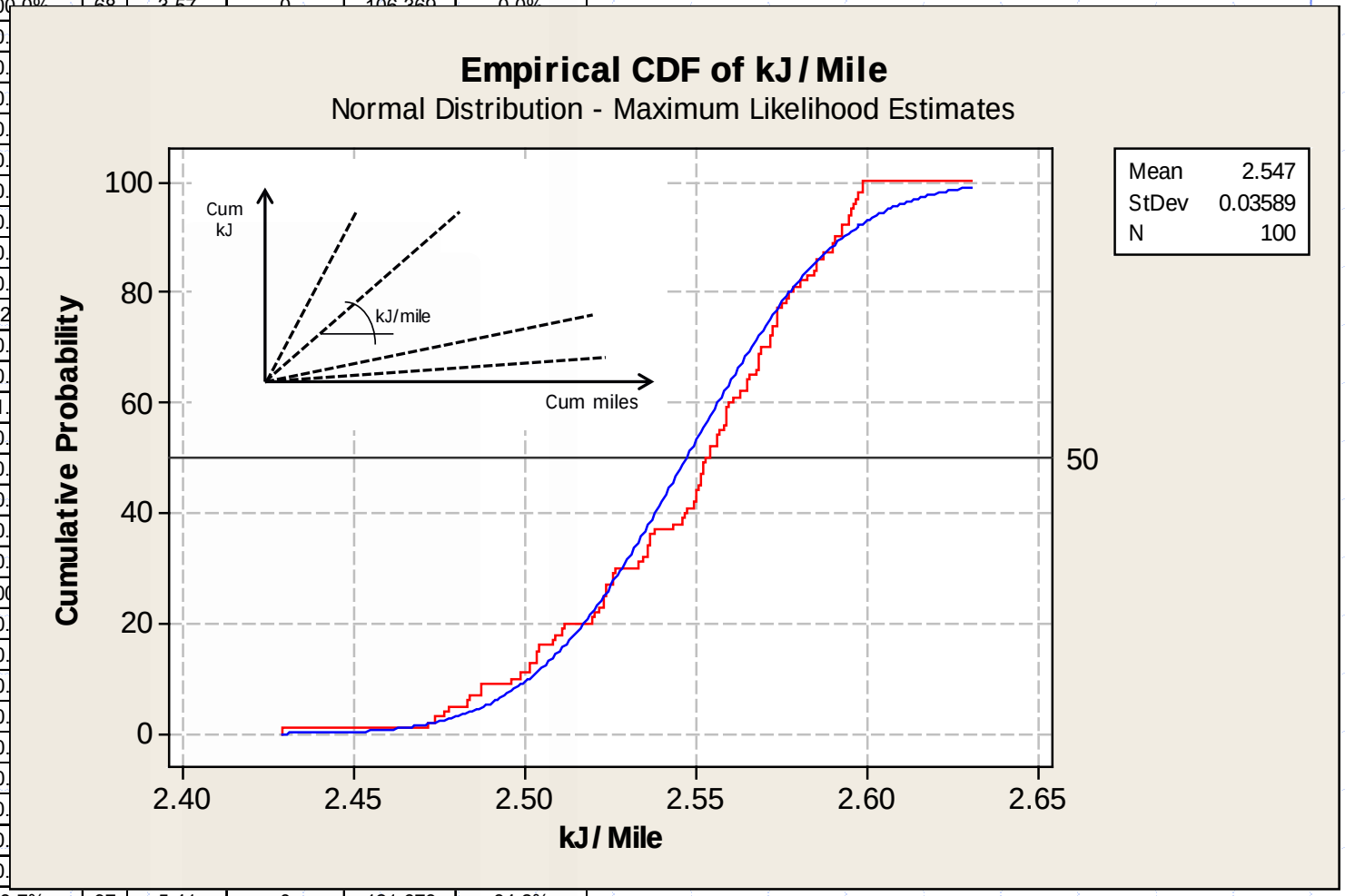
Standardized Residuals = 3.368
Cox-Snell Residuals = 3.357

FORD ANALYTICS
Global Data Insight & Analytics

Probability of Wear Exceeding 6.5mm by VIN

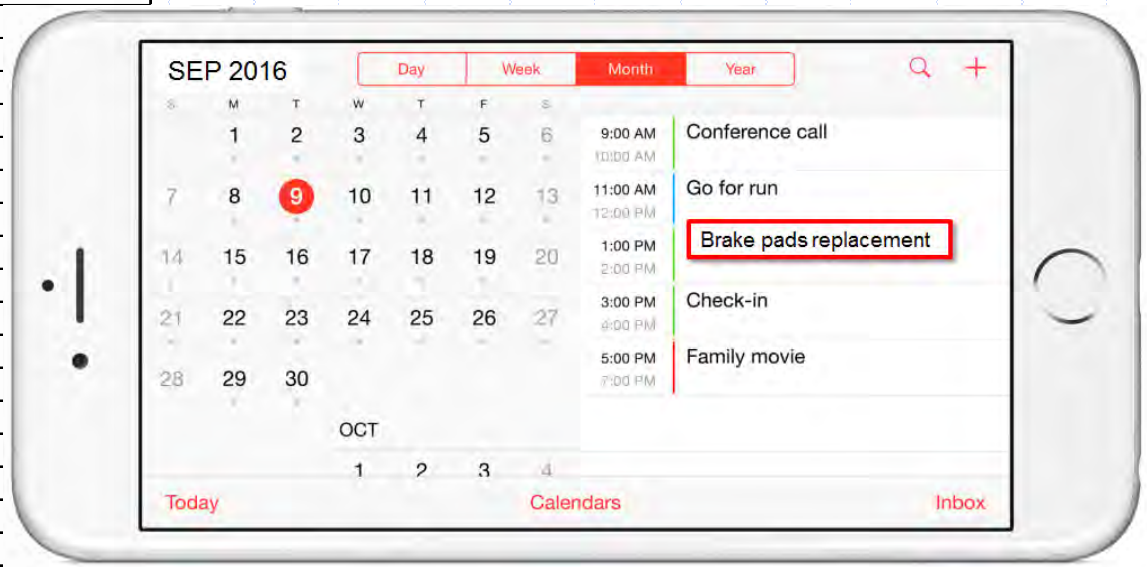
	Censored Sample		Prediction			Censored Sample		Prediction			Censored Sample		Prediction	
VIN	Wear (mm)	1=Comp 0=Cens	Energy, kJ	Prob (w>6.5mm)	VIN	Wear (mm)	1=Comp 0=Cens	Energy, kJ	Prob (w>6.5mm)	VIN	Wear (mm)	1=Comp 0=Cens	Energy, kJ	Prob (w>6.5mm)
1	4.33	1	85,174	0.0%	34	2.98	0	101,005	0.0%	67	4.52	0	107,086	0.0%
2	4.94	1	93,523	0.0%	35	1.44	0	149,004	100.0%	68	3.57	0	106,369	0.0%
3	4.97	1	96,627	0.0%	36	3.04	0	101,604	0.					
4	5.03	1	97,509	0.0%	37	4.67	0	102,978	0.					
5	0.38	0	98,826	0.0%	38	3.53	0	102,140	0.					
6	4.64	0	96,917	0.0%	39	5.68	1	104,759	0.					
7	5.23	1	98,816	0.0%	40	1.79	0	101,328	0.					
8	0.64	0	93,715	0.0%	41	5.68	1	106,389	0.					
9	0.15	0	97,493	0.0%	42	1.77	0	116,492	0.					
10	2.77	0	96,873	0.0%	43	1.78	0	108,667	0.					
11	3.74	0	97,752	0.0%	44	2.45	0	102,123	0.					
12	4.20	0	98,156	0.0%	45	1.83	0	119,629	32					
13	0.33	0	96,802	0.0%	46	2.57	0	102,464	0.					
14	3.40	0	97,841	0.0%	47	5.73	1	106,181	0.					
15	3.29	0	97,841	0.0%	48	1.97	0	117,006	1.					
16	0.45	0	110,082	0.0%	49	4.80	0	104,887	0.					
17	1.86	0	97,309	0.0%	50	5.76	1	106,952	0.					
18	5.41	1	100,972	0.0%	51	5.77	1	106,018	0.					
19	5.42	1	100,681	0.0%	52	2.09	0	103,950	0.					
20	3.05	0	98,497	0.0%	53	2.85	0	103,724	0.					
21	4.51	0	99,796	0.0%	54	2.18	0	128,458	100					
22	0.75	0	115,142	0.0%	55	4.30	0	105,463	0.					
23	0.78	0	103,395	0.0%	56	4.92	0	106,118	0.					
24	2.83	0	98,935	0.0%	57	4.55	0	105,911	0.					
25	0.86	0	97,952	0.0%	58	2.38	0	111,092	0.					
26	0.94	0	97,664	0.0%	59	2.43	0	110,512	0.					
27	5.49	1	101,899	0.0%	60	3.25	0	105,160	0.					
28	1.00	0	114,682	0.0%	61	2.46	0	114,311	0.					
29	5.52	1	102,820	0.0%	62	5.88	1	108,987	0.					
30	1.17	0	118,054	5.6%	63	2.58	0	108,928	0.					
31	2.38	0	100,019	0.0%	64	2.66	0	123,365	98.7%	97	5.41	0	121,673	84.2%
32	1.27	0	103,405	0.0%	65	2.66	0	116,424	0.3%	98	5.73	0	130,634	100.0%
33	4.27	0	101,783	0.0%	66	2.67	0	112,773	0.0%	99	6.71	1	126,404	100.0%
										100	6.11	0	143,458	100.0%

Brake energy per mile by VIN



Incremental Mileage to Critical Wear (6.5mm) by VIN @ 95% Confidence Probability: $Pr(w \geq 6.5 | \Delta m \leq m_0) = 0.95$

VIN	Current Energy, kJ	Current Mileage	Increm. Mileage to Critcal Wear (6.5 mm)	VIN	Energy, kJ	Current Mileage	Increm. Mileage to Critcal Wear (6.5 mm)	VIN	Energy, kJ	Current Mileage	Increm. Mileage to Critcal Wear (6.5 mm)
1	85,174	33,162	12,214	34	101,005	40,669	4,707	67	107,086	42,005	3,371
2	93,523	36,649	8,726	35	149,004	57,592	0	68	106,369	41,474	3,901
3	96,627	38,286	7,090	36	101,604	39,803	5,573	69	107,696	41,806	3,570
4	97,509	39,065	6,310	37	102,978	40,608	4,768	70	108,764	42,294	3,082
5	98,826	39,213	6,163	38	102,140	40,439	4,937	71	115,706	44,957	419
6	96,917	37,642	7,734	39	104,759	41,305	4,071	72	111,724	44,018	1,358
7	98,816	39,946	5,430	40	101,328	39,452	5,924	73	108,249	42,858	2,517
8	93,715	36,288	9,088	41	106,389	42,408	2,968	74	120,261	47,015	0
9	97,493	37,879	7,496	42	116,492	45,363	13	75	128,423	49,802	0
10	96,873	37,304	8,072	43	108,667	42,544	2,832	76	112,112	43,779	1,597
11	97,752	38,765	6,611	44	102,123	41,323	4,053	77	114,569	44,233	1,142
12	98,156	39,531	5,844	45	119,629	47,037	0	78	114,942	44,742	634
13	96,802	37,958	7,418	46	102,464	40,039	5,337	79	110,311	44,059	1,317
14	97,841	38,346	7,030	47	106,181	41,198	4,177	80	111,238	44,925	451
15	97,841	39,110	6,265	48	117,006	45,465	0	81	111,895	43,735	
16	110,082	43,630	1,746	49	104,887	41,384	3,992	82	111,732	44,485	
17	97,309	37,509	7,867	50	106,952	43,003	2,373	83	111,799	43,081	
18	100,972	39,358	6,018	51	106,018	41,339	4,037	84	119,269	46,853	
19	100,681	41,443	3,933	52	103,950	41,523	3,853	85	114,238	45,269	
20	98,497	38,833	6,542	53	103,724	40,733	4,643	86	113,638	43,731	
21	99,796	39,355	6,021	54	128,458	49,944	0	87	115,484	46,213	
22	115,142	45,044	332	55	105,463	41,404	3,972	88	116,146	44,769	
23	103,395	39,811	5,565	56	106,118	41,408	3,968	89	116,649	45,354	
24	98,935	39,165	6,211	57	105,911	40,853	4,522	90	118,022	45,573	
25	97,952	39,052	6,324	58	111,092	43,458	1,917	91	118,839	46,533	
26	97,664	38,710	6,665	59	110,512	42,765	2,611	92	124,132	48,493	
27	101,899	39,926	5,449	60	105,160	41,735	3,641	93	119,340	46,787	
28	114,682	46,115	0	61	114,311	44,674	702	94	121,323	48,970	
29	102,820	40,045	5,331	62	108,987	42,629	2,747	95	125,575	48,371	
30	118,054	47,012	0	63	108,928	42,140	3,235	96	123,799	47,641	
31	100,019	39,489	5,887	64	123,365	47,805	0	97	121,673	47,319	
32	103,405	39,998	5,378	65	116,424	44,903	473	98	130,634	52,227	0
33	101,783	39,914	5,462	66	112,773	45,043	333	99	126,404	49,546	0
								100	143,458	55,378	0



Prof. Philip Koopman

Carnegie Mellon University

The Big Picture for Self-Driving Car Safety

Workshop on Risk Analysis for Autonomous Vehicles, April 26 2019

@PhilKoopman

EDGE CASE RESEARCH

© 2019 Philip Koopman

Overview

EDGE CASE RESEARCH

- Conventional vehicle software safety
- Driver assistance safety
  - "ADAS"/"SOTIF"
- Fully autonomous safety
  - Perception
  - Operations
  - System life cycle
  - Societal & ethical issues

[General Motors]

© 2019 Philip Koopman

Brute Force Road Testing

EDGE CASE RESEARCH

- **Good for identifying "easy" cases**
  - Expensive and potentially ***dangerous***

Unrealistic to Brute Force Safety

EDGE CASE RESEARCH

- **If 100M miles/critical mishap…**
  - Test 3x–10x longer than mishap rate
    ➔ Need 1 Billion miles of testing
- **That's ~25 round trips on every road in the world**
  - With fewer than 10 critical mishaps

…

- **Instead, use standards-based safety engineering**

WolframAlpha computational knowledge engine

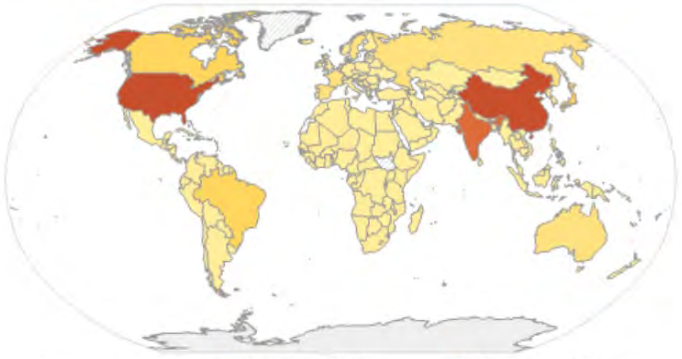
miles of roads

Summary:

total	20.46 million mi
median	11630 mi
highest	4.03 million mi (United States)
lowest	4.97 mi (Tuvalu)

(1994 to 2008)
(based on 225 values; 24 unavailable)

Total road length map:



(in miles)

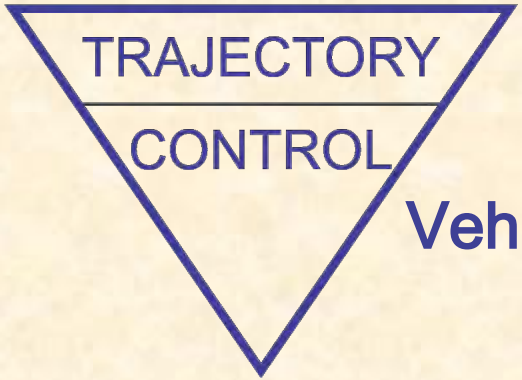
© 2019 Philip Koopman

Conventional Vehicle Safety

EDGE CASE RESEARCH

- **Human driver ultimately responsible for safety**
  - "Functional Safety" – respond to equipment; avoid design faults
  - Human does the right thing for malfunctions ("Controllability")

ISO 26262:
- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*



Perform turns, etc.

Vehicle motion

© 2019 Philip Koopman

Example Automotive Software Defects

EDGE CASE RESEARCH

- ***Small*** **sampling of NHTSA recalls (i.e., confirmed bugs)**
  - 17V-713: Engine does not reduce power due to ESP software defect
  - 17V-686 *and MANY others*: Airbags disabled
  - 15V-569: Unexpected steering motion causes loss of control
  - 15V-460 *and others*: Airbags deploy when they should not
  - 15V-145: Unattended vehicle starts engine → carbon monoxide poisoning
  - 14V-370: Turns off headlights when driving
  - 14V-204: 1.5 seconds reverse while displaying Drive

  Voluntary Recalls:
  - 2018 hybrid engine stall at high speeds (https://bloom.bg/2y21T71)
  - 2014 sudden unintended acceleration (https://goo.gl/R9zgL1)

© 2019 Philip Koopman

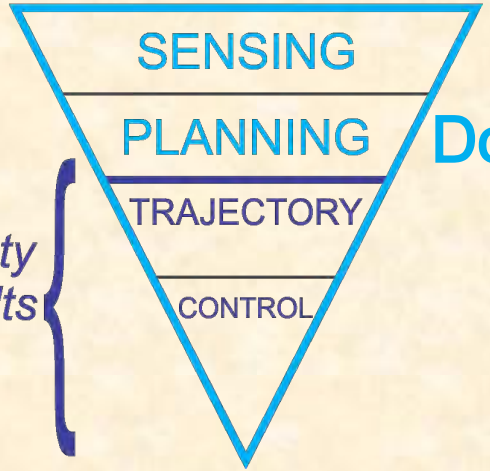
Advanced Driver Assistance Systems (ADAS)

EDGE CASE RESEARCH

- **Lane keeping, forward collision avoidance**
  - Driver still responsible for safety, but these help out
- **Safety Of Intended Function (SOTIF)**
  - Malfunctions can occur even with defect-free equipment
    - Example: camera does not detect white vehicle on white background

ISO 21448 (SOTIF):
- *Enumerate Scenarios*
- *Triggering Events*
- *Historically for ADAS*

ISO 26262:
- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*



Radar, Lidar, etc.

Don't hit things

© 2019 Philip Koopman

SOTIF Is All About the Scenarios

EDGE CASE RESEARCH

- **Will the sensors detect objects?**
  - Impaired by rain, snow, glare
- **Is this something the car knows how to do?**
  - Road geometries
  - Other vehicles & pedestrians
  - Traffic lights & road signs
  - Road surface conditions
  - Weather
- **ISO 21448 SOTIF Strategy:**
  - Giant scenario database
  - Push everything into "SAFE" bin

© 2019 Philip Koopman

Closed Course Testing

EDGE CASE RESEARCH

- **Safer than road testing, but expensive**
  - Not scalable
  - Only tests things you have thought of!

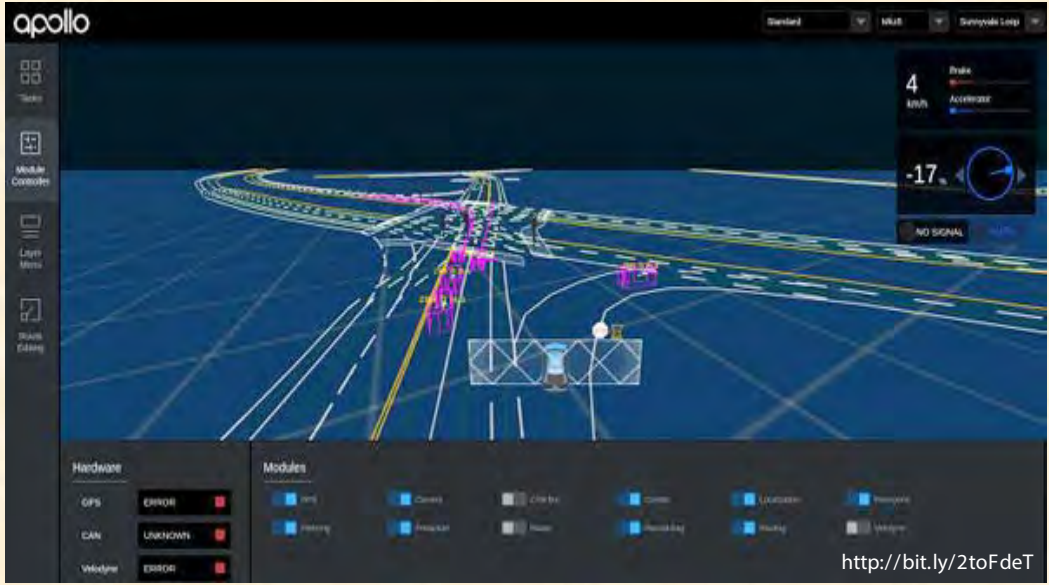
Volvo / Motor Trend

Simulation

EDGE CASE RESEARCH

- **Highly scalable; less expensive**
  - Only tests things you have thought of!
  - Need higher coverage for full autonomy compared to ADAS

Udacity

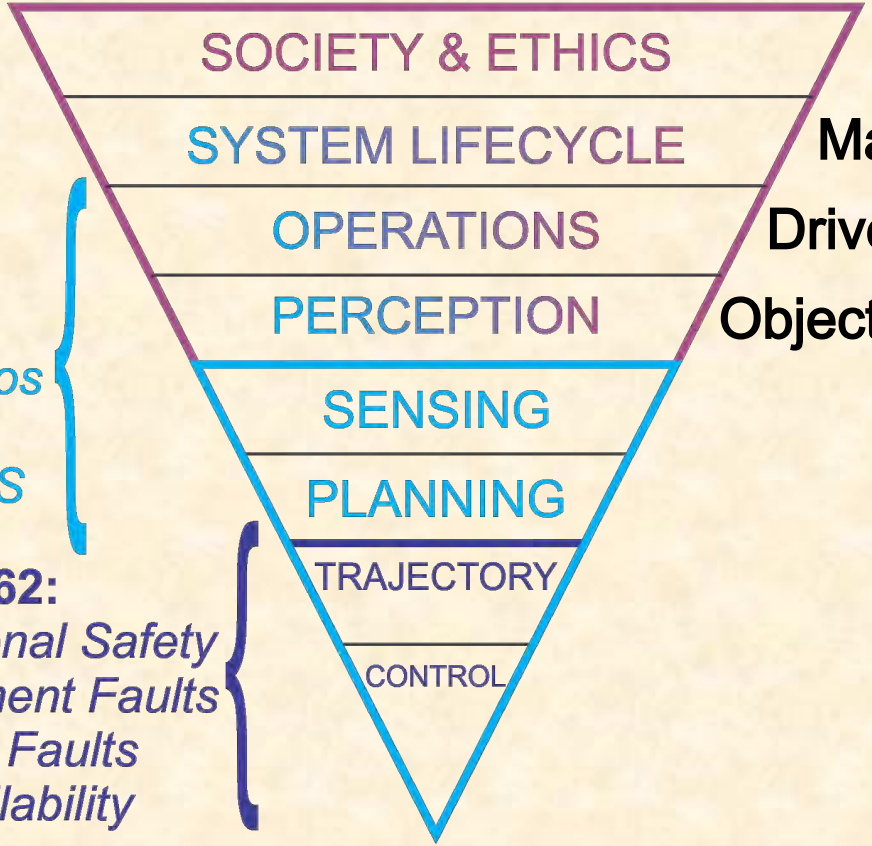


Apollo

© 2019 Philip Koopman

But Wait – There's More!

EDGE CASE RESEARCH



How safe is enough?

Maintenance, Updates

Drivers do more than drive

Object Classification

ISO 21448 (SOTIF):
- *Enumerate Scenarios*
- *Triggering Events*
- *Historically for ADAS*

ISO 26262:
- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*

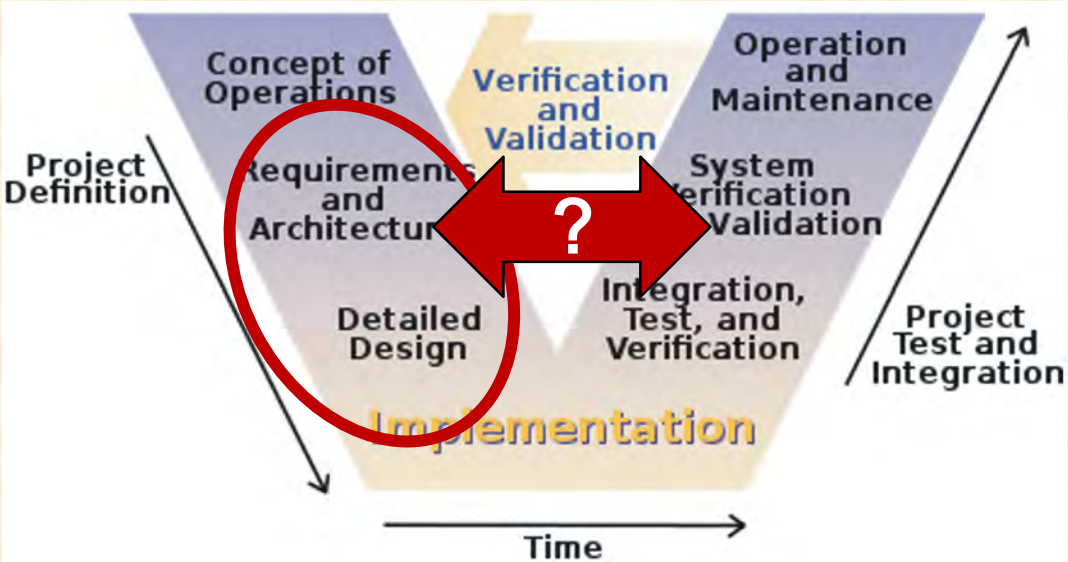
© 2019 Philip Koopman

Perception Use of Machine Learning

EDGE CASE RESEARCH

- **Learn by example**
  - Training data instead of design
  - E.g., 1 million pictures of people
- **Inductive training**
  - No requirements
  - No design insight

Traditional safety includes validation against requirement



What About Edge Cases?

EDGE CASE RESEARCH

- **Gaps in training data can lead to perception failure**
  - Safety needs to know: "Is that a person?"
  - Machine learning provides: "Is that thing like the people in my training data?"

PREDICTED CONCEPT	PROBABILITY
bird	0.997
no person	0.990
one	0.975
feather	0.970
nature	0.963
poultry	0.954
outdoors	0.936
color	0.910
animal	0.908

https://www.clarifai.com/demo

- **Edge Case are surprises**
  - You won't see these in training or testing

    ➔ Edge cases are the stuff you didn't think of!

© 2019 Philip Koopman

Need An Edge Case "Zoo"

EDGE CASE RESEARCH

- Novel objects (missing from zoo) are triggering events

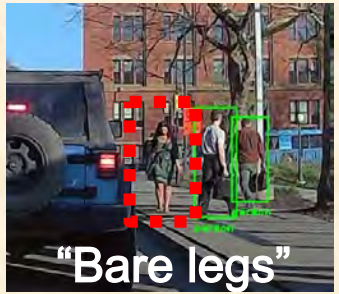
Example Triggering Events via Hologram

EDGE CASE RESEARCH

- Mask-R CNN: examples of systemic problems

"Camouflage"

"Children"


"Bare legs"

"Sun glare"

"Red objects"

"Columns"

"Single Lane Control"

Baseline, un-augmented images. (Your mileage will vary.)

HOLOGRAM

© 2019 Philip Koopman

Operations & Human Interactions

EDGE CASE RESEARCH

- **Drivers do more than just drive**
  - Occupant behavior, passenger safety
  - Detecting and managing equipment faults
- **Operational limitations & situations**
  - System exits Operational Design Domain
  - Vehicle fire or catastrophic failure
  - Post-crash response
- **Interacting with non -drivers**
  - Pedestrians, passengers
  - Police, emergency responders

https://bit.ly/2GvDkUN

https://bit.ly/2PhzilT

© 2019 Philip Koopman

Lifecycle Issues

EDGE CASE RESEARCH

- **Handling updates**
  - Fully recertify after every weekly update?
  - Security in general
- **Vehicle maintenance**
  - Pre-flight checks, cleaning
  - Corrective maintenance
- **Supply chain issues**
  - Quality fade
  - Supply chain faults

Is windshield cleaning fluid life critical?

© 2019 Philip Koopman

Safety Standard Landscape

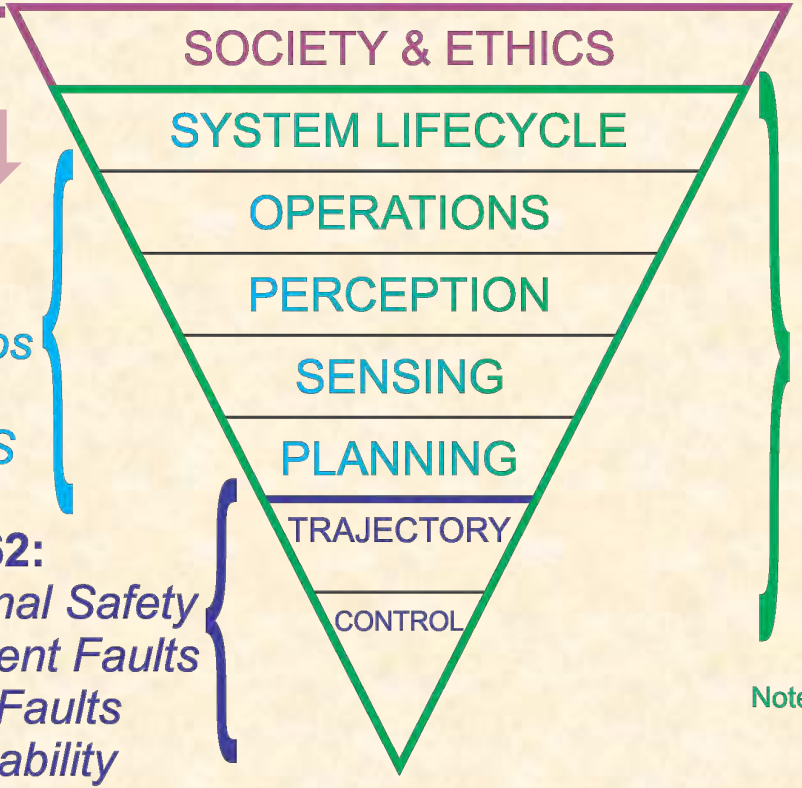
EDGE CASE RESEARCH

IEEE P700x
- *Ethical Life-Cycle*

ISO 21448 (SOTIF):
- *Enumerate Scenarios*
- *Triggering Events*
- *Historically for ADAS*

ISO 26262:
- *Functional Safety*
- *Equipment Faults*
- *Design Faults*
- *Controllability*

Note: ISO 26262 covers functional safety lifecycle activities.



UL 4600: (Draft Scope)
- *Machine Learning Faults*
- *External Operational Faults*
- *Non-Driver Human Faults*
- *Nondeterminism*
- *High Residual Unknowns*
- *Field Feedback and Updates*
- *Lack of Human Oversight*
- *System-Level Safety Metrics*
- *Full Autonomous Driving: Excludes Human Supervision*

Note: Provides significantly more detailed treatment regarding autonomous systems for those topics also mentioned in ISO 21448, ISO 26262. Intended to supplement, not replace these.

© 2019 Philip Koopman

Why Does Society Want This Technology?

EDGE CASE RESEARCH

- **Where did "94%" come from?**
  - "The critical reason was assigned to drivers in an estimated 2,046,000 crashes that comprise 94 percent of the NMVCCS crashes at the national level.

    However, in none of these cases was the assignment intended to blame the driver for causing the crash."

    [DOT HS 812 115]

"94%"

NHTSA

Benefits of Automation

SAFETY

The safety benefits of automated vehicles are paramount. Automated vehicles' potential to save lives and reduce injuries is rooted in one critical and tragic fact: 94 percent of serious crashes are due to human error. Automated vehicles have the potential to remove human error from the crash equation, which will help protect drivers and passengers, as well as bicyclists and pedestrians. When you consider more than 35,092 people died in motor vehicle-related crashes in the U.S. in 2015, you begin to grasp the lifesaving benefits of driver assistance technologies.

https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

- **Practical improvement perhaps only 50%**
  - Casualty Actuarial Society, 2014 https://bit.ly/2IIXj3L

© 2019 Philip Koopman

It's Not All Cell Phone Distraction

EDGE CASE RESEARCH

- **37,133 Fatalities**
  - 63% Passenger vehicles
  - 14% Motorcycles
  - 19% Pedestrians, bikes, etc.
  - 2% Large trucks (+ 2% other = 100%)

U.S. Department of Transportation
National Highway Traffic Safety Administration
TRAFFIC SAFETY FACTS
Research Note
NHTSA

(2017 data DOT HS-812-603)

- **One fatality per 86 million miles, including impaired drivers**
  - 29% Alcohol Impairment
  - 27% Seat belt not used in passenger vehicle
  - 26% Speed (can be too fast for conditions)
  - 9% Distracted driving (total of all sources was more than 100% due to overlap)
- **The bar is set high for unimpaired humans**
  - 99.999999%+ fatality-free miles

© 2019 Philip Koopman

Points to Ponder

EDGE CASE RESEARCH

- **True self-driving cars will take a long time**
  - "Disengagement" is the wrong metric to use for road testing
  - Start with very limited operational design domains (ODDs)
  - "Self driving cars will be safer" is aspirational
- **Driver assistance (ADAS) offer low hanging fruit**
  - Safety-net functions such as AEB can help, even if imperfect
  - **BUT:**
    - False activations can be a problem (e.g., false alarm panic braking)
    - Pretty good autonomy results in bad human supervision

If you blame the human operator for a crash, it's not a self-driving car

© 2019 Philip Koopman

Ways To Improve AV Safety

EDGE CASE RESEARCH

- **More safety transparency**
  - Independent safety assessments
  - Industry collaboration on safety
- **Minimum performance standards**
  - "Driver test" is necessary -- but not sufficient
    - How do you measure maturity?
- **Autonomy software safety standards**
  - ISO 26262/21448 + UL 4600 + IEEE P700x
  - Dealing with uncertainty and brittleness

http://bit.ly/2MTbT8F (sign modified)

A Decentralized Energy-Optimal Control Framework for Connected and Automated Vehicles

Andreas A. Malikopoulos, PhD
Terri Connor Kelly and John Kelly Career Development Associate Professor
Department of Mechanical Engineering
University of Delaware

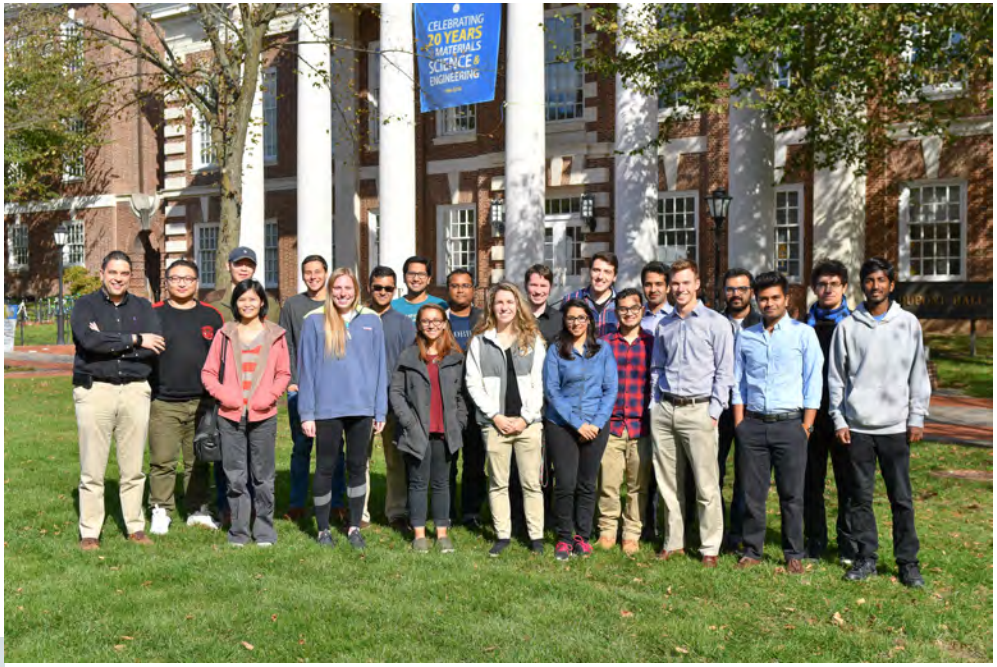
Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions
University of Maryland

April 26, 2018

UNIVERSITY OF DELAWARE

Acknowledgements

- My students and postdocs



- Our sponsors

arpa·e
CHANGING WHAT'S POSSIBLE

U.S. DEPARTMENT OF ENERGY

U.S. DEPARTMENT OF ENERGY
SMARTMOBILITY
Systems and Modeling for Accelerated Research in Transportation

UNIVERSITY OF DELAWARE

Mobility has evolved over the years…

Late 1800's

Early 1900's

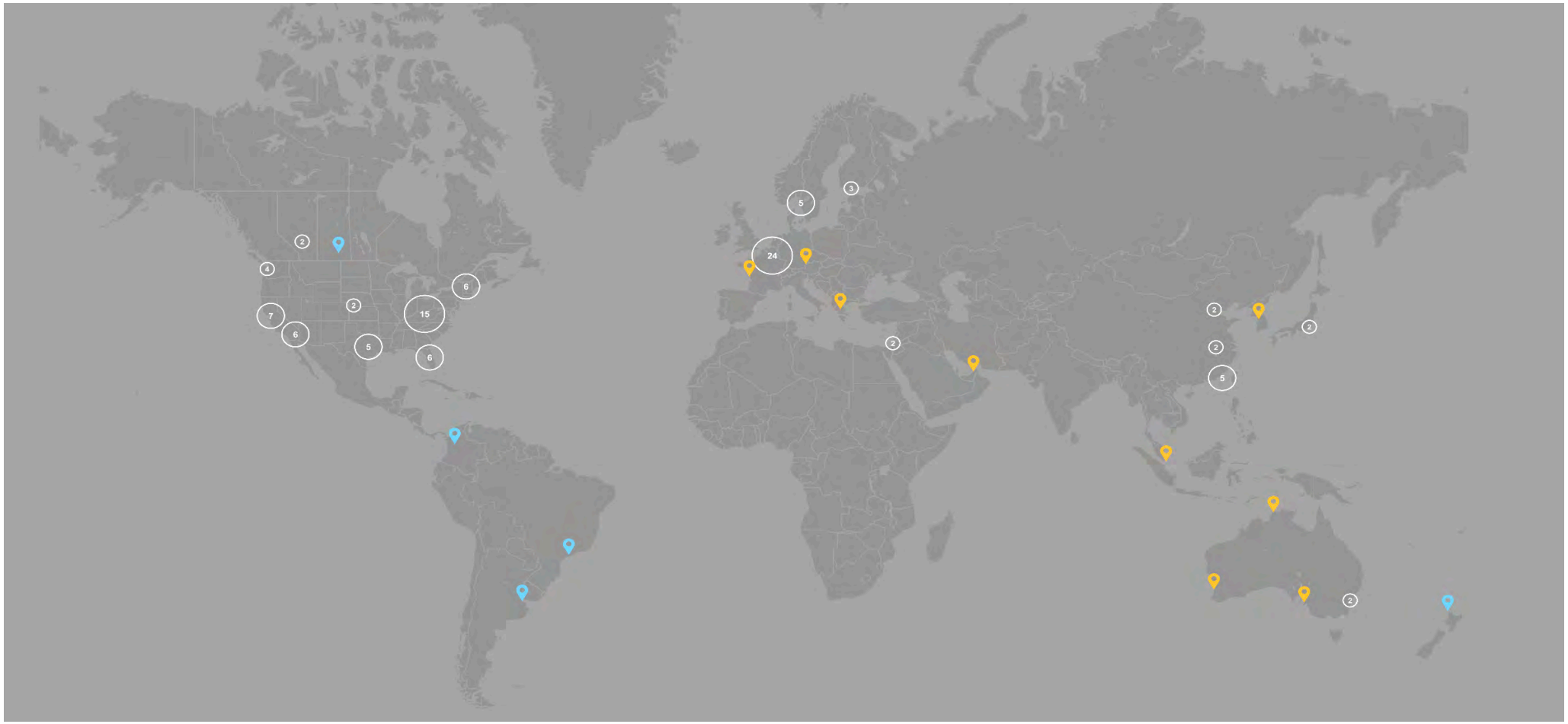
Today

Near future…

UNIVERSITY OF DELAWARE

Where do we stand today?

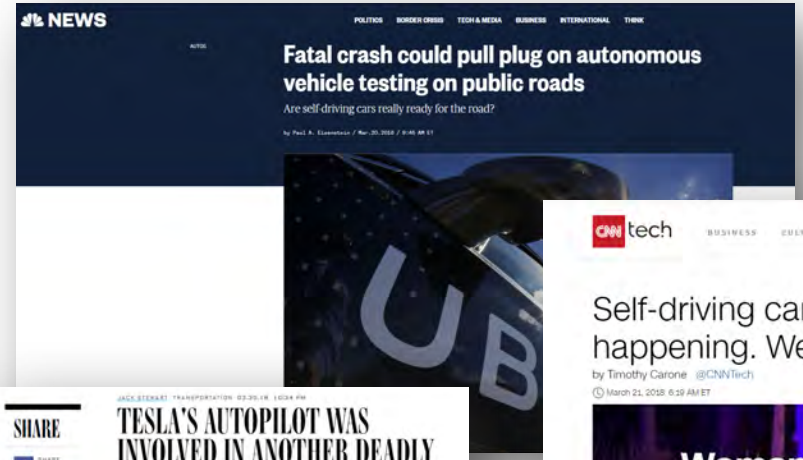
- At least 47 cities around the world are piloting autonomous cars today
- An additional 22 cities have begun considering pilot programs

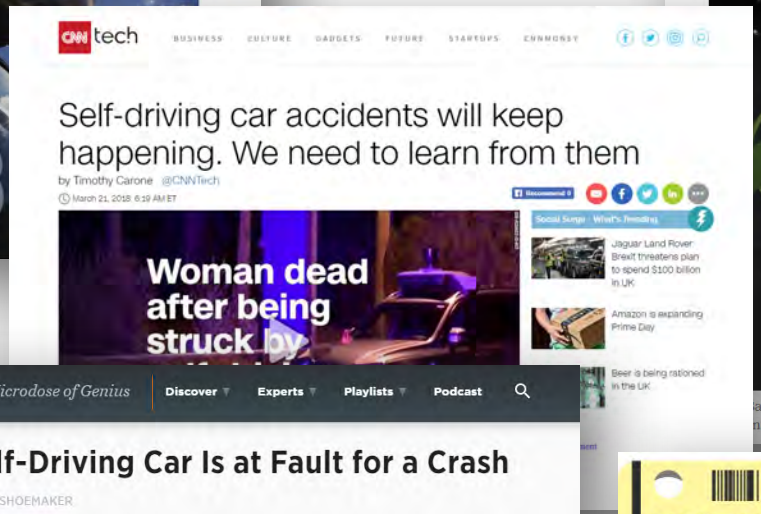


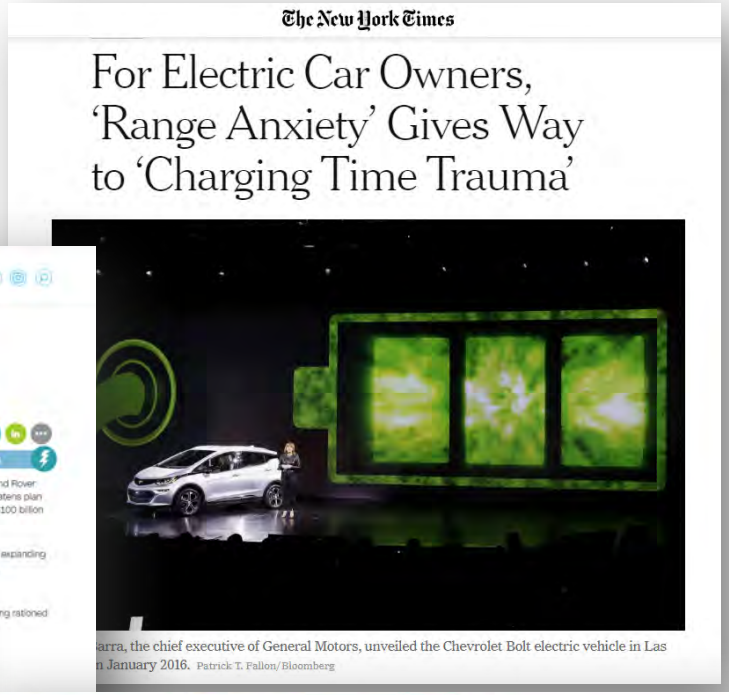
Source: Bloomberg Philanthropies

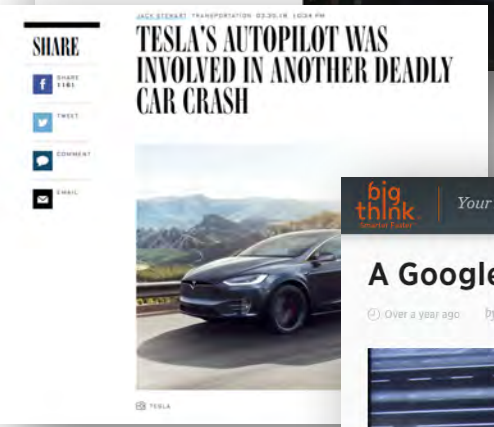
UNIVERSITY OF DELAWARE

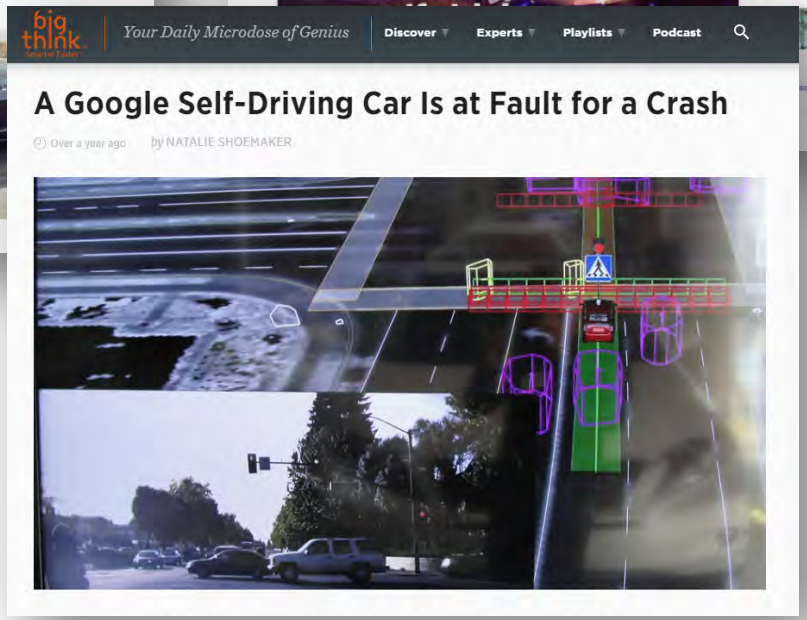
The focus has been on safety

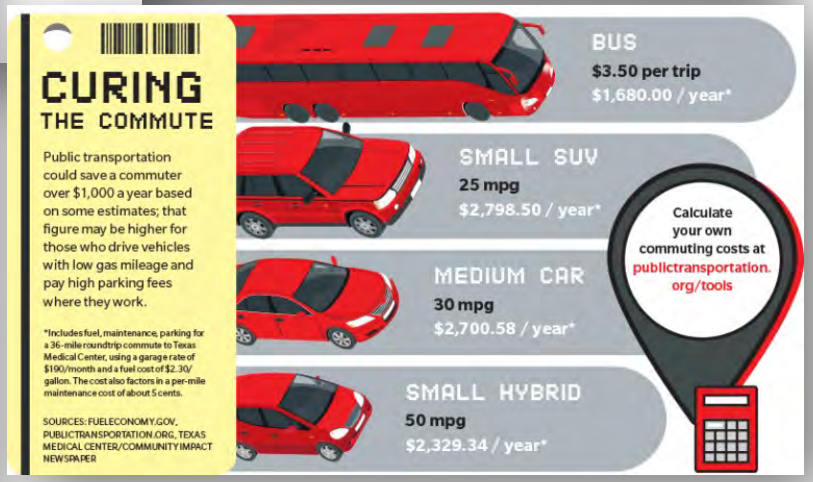










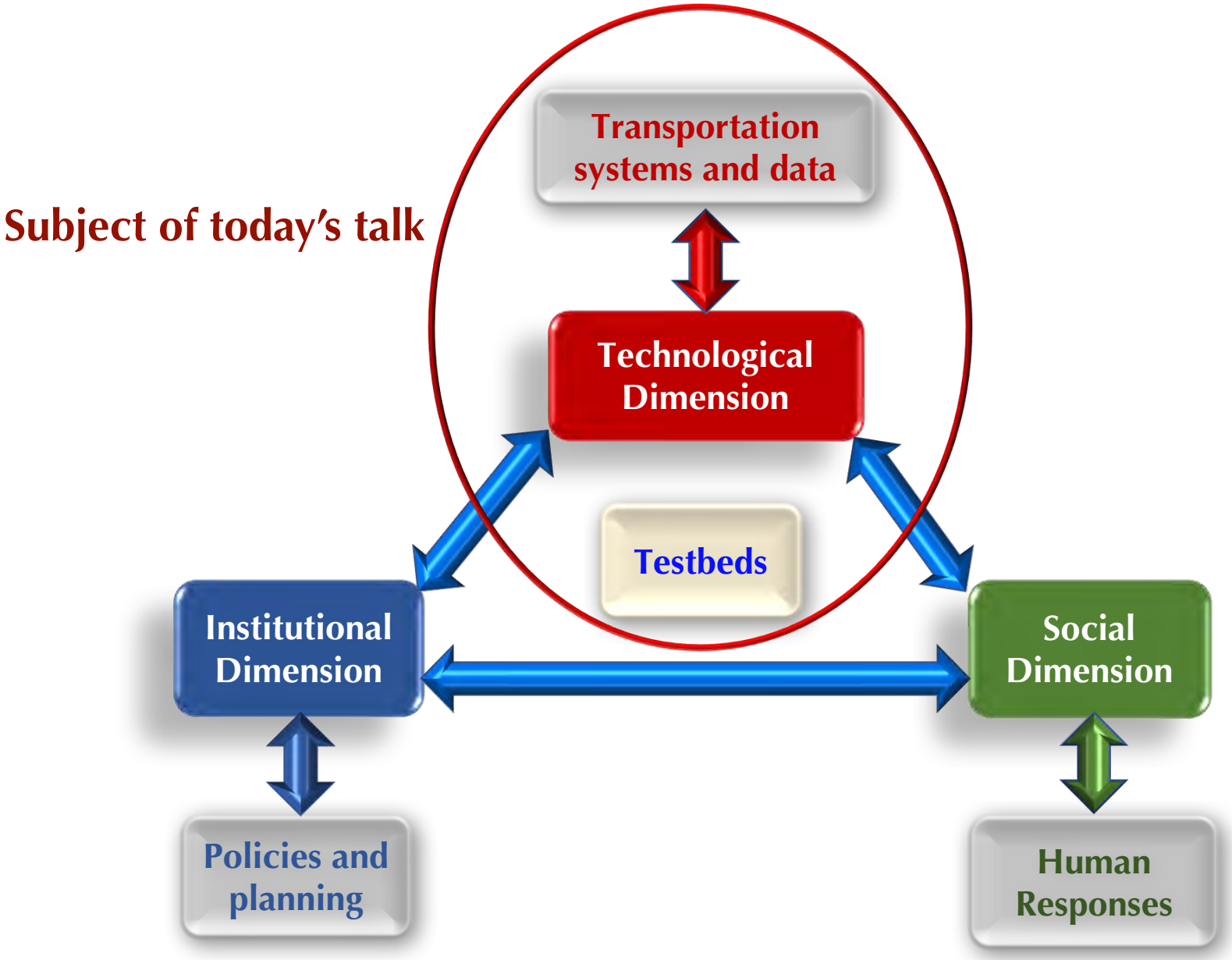


Can we also address efficiency?

Can we coordinate vehicles?

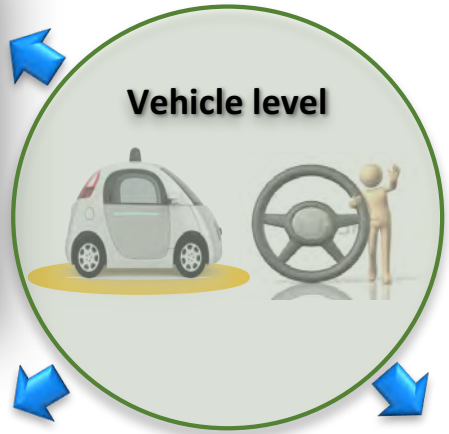
Can we then scale up?

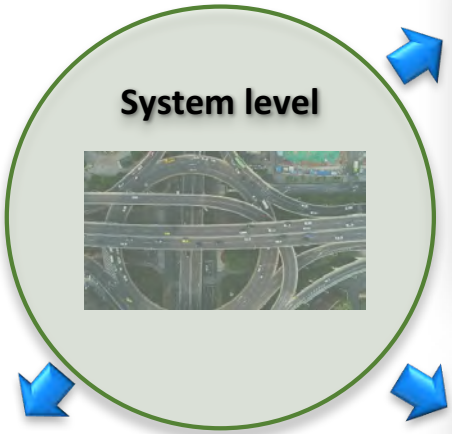
Sociotechnical system approach



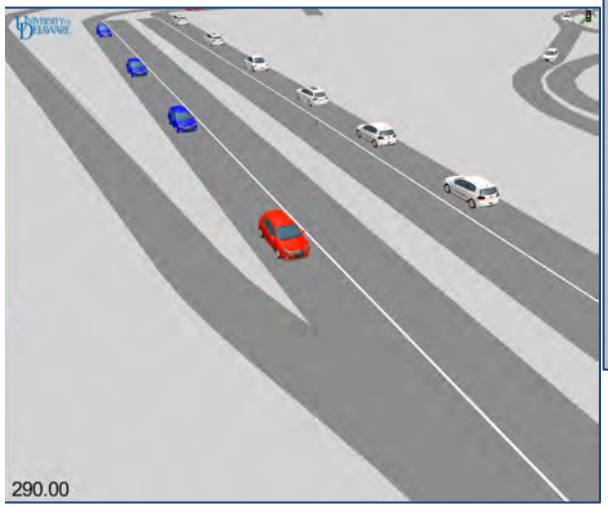
ARPAE NEXTCAR project

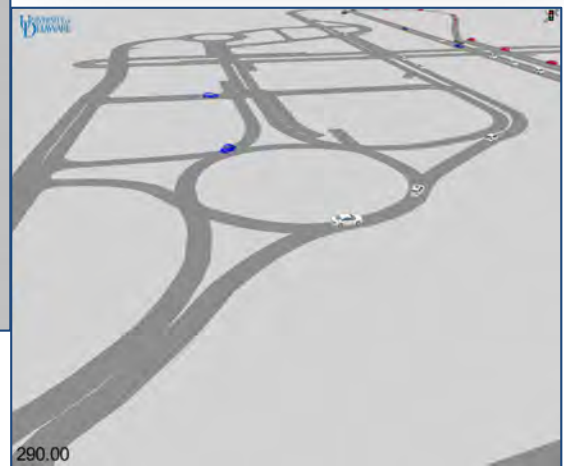
Source:
https://www.electronicsweekly.com





Source:
https://faf.ornl.gov/faf4/



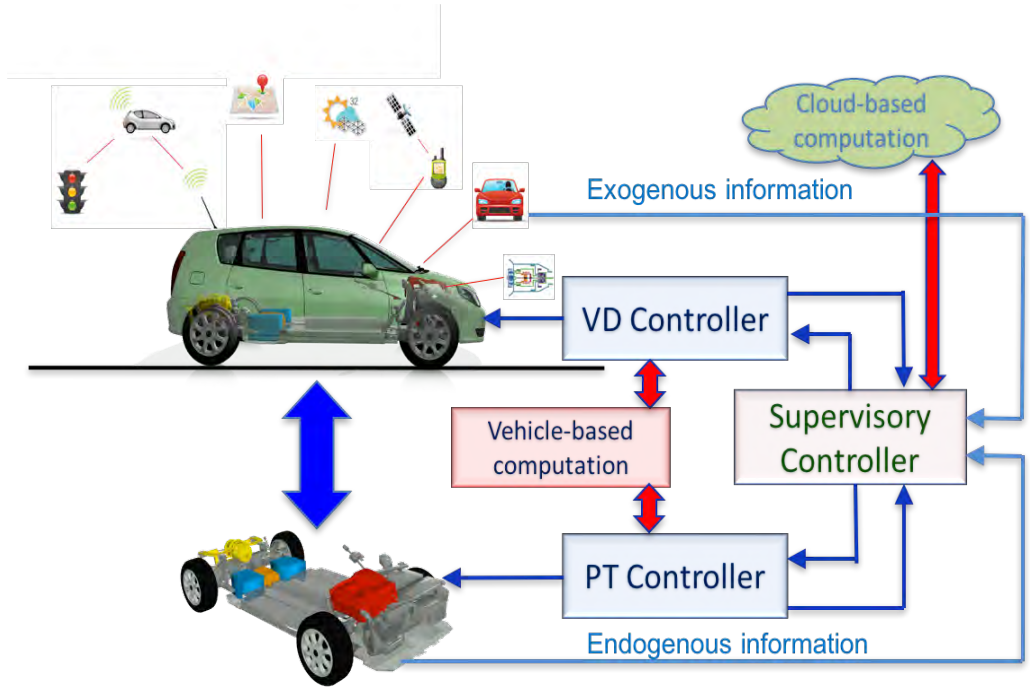


Control architecture

We develop control technologies in an **Audi A3 e-tron plug-in hybrid electric** vehicle based on a **two-level joint** optimization framework:

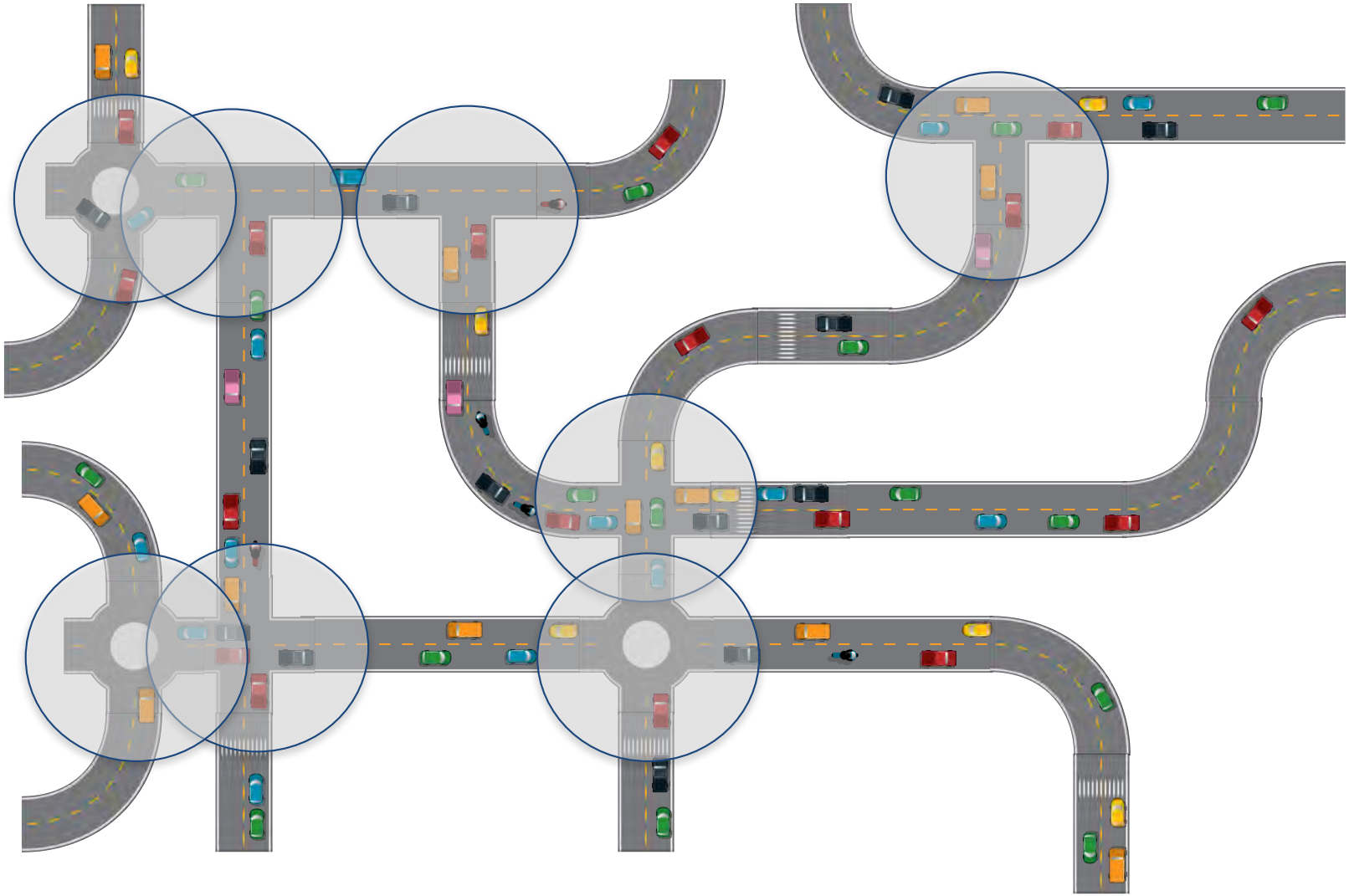
(1) the supervisory and vehicle dynamic (VD) controllers will perform the **level I** optimization, e.g., routing, acceleration/deceleration and speed profiles aimed at minimizing (ideally, eliminating) stop-and-go driving, and

(2) the powertrain (PT) controller will perform a **level II** powertrain optimization for the optimal vehicle speed profile imposed by level I optimization.

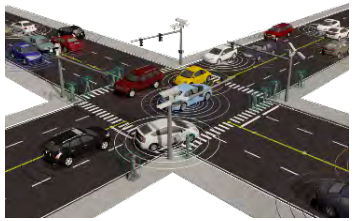


Transportation network

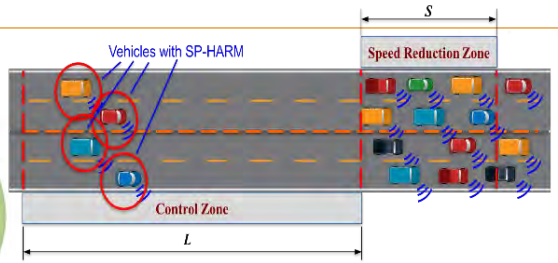
Focus on individual transportation segments



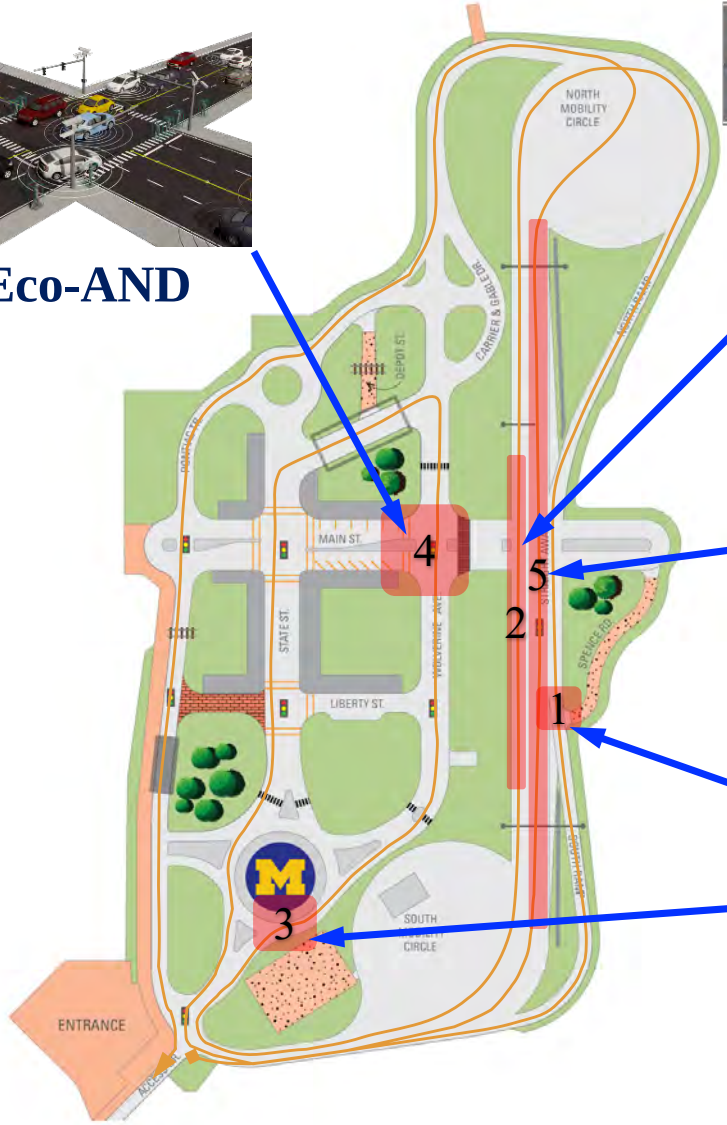
Route in Mcity

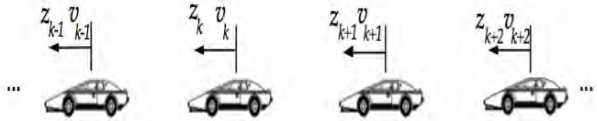


Eco-AND

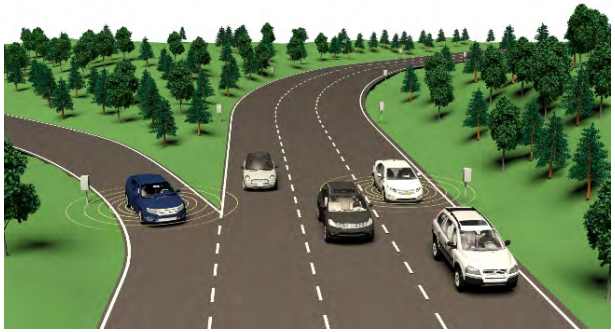


SPD-HARM approach



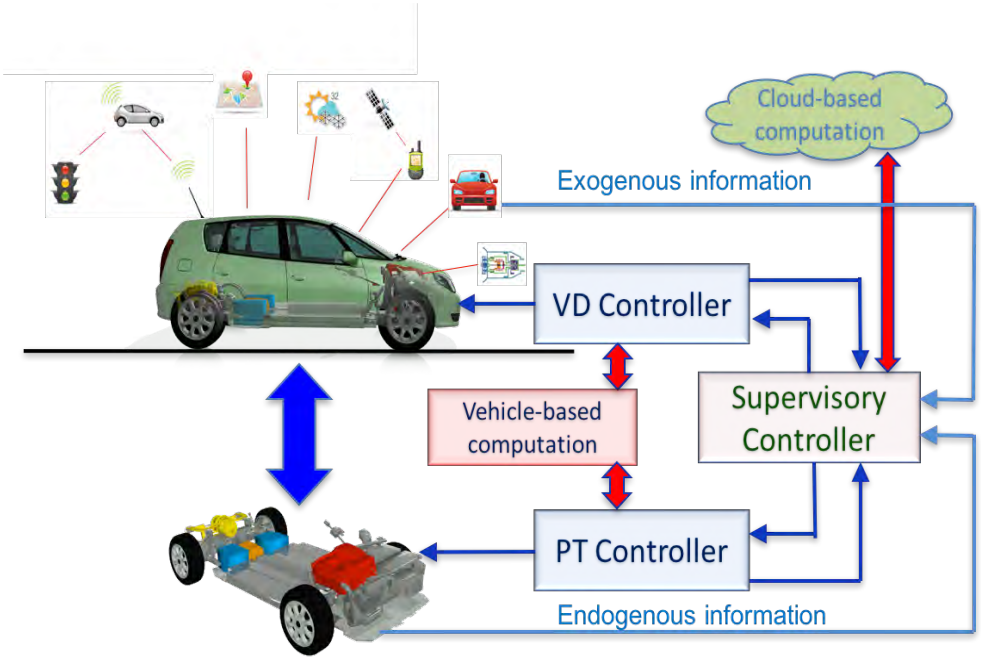


CACC



Vehicle Merging

Integration at UD's driver simulation testbed



Vehicle merging

- We model each vehicle *i* as a double integrator

$$\begin{aligned} \dot{p}_i &= v_i(t) \\ \dot{v}_i &= u_i(t) \end{aligned} \tag{1}$$

- State and control constraints

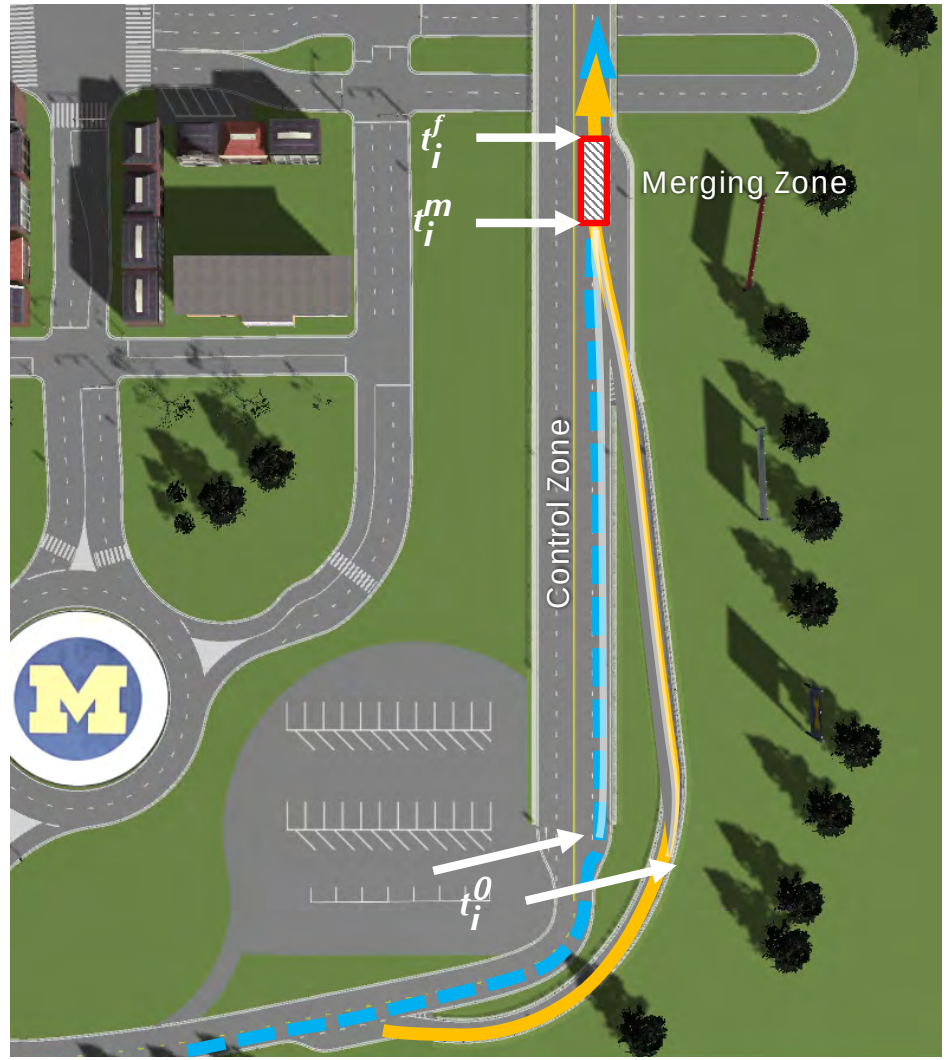
$$\begin{aligned} u_{min} \leq u_i(t) \leq u_{max}, \text{ and} \\ 0 \leq v_{min} \leq v_i(t) \leq v_{max}, \ \forall t \in [t_i^0, \ t_i^m] \end{aligned} \tag{2}$$

- Rear-end safety constraint

$$s_i(t) = p_{i-1}(t) - p_i(t) \geqslant \delta(v_{ave}(t)), \ \forall t \in [t_i^0, t_i^m] \tag{3}$$

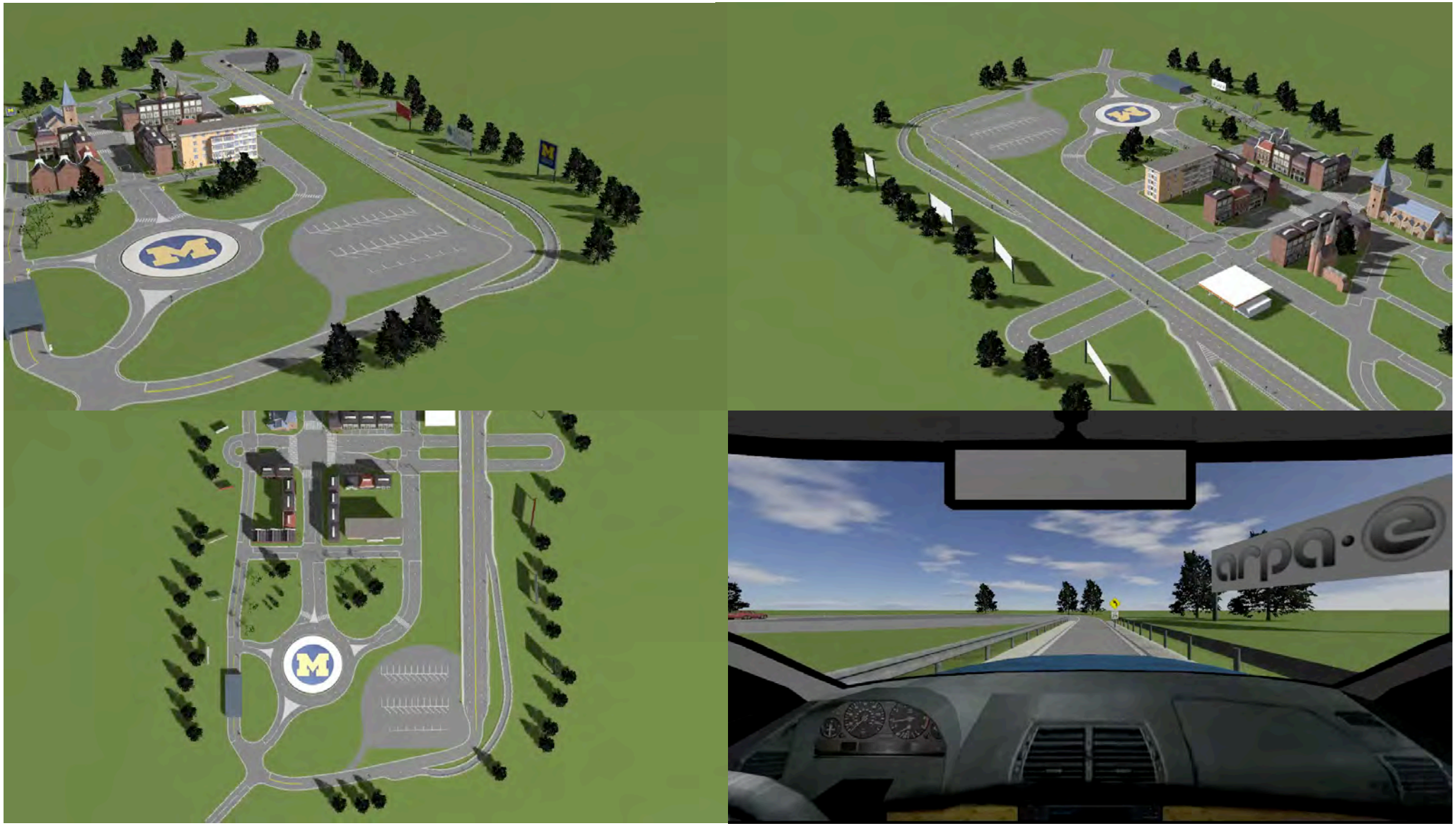
- Lateral collision avoidance constraint

$$\begin{aligned} \Gamma_i &\triangleq \left\{ t \mid t \in [t_i^m, t_i^f] \right\} \\ \Gamma_i \cap \Gamma_j &= \varnothing, \quad \forall t \in [t_i^m, t_i^f] \end{aligned} \tag{4}$$



[1] Rios-Torres, J., and Malikopoulos, A.A., , "A Survey on the Coordination of Connected and Automated Vehicles at Intersections and Merging at Highway On-Ramps," IEEE Trans. Intell. Transp. Syst., Vol. 18, 5, pp. 1066–1077, 2017.
[2].Rios-Torres, J., and Malikopoulos, A.A., , "Automated and Cooperative Vehicle Merging at Highway On-Ramps," IEEE Trans. Intell. Transp. Syst., Vol. 18, 4, pp. 780–789, 2017.

Vehicle merging

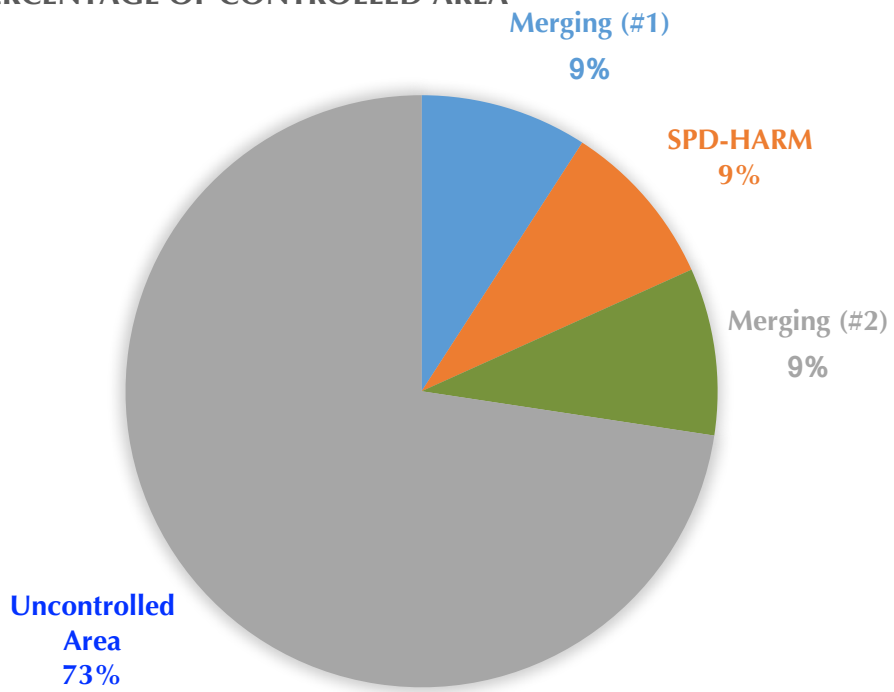


Merging at a roundabout

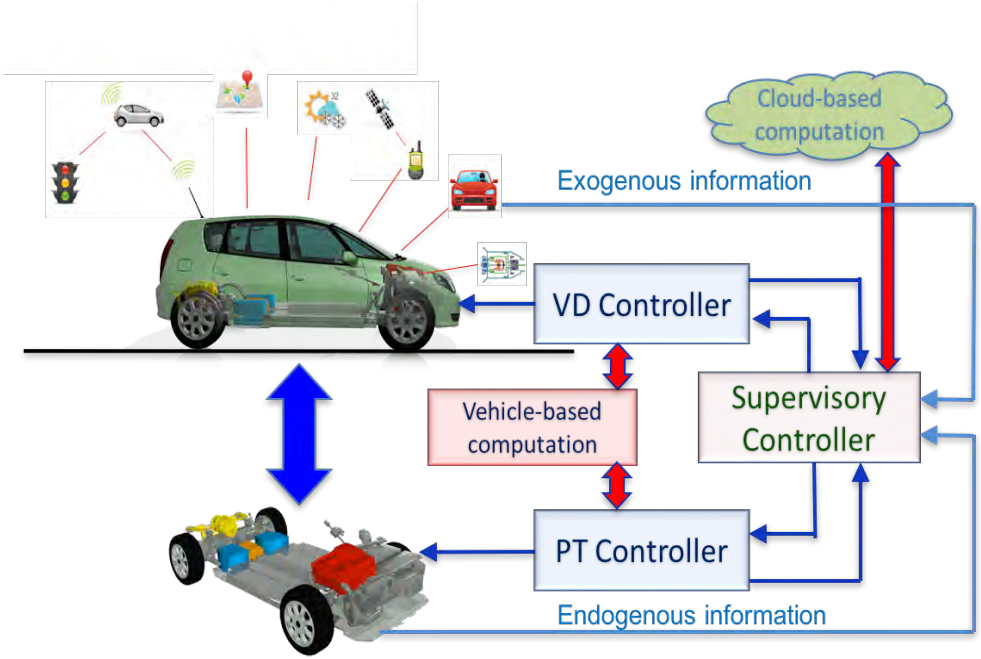
Simulation Results

CAV Penetration	Audi Controller	Optimal PT Controller	Improvement due to PT Controller
0%	28.0	33.8	**20.7%**
100%	32.2	34.2	**6.2%**
Improvement due to VD Controller	**15.0%**	**1.2%**	**22.1%**

PERCENTAGE OF CONTROLLED AREA

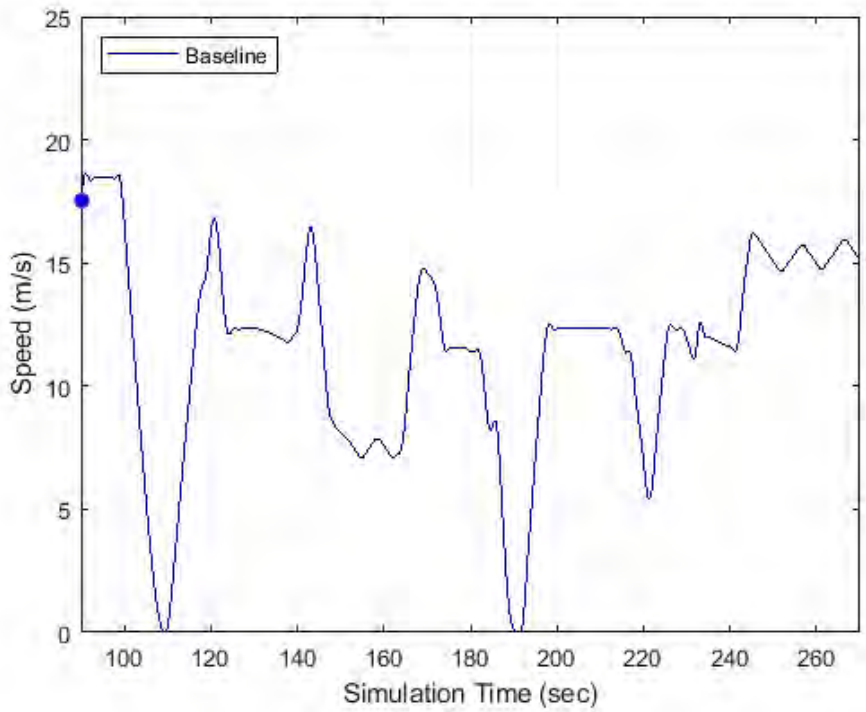


Integration at Bosch facilities

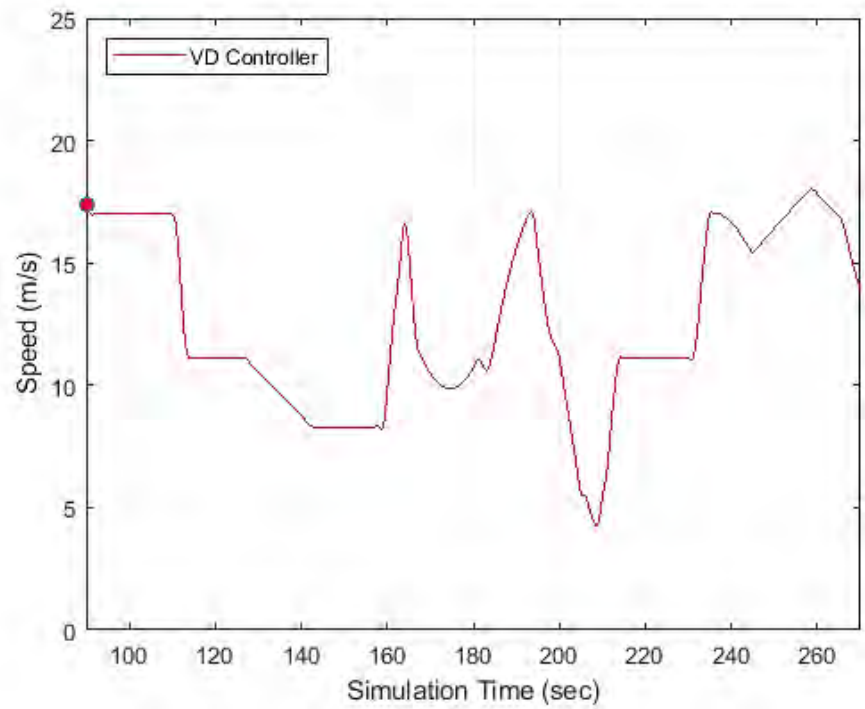


Integration at Bosch facilities

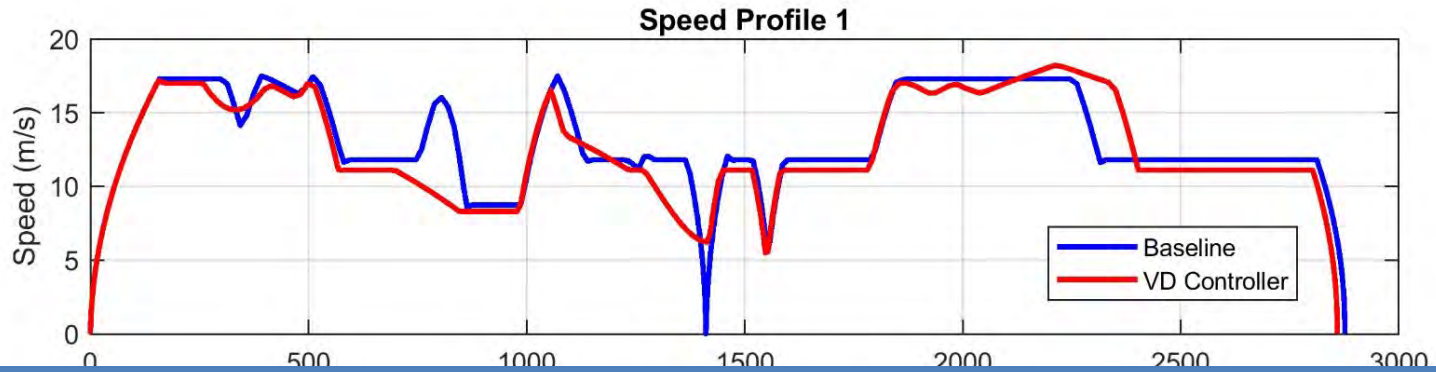
Baseline scenario



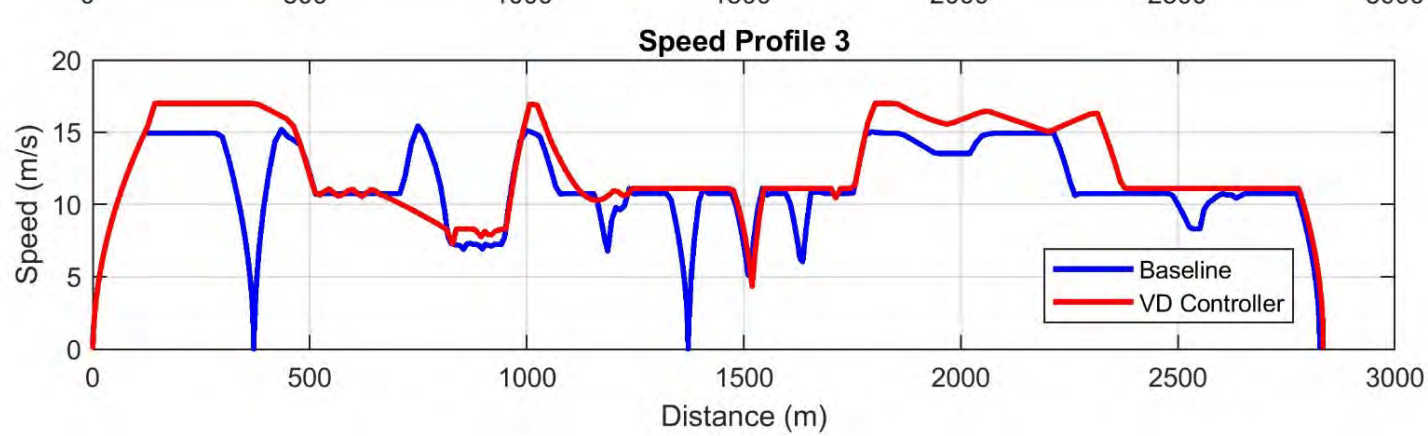
Scenario with VD Controller



Dyno Results at Bosch Facilities

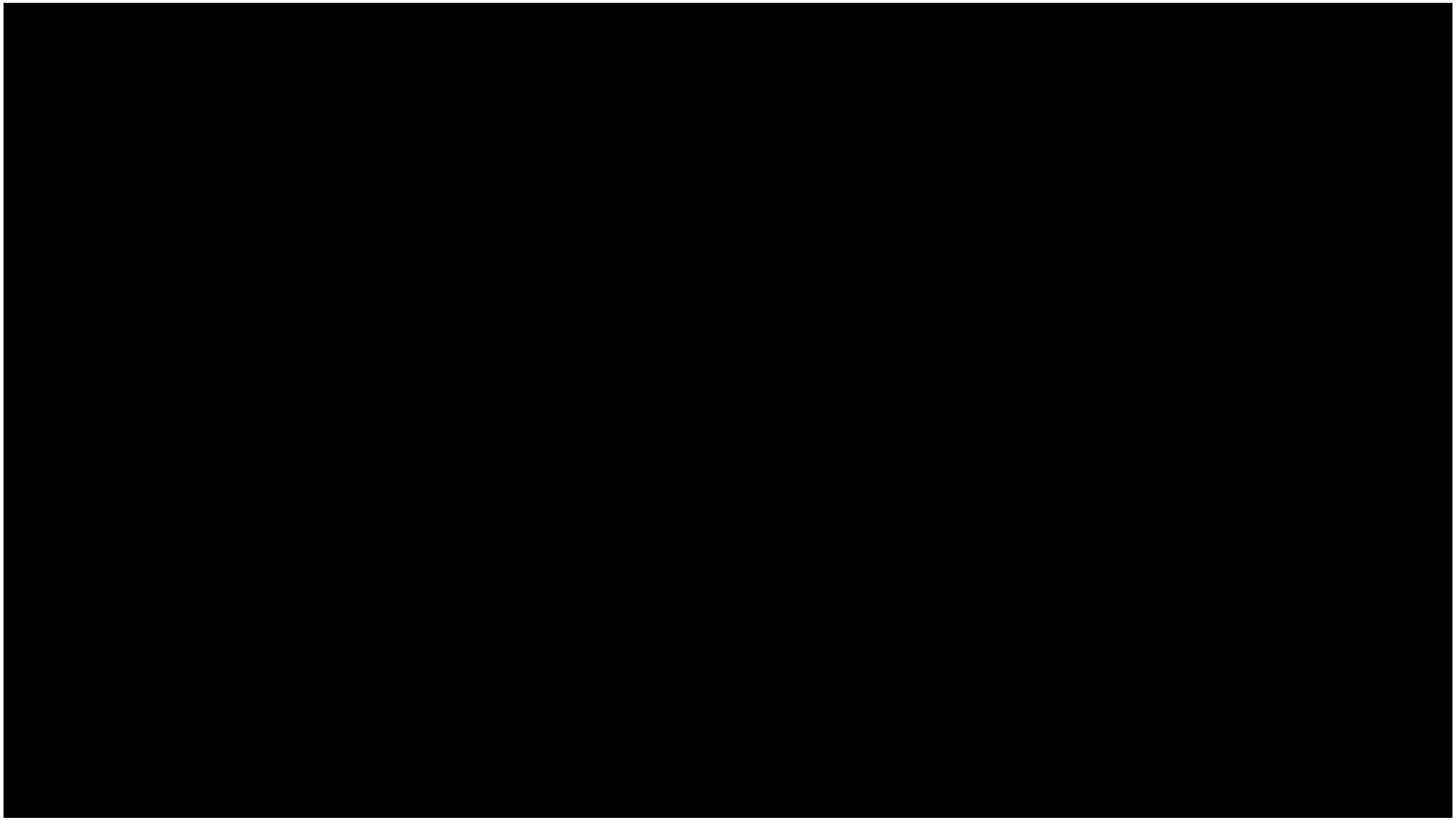


Improvement on MPGe (%)	Speed Profile		
	Speed profile 1	Speed profile 2	Speed profile 3
Dyno (Initial SoC)	**Improvement [%]**	**Improvement [%]**	**Improvement [%]**
60%	13.8	33.7	18.7
75%	29.0	17.4	34.2

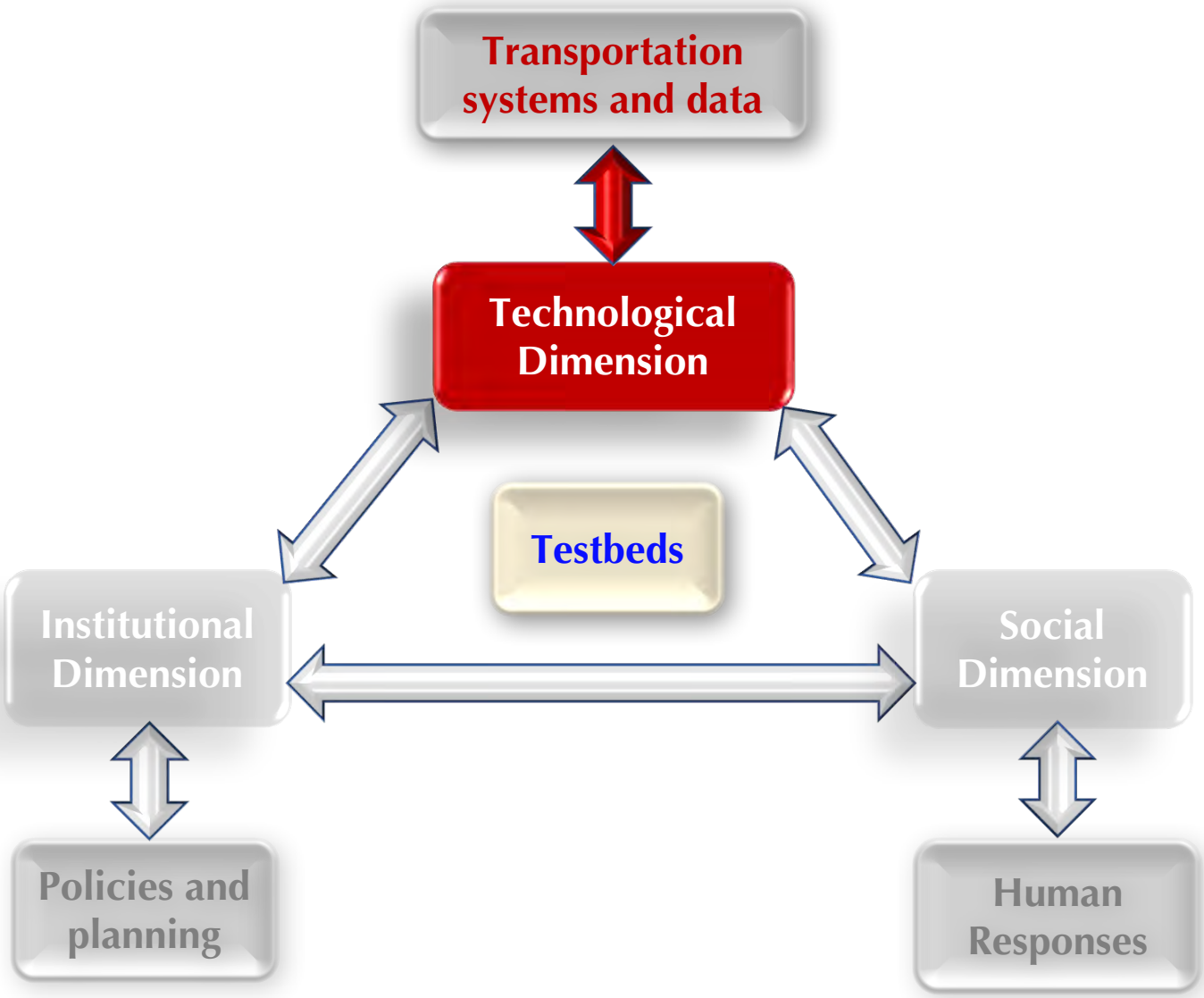


Field testing in MCity

Field testing in Mcity



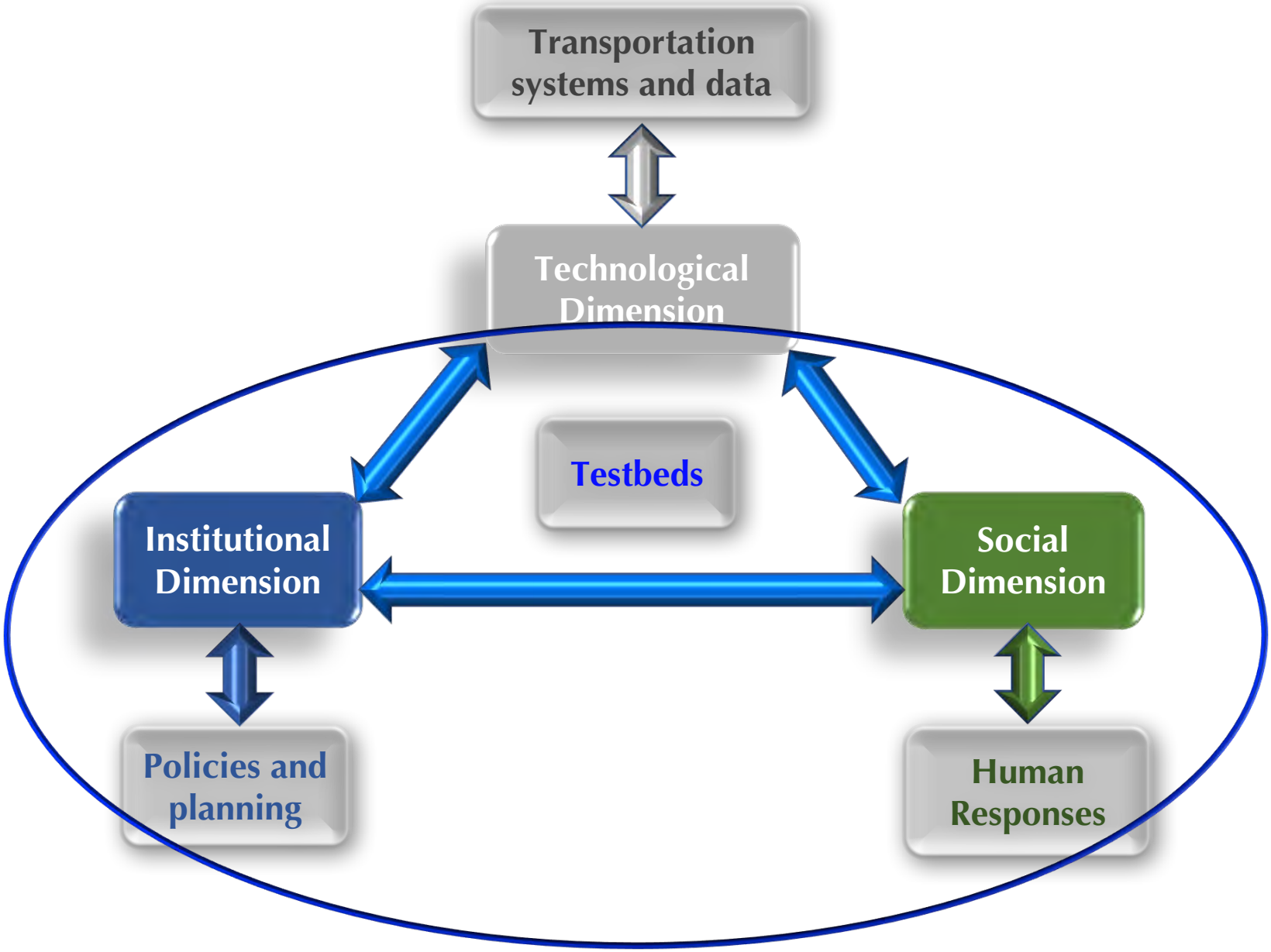
Sociotechnical system approach



UD's scaled smart city (UDSSC) testbed

Team formations

Sociotechnical system approach



Thank you for your Attention!

Andreas A. Malikopoulos, Ph.D.
Terri Connor Kelly and John Kelly Career Development Associate Professor
Director, Information and Decision Science Lab
Department of Mechanical Engineering
University of Delaware

e-mail: andreas@udel.edu
URL: http://sites.udel.edu/ids-lab/

MARYLAND DEPARTMENT OF TRANSPORTATION™

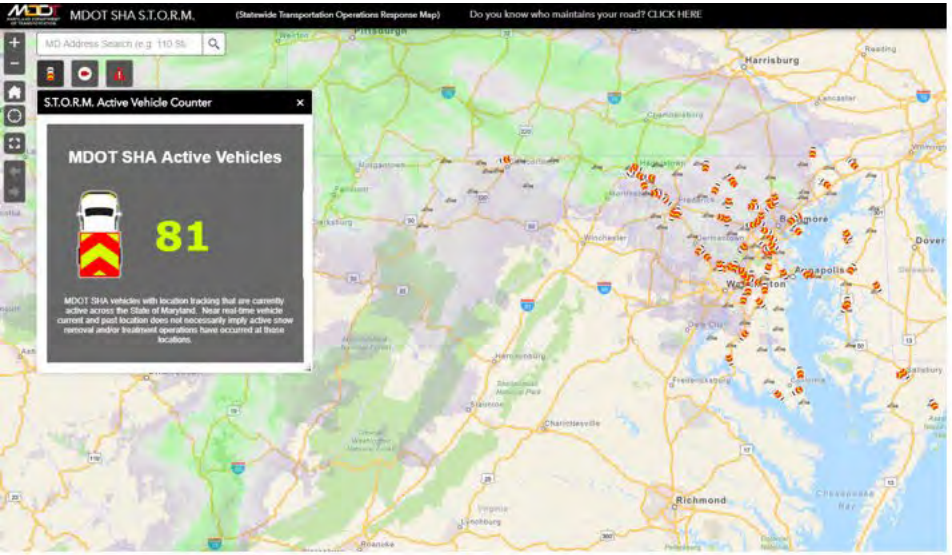
STATE HIGHWAY ADMINISTRATION

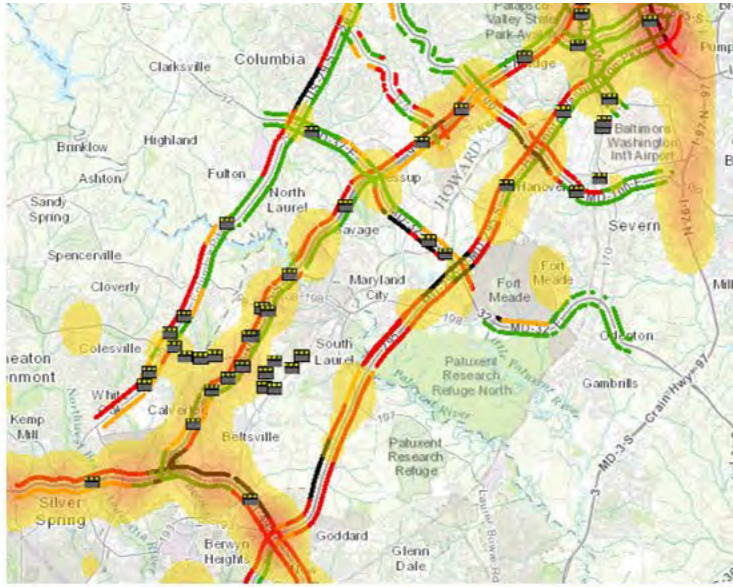
Maryland Cybersecurity Initiatives in a Connected and Autonomous World

April 26, 2019

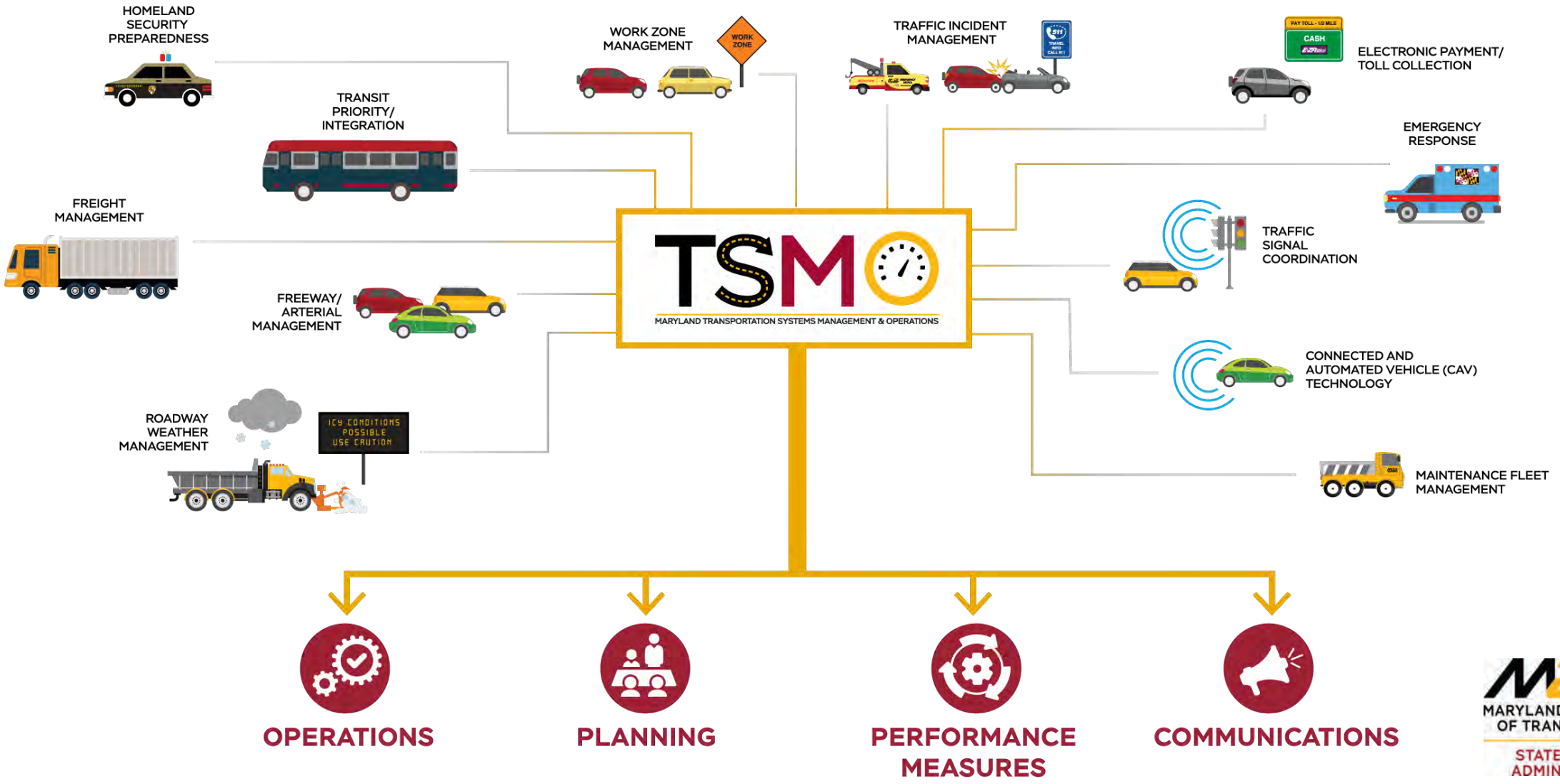
University of Maryland
Center for Risk and Reliability

MDOT SHA OPERATIONS



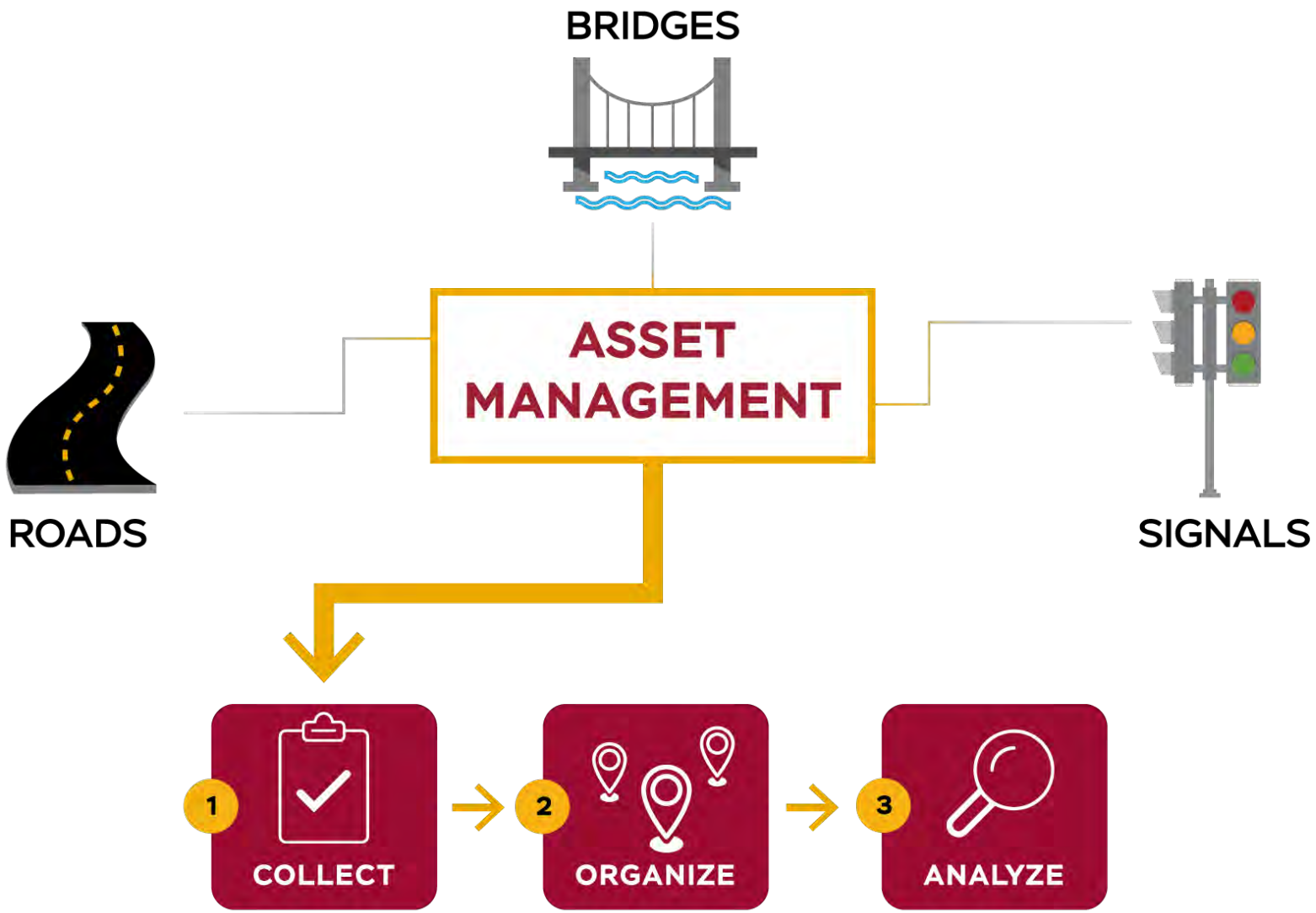


MDOT SHA SYSTEM OF SYSTEMS APPROACH



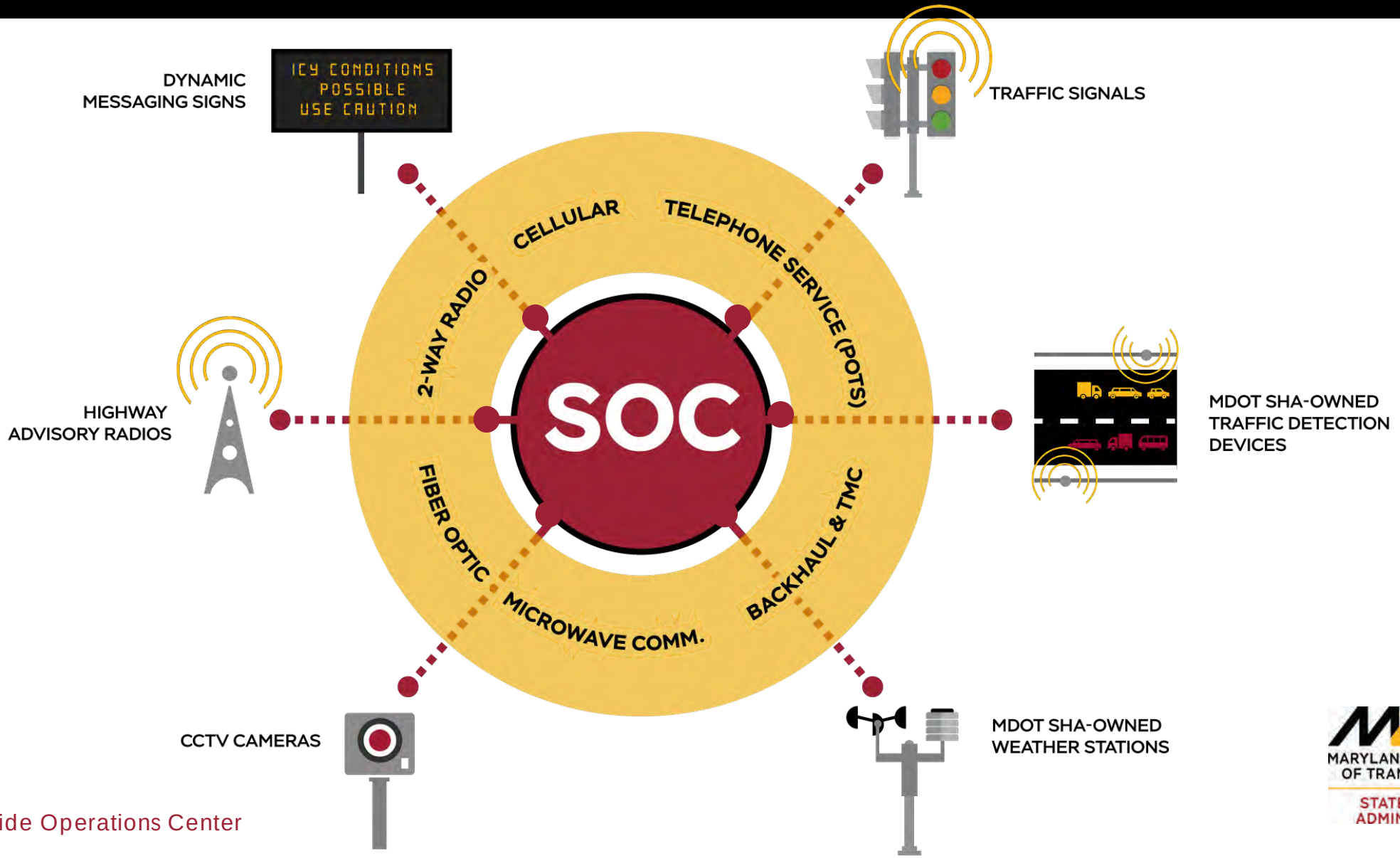
MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

MDOT SHA ASSET MANAGEMENT



MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

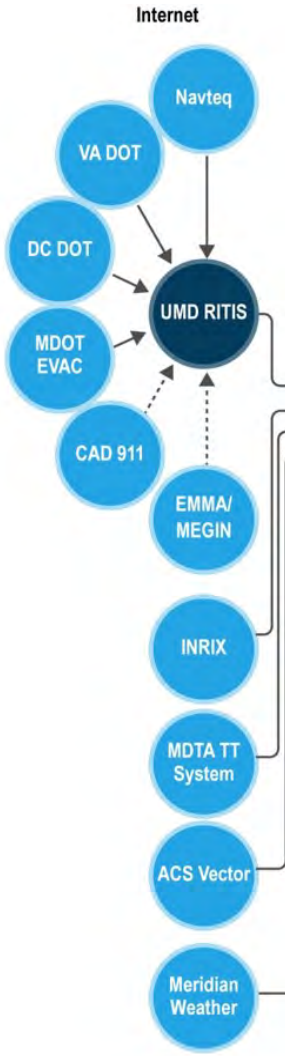
MDOT SHA DIGITAL NETWORK



MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

SOC: Statewide Operations Center

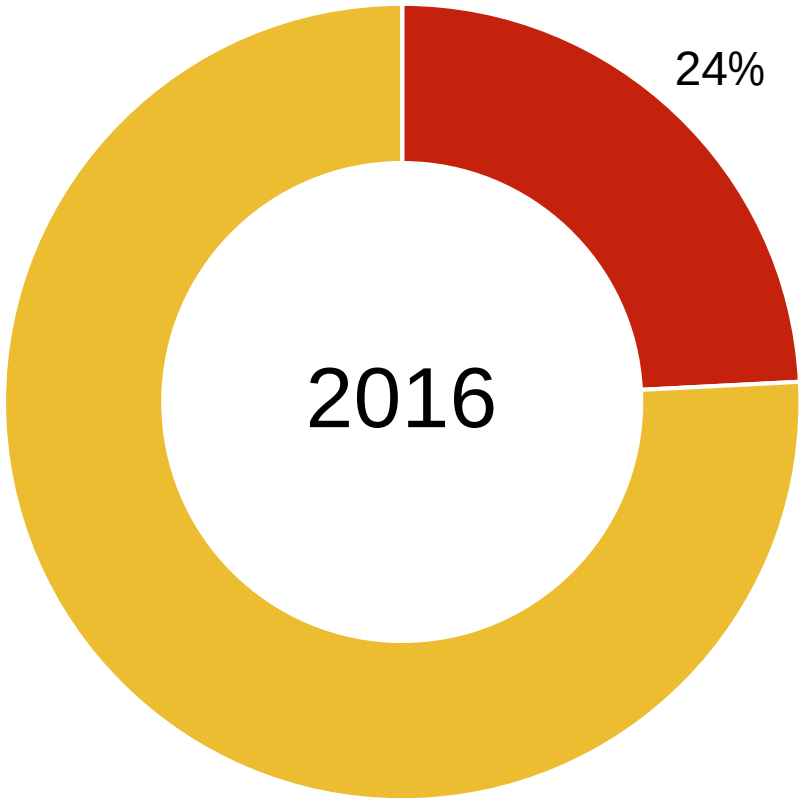
MDOT SHA DIGITAL INFRASTRUCTURE



MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

EXISTING CYBERSECURITY THREATS

Security Incidents vs. all others:



Security Incidents

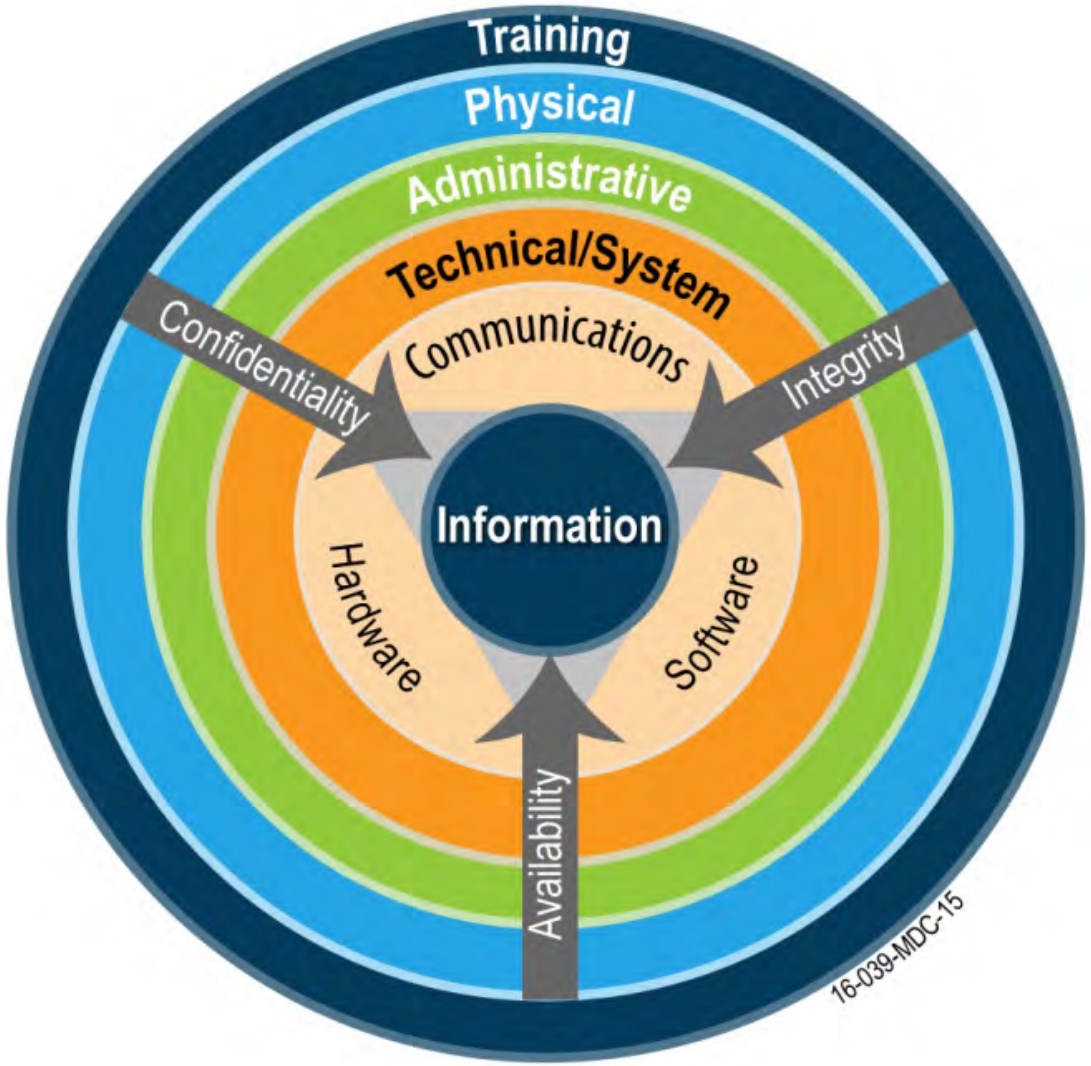
All other Incidents

Reasons for the reduction of security incidents include:

- Aggressive intrusion detection, intrusion prevention, vulnerability scanning and remediation across the Enterprise by MDOT's Office of Transportation Technology Services (OTTS)
- Firewalls have been upgraded across the Enterprise
- Operating Systems, VMWare and infrastructure environments have been upgraded to newer versions with security being a major focus of the vendor updates

MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

OVERVIEW OF POSSIBLE THREATS



MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

REDUCING THREATS AT MDOT SHA

DEVELOPMENT

- Separate production, test and development environments
- Hardware/Software hardening procedures
- State vs Contractor data separate
- “Stateful” Programming
- User Authentication
- Role-based access to sensitive data and applications

OPERATIONS

- Security Logging
- Systems and Network Environments separated by firewalls
- Restrict network connections
- Reviewing firewall rules
- Non-MDOT SHA equipment cannot connect to network
- Anti-virus and anti-malware
- Vulnerability Scanning

DATA

- Encryption
- HTTPS communications
- Ensure sensitive state data is protected
- Password protected role-based access
- Data Classification Document with impact ratings for Confidentiality, Integrity and Availability
- Data Governance

MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

CAV CYBERSECURITY POLICY

Connected and Automated Vehicles (CAV) Working Group

Created by Maryland Department of Transportation Secretary Pete Rahn in December 2015

CAV Technical SubGroup
(MDOT, MSP, other agencies as necessary)

- **Triage Team for CAV Applications**
  (MDOT, MSP, other agencies as necessary)
- **Technical/Project Coordination**
  (MDOT)

CAV Policy SubGroup
(includes external partners)

- **Develop / Modify CAV Permit Process**
  (includes external partners)
- **Policy/Planning Coordination**
  (MDOT)

CAV Freight SubGroup
(includes external partners)

Emergency Responder SubGroup
(includes external partners)

FUTURE CYBERSECURITY THREATS

New entry points will offer potential cybersecurity threats

Private sector consumer driver products and systems require new security protocols

Examples:

Distributed Denial of Service (DDOS)
Service of systems is denied by attacks and results in disruption of traffic signals and flow and potential damage to infrastructure

Remote access
Used to inject malware or viruses, view or steal data, or cause damage to targeted computer or network

OPPORTUNITIES FOR IMPROVEMENT

ROADBLOCKS

- Policy constraints

- Procurement limitations at the state level

POTENTIALS

- New opportunities and increased mobility

- Public confidence

- Safe and reliable transportation network

MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

MDOT SHA SYSTEMWIDE INITIATIVES

Telecommunication plan expansion

Partnerships with stakeholders and businesses

Educational programs to better the community's understanding of CAVs

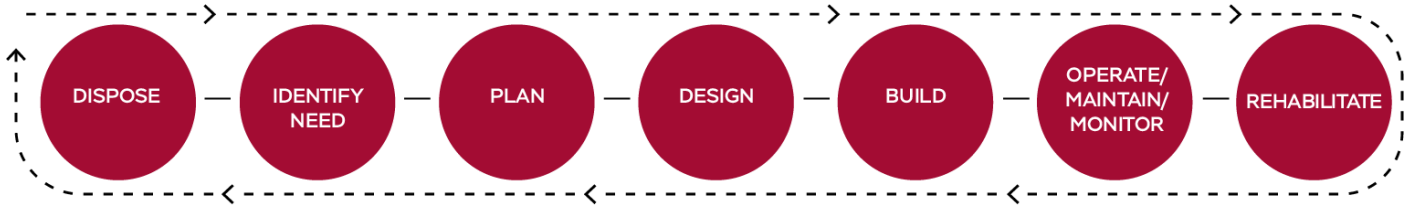
MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

CAV ASSET MANAGEMENT

Robust CAV Asset Management:

- Pavement, bridge, fleet asset data collection from CAV sensors.
- Predictive analytics based on CAV, ITS and Weather data.
- Communication systems, field controllers, and networks can be added to future asset inventory and conditions.
- For future CAV assets, the Security Credential Management System (SCMS) utilizes encryption and certificate management to facilitate trusted communication within the CAV ecosystem.

Best Asset Management Practice!!!



Adapted from: International Infrastructure Management Manual 2015

Current TAMP plan includes:

- *Inventory of pavement and bridges*
- *Assess historic condition information*
- *New assets being built*

MARYLAND DEPARTMENT OF TRANSPORTATION
STATE HIGHWAY ADMINISTRATION

Safe to Cross

Warning
Adjust Speed
35
MPH

Warning
Red Light

27 minutes to destination
25 minutes to destination
20 minutes to destination

RESOURCES

Gregory Slater
Administrator, MDOT State Highway Administration
410-545-0400 | gslater@sha.state.md.us

Maryland Connected Automated Vehicles
http://www.mva.maryland.gov/safety/MarylandCAV/

MDOT SHA CAV Strategic Plan (link)

QUESTIONS?

NHTSA

NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

NHTSA's FMVSS Considerations for Vehicles with Automated Driving Systems

UMD Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions

04.26.2019

National Highway Traffic Safety Administration's (NHTSA's) mission is:

to save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement activity.

RESEARCH PROGRAM PHILOSOPHY

Mission: Strategize, plan, and implement research programs to continually further Agency's goals in reduction of crashes, fatalities, and injuries.

- **Aligned with Congressional Mandates, DOT & NHTSA goals**
- **Portfolio spans exploratory to regulatory support**
- **Prioritized based on potential for crash/fatality/injury reduction**
- **Consideration for special populations and risk scenarios**
- **Support Defects Office with testing and analysis**
- **Collaborative Research with Industry and Foreign Governments**

Primary Outputs

- Evaluating Emerging Safety Issues and Trends
- Building Knowledge of New Technologies and Issues
- Developing Technology Neutral Test Procedures and Assessment Tools
- Modernizing Requirements and Performance Criteria
- Issuing Best Practices and Guidance
- Building New and Enhanced Capabilities

Automation Technology and Safety

Automated vehicle technology that accurately detect, recognize, anticipate, and respond to the movements of all transportation system users could lead to breakthrough gains in transportation safety.

Safety by the Numbers

- An estimated **39,141** people lost their lives on all modes of our transportation system in 2017. The vast majority—37,133 deaths—were from motor vehicle crashes[A,B]
- *Driver Factors:* Of all serious motor vehicle crashes, **94 percent** involve driver-related factors, such as impaired driving, distraction, and speeding or illegal maneuvers.

  In 2017:
  - Nearly **11,000** fatalities involved drinking and driving.[B]
  - Speeding was a factor in nearly **10,000** highway fatalities.[B]
  - Nearly **3,500** fatal crashes* involved distracted drivers.[B]
- *Commercial Vehicles:* **13 percent** of annual roadway fatalities occur in crashes involving large trucks.[B]
- In 2017, **82 percent** of victims in fatal large truck crashes were road users who were not an occupant of the truck(s) involved.[B]
- *Professional Drivers:* Professional drivers are **ten times** more likely to be killed on the job, and nearly nine times more likely to be injured on the job compared to the average worker.[C]
- *Pedestrians:* **5,977** pedestrians were killed by motor vehicles in 2017, representing 16 percent of all motor vehicle fatalities.[B]
- *Highway-Rail Grade Crossings:* Over the past decade, highway rail grade crossing fatalities averaged **253** per year, representing about one-third of total railroad-related fatalities.[A]

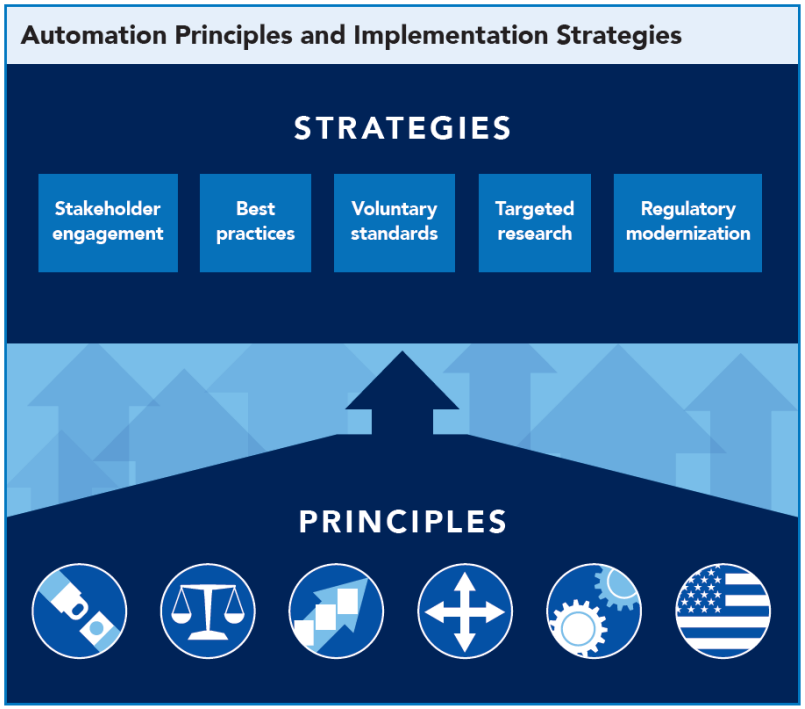
Sources:
A U.S. Department of Transportation, Bureau of Transportation Statistics, special tabulation, September 8, 2018
B NHTSA 2017 Fatal Motor Vehicle Crashes: Overview (DOT HS 812 603)
C Beede, David, Regina Powers, and Cassandra Ingram, *The Employment Impact of Autonomous Vehicles*, U.S. Department of Commerce, Washington, DC: http://www.esa.doc.gov/sites/default/files/Employment%20Impact%20Autonomous%20Vehicles_0.pdf

* *This number is likely underreported.*

OVERVIEW

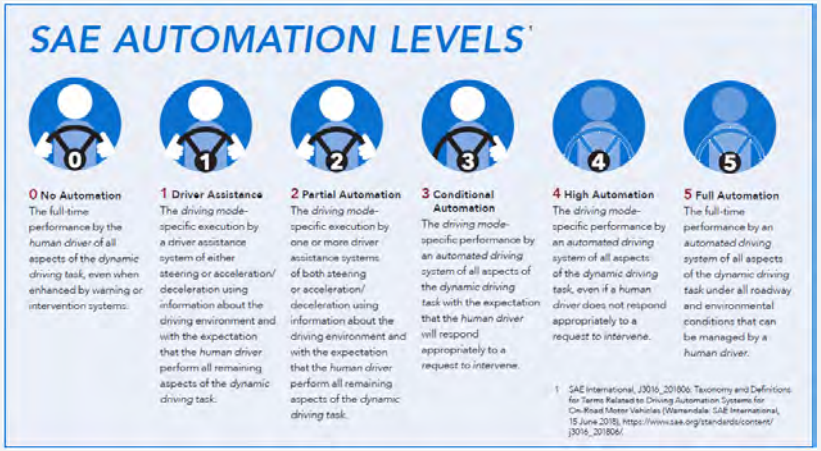
- Policy (3.0, 2.0)
- Research
- Regulatory Efforts

POLICY



Preparing for the Future of Transportation (AV 3.0)

- Released October 2018
  - New multimodal safety guidance
  - Clarifies policy and roles
  - Outlines how to work with U.S. DOT as automation technology evolves



POLICY

A Vision for Safety (AV 2.0)

- Voluntary guidance on design, testing, and safe deployment of ADS remains central to U.S. DOT's Approach.
- Released September 2017.
- Encourages companies to consider and document their approach to 12 safety elements.

1. Vehicle Cybersecurity
2. System Safety
3. Operational Design Domain
4. Object and Event Detection and Response
5. Fallback (Minimal Risk Condition)
6. Validation Methods
7. Human Machine Interface
8. Crashworthiness
9. Post-Crash ADS Behavior
10. Data Recording
11. Consumer Education and Training
12. Federal, State, and Local Laws

Company VSSA Disclosures

- Apple
- AutoX
- Ford
- GM
- Mercedes-Benz/Bosch L4-L5
- Mercedes Benz L3
- Navya
- Nuro
- Nvidia
- Starsky Robotics
- Uber
- Waymo
- Zoox

As of 4/2419

RESEARCH

1. **Removing Regulatory Barriers**
2. **ADS System Safety Performance; Functional Safety; Cybersecurity**
3. **Human Factors**
4. **Crashworthiness Occupant Protection**

Removing Regulatory Barriers

Background: Review of Federal Motor Vehicle Safety Standards (FMVSS) for Automated Vehicles

- Preliminary Report, March 2016

  https://rosap.ntl.bts.gov/view/dot/12260

- Volpe National Transportation Systems Center
  - Identify instances where existing FMVSS may pose challenges to the introduction of automated vehicles.
- Research Objectives
  - Driver scan for explicit or implicit reference to a human driver.
  - Automated vehicle concept scan to identify challenges for a wide range of automated vehicle capabilities and concepts.

Removing Regulatory Barriers

FMVSS Considerations for Vehicles with Automated Driving Systems

- Multi-year project, initiated in September 2017
- Virginia Tech Transportation Institute (VTTI)
- Research Objectives:
  - Provide technical translation options of FMVSS and related compliance test procedures for ADS-equipped vehicles.
  - Identify any regulatory barriers to self-certification and compliance verification of innovative new vehicle designs with ADS.

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Phase 1

- 30 FMVSS
- Focus: ADS-DVs without manual controls.

Approach

- Code the translation category.
- Detailed analysis of regulatory text & compliance test procedures.
- Engage subject matter experts for review.

Crash Avoidance			Crashworthiness & Occupant Protection		
101 Controls and displays	110 Tire selection and rims and motor home/recreation vehicle trailer load carrying capacity information	124 Accelerator control systems	201 Occupant protection in interior impact	206 Door locks and door retention components	216a Roof crush resistance
102 Transmission shift position sequence, starter interlock, and transmission braking effect	111 Rear visibility	125 Warning devices	202a Head restraints	207 Seating systems	219 Windshield zone intrusion
103 Windshield defrosting and defogging systems	113 Hood latch system	126 Electronic stability control systems for light vehicles	203 Impact protection for the driver from the steering control system	208 Occupant crash protection	222 School bus passenger seating and crash protection
104 Windshield wiping and washing systems	114 Theft protection and rollaway prevention	138 Tire pressure monitoring systems	204 Steering control rearward displacement	210 Seat belt assembly anchorages	225 Child restraint anchorage systems
108 Lamps, reflective devices, and associated equipment	118 Power-operated window, partition, and roof panel systems	141 Minimum Sound Requirements for Hybrid and Electric Vehicles	205 Glazing materials	214 Side impact protection	226 Ejection Mitigation

Reason		Technical Translation Type Description
0	Not performed	Translation evaluated but not performed.
1	Translation is straightforward	The translation performed is straightforward.
2	Limited research may be beneficial	Can translate standards or provisions of standards, maintaining current performance levels, with some limited amount of research for NHTSA to conduct compliance verification for both conventional vehicle designs and new vehicle designs associated with Automated Driving System - Dedicated Vehicles (ADS-DVs).

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

VIRGINIA TECH TRANSPORTATION INSTITUTE

Core Team

Myra Blanco, Ph.D.
PI & Program Manager

Michelle Chaka, M.S.
Co-PI & Crash Avoidance Lead

Warren Hardy, Ph.D.
Co-PI & Crashworthiness Lead

VTTI's FMVSS Expert Group

William Hollowell, Ph.D.
Joseph Kanianthra, Ph.D.
Stephen W. Rouhana, Ph.D.
George Soodoo, M.B.A.
Kenneth Weinstein, J.D.

Research Team Members

Industry Group: GM, NISSAN

Research Institutions: Booz | Allen | Hamilton, SwRI

Test Facilities: DRI Dynamic Research, Inc., mga research corporation

NHTSA — NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Core Group: VIRGINIA TECH TRANSPORTATION INSTITUTE

Stakeholder/ SME Reviewer Group

ADVOCATES FOR HIGHWAY & AUTO SAFETY
AUTO ALLIANCE DRIVING INNOVATION
Automotive Safety Council Prevent Protect Notify
BOSCH
Calspan Safer Highways ... Safer Skies
The Center for Auto Safety
Continental
DAIMLER Daimler Trucks North America
ema Truck & Engine Manufacturers Association
FCA FIAT CHRYSLER AUTOMOBILES
GlobalAutomakers
IIHS Insurance Institute for Highway Safety
MEMA
Mercedes-Benz
NATIONAL SAFETY COUNCIL
NIO
Peloton
SAE INTERNATIONAL
SELF-DRIVING COALITION FOR SAFER STREETS
TESLA
Valeo
Volkswagen
WAYMO
ZOOX

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Crash Avoidance Challenges (FMVSS 100-series)

- FMVSS use of a “human” driver using manually-operated driving controls (steering wheel, brakes, etc.).
- FMVSS that specify the “manner in which a vehicle is controlled” required careful review and consistent translation approach.

Crashworthiness Challenges (FMVSS 200-series)

- FMVSS use of the terms: *driver, driver’s seat, driver’s designated seating position*, and similar terms.
- FMVSS primarily aimed at driver/front row protection.

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Crash Avoidance Challenges (FMVSS 100-Series)

- Cross-walk on functionality categories for physical test execution:

Category	Functionality	102	108	114	118	138	141	101	103	104	110	111	113	124	125	126
Driving Tasks	Steering control			●		●	●				○	○				○
	Speed control (vehicle/engine)			●		●	●		○	○	○	○		○		○
	Service brake application			●		●	●				○	○				○
	Parking brake			●			●					○				
	Gear selection	●		●		●	●		○	○	○	○				○
Vehicle Communications	Telltales/warnings/indicators	●	●	●		●		○						○		○
Key/Ignition Function	Key insertion/removal			●												
	Iginition start/stop	●		●	●	●			○	○	○	○		○		○
	Accessory mode			●	●											
Non-driving Tasks	Door open/close			●	●											
	Non-driving controls		●		●				○	○		○				
Environment Awareness	Visibility							○	○	○		○	○			

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Crash Avoidance Challenges (FMVSS 100-Series)

Evaluation of Test Procedure Methods

FMVSS Considerations for Vehicles with Automated Driving Systems – VTTI

Stakeholder Meetings:
April 2018 & November 2018

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Examples of Cross-cutting Themes in FMVSS

- Use of driver (operator); driver/passenger presence
- Equipment may not be applicable
- Controls, telltales, indicators, and auditory alerts

Analysis of Information Communicated in Vehicles

Categories	Analysis Questions	Examples
Information Communicated	**What is communicated? What type of communication?**	Engaged, warning, malfunction, identification
Delivery Method	**How is information delivered?**	Illumination of a telltale, auditory alert, indicator
Intended For	**Whom is the information for?**	Driver, non-driving occupants, maintenance entity
Expected Response	**What action is expected in response to information?**	After a low tire pressure warning is activated, someone is expected to check the tire(s) and take appropriate action

FMVSS Considerations for Vehicles with Automated Driving Systems - VTTI

Next Steps

- Near–term Completion of Volume 1 Report (12 FMVSS)
- Draft Volume 2 Report (18 FMVSS)

Ellen Lee
NHTSA COR (TO)
E-mail: ellen.lee@dot.gov
Phone: 202-366-1435

Myra Blanco
VTTI PI/Project Manager
E-mail: mblanco@vtti.vt.edu
Phone: 540-231-1551

Regulatory Efforts

Pilot Program ANPRM

Notices of Receipt – Petitions for Temporary Exemption

Regulatory Efforts

Pilot Program for Collaborative Research on Motor Vehicles with High or Full Driving Automation

- Advance Notice of Proposed Rulemaking (ANPRM)
  - Published 10.10.18
  - Seeks public comment related to the near-term & long-term challenges of ADS testing, development & eventual deployment.
    - Potential factors to be considered in designing a pilot program;
    - Use of existing statutory provisions and regulations;
    - Additional elements of regulatory relief; and
    - Exemption petition evaluation.
- Regulations.gov: Docket No. NHTSA-2018-0092.

Regulatory Efforts

Petitions for Temporary Exemptions

- 49 Code of Federal Regulations Part 555 Final Rule
  - Published 12.26.18; Regulations.gov: Docket No. NHTSA-2018-0103.
  - Aims to streamline the application & review process for petitions submitted by manufacturers while continuing to prioritize safety for drivers, occupants, and other road users.
- Notices of Receipt - Temporary Exemption Petitions
  - Published 03.19.19
  - General Motors, LLC (Zero-Emission Autonomous Vehicle or ZEAV)
    - Regulations.gov: Docket No. NHTSA-2019-0016.
  - Nuro, Inc. (R2X)
    - Regulations.gov: Docket No. NHTSA-2019-0017.

Thank you for your attention.

COME WORK FOR US – WE ARE PEOPLE SAVING PEOPLE!!!

Contact Information:

Dee Williams, NHTSA

Email: dee.williams@dot.gov

RAND CORPORATION

Measuring Automated Vehicle Safety: Building Better Outcomes and Policy

Public and policy makers . . .

- Seek information about AV safety that makes sense to them
- Like comparisons to conventional vehicles (which themselves are evolving)
- Want common parameters for AVs, as there are for other motor vehicles
  - Differing and dynamic Operational Design Domains (ODDs) add to differing designs and testing
- Have familiar challenges in understanding risks

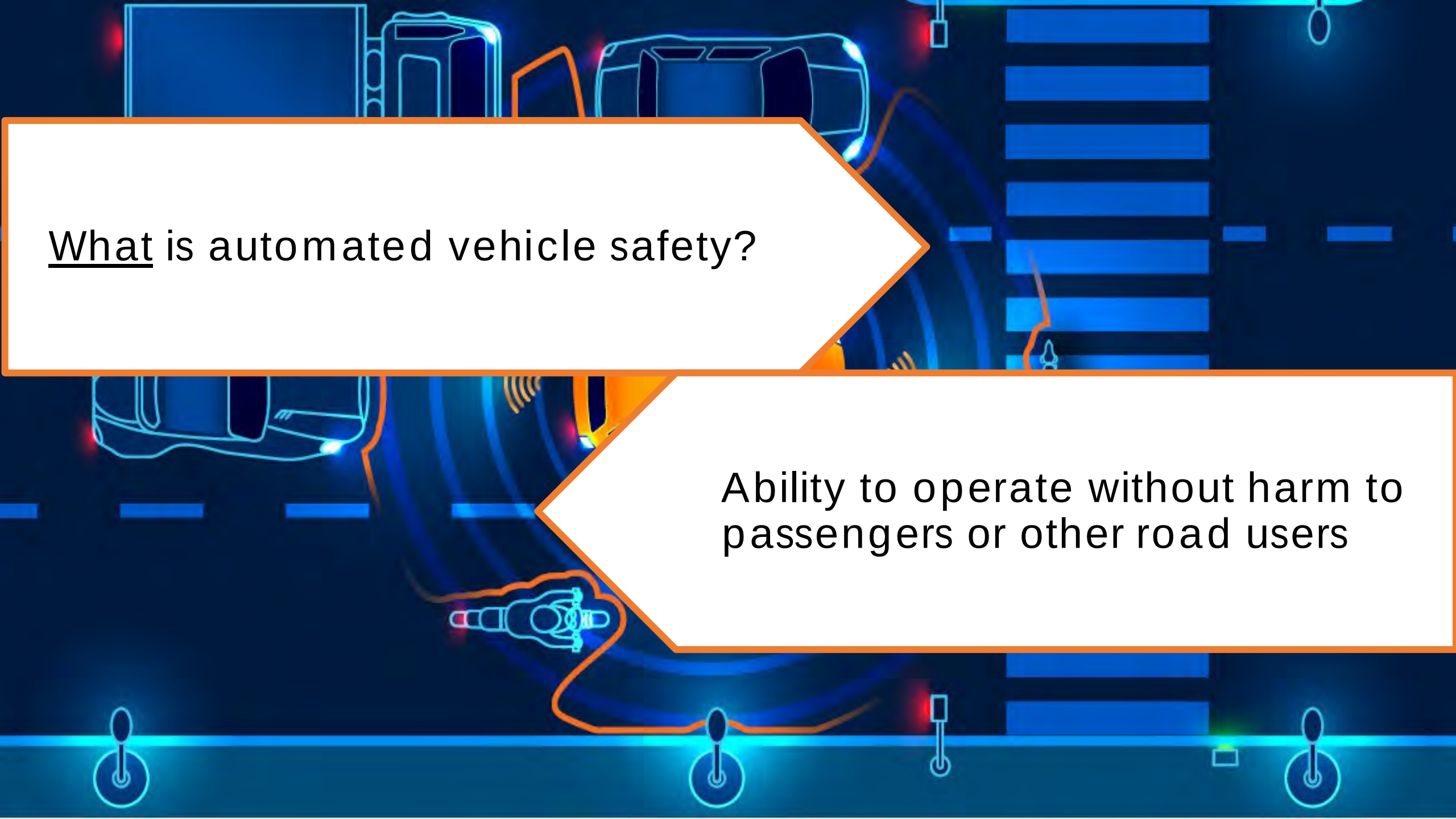
© RAND Corporation, 2019

What is automated vehicle safety?

Where can safety be measured?

When can safety be measured?

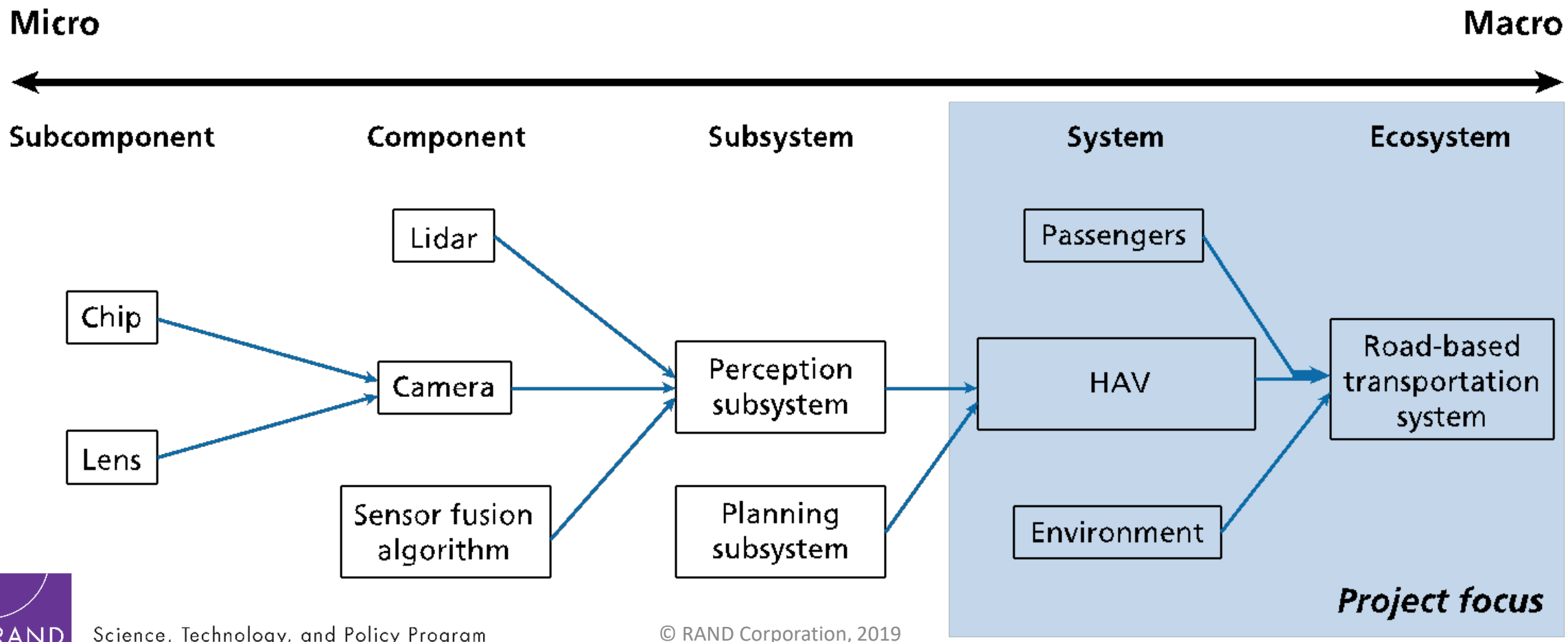
How can safety be measured?



<u>What</u> is automated vehicle safety?

Ability to operate without harm to passengers or other road users

Safety can be and is shaped and measured differently



© RAND Corporation, 2019

AV developers . . .

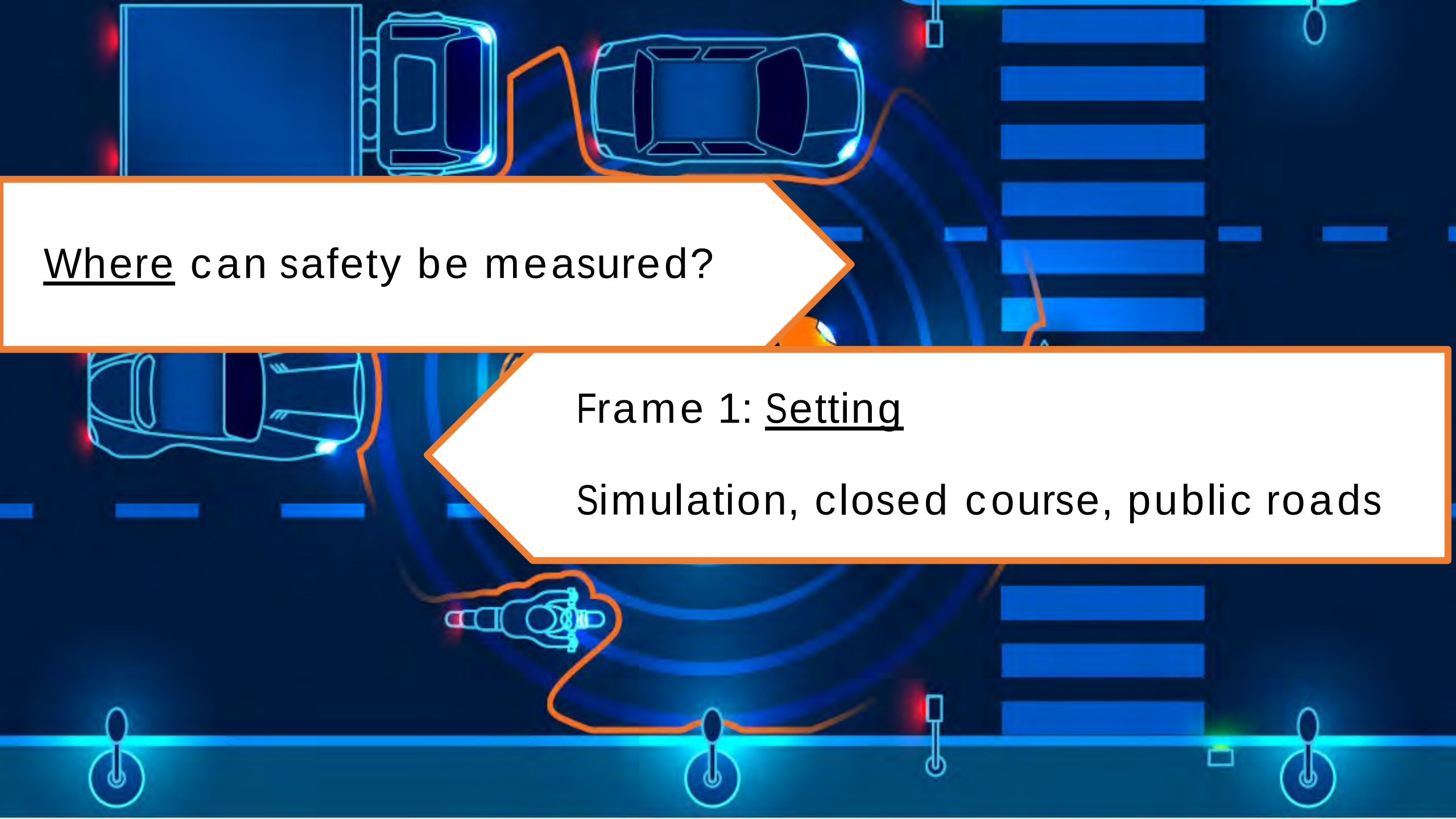
Do different things…

- Different technologies (e.g., cameras, radar, LIDAR, …)
- Different testing protocols and scenarios
- Different capabilities

Are not transparent…

- Different approaches to reporting even when seeming to use the same measure (disengagements)
- Accentuate the positive and share selectively (voluntary safety self-assessments)

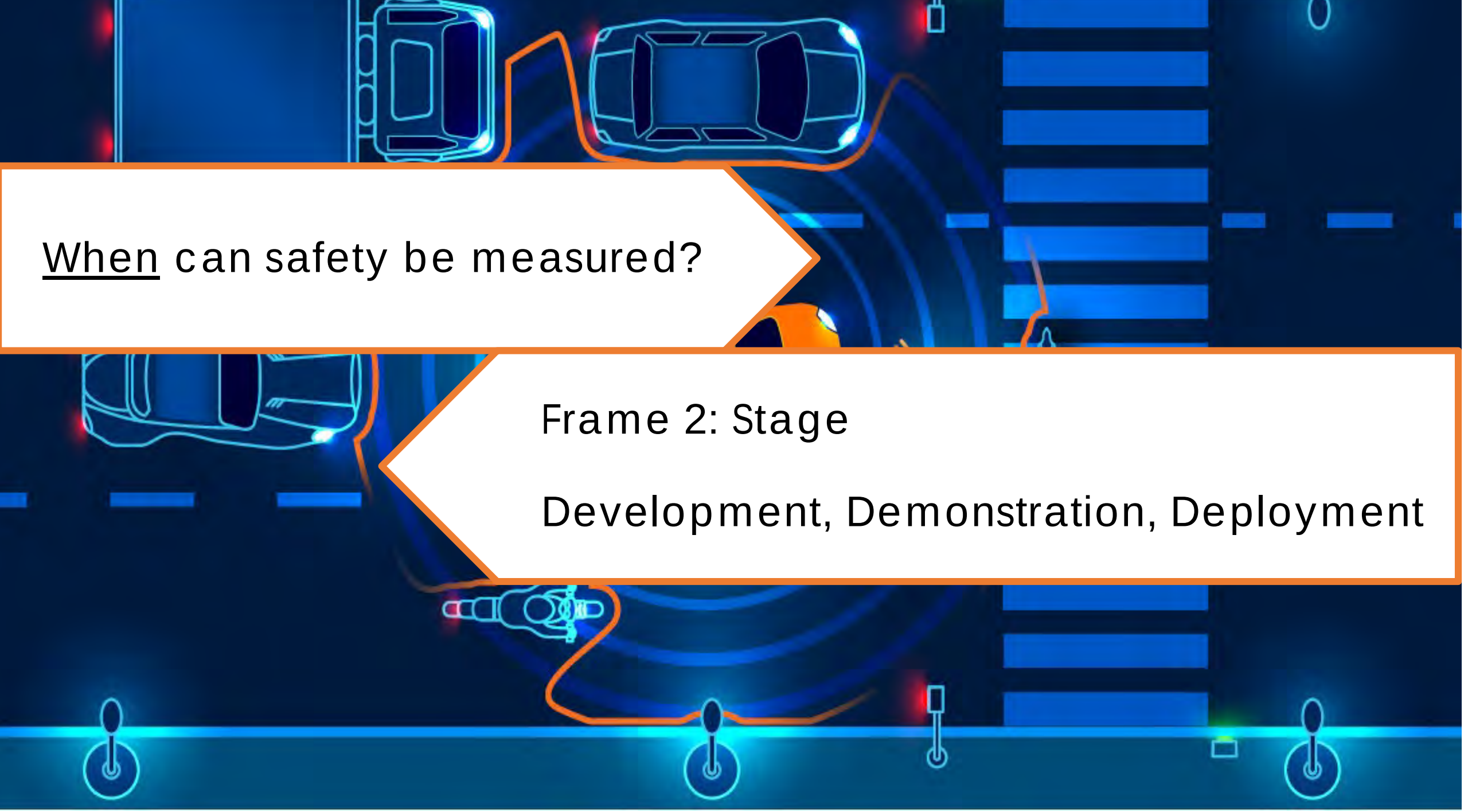
© RAND Corporation, 2019



Where can safety be measured?

Frame 1: Setting

Simulation, closed course, public roads



When can safety be measured?

Frame 2: Stage

Development, Demonstration, Deployment

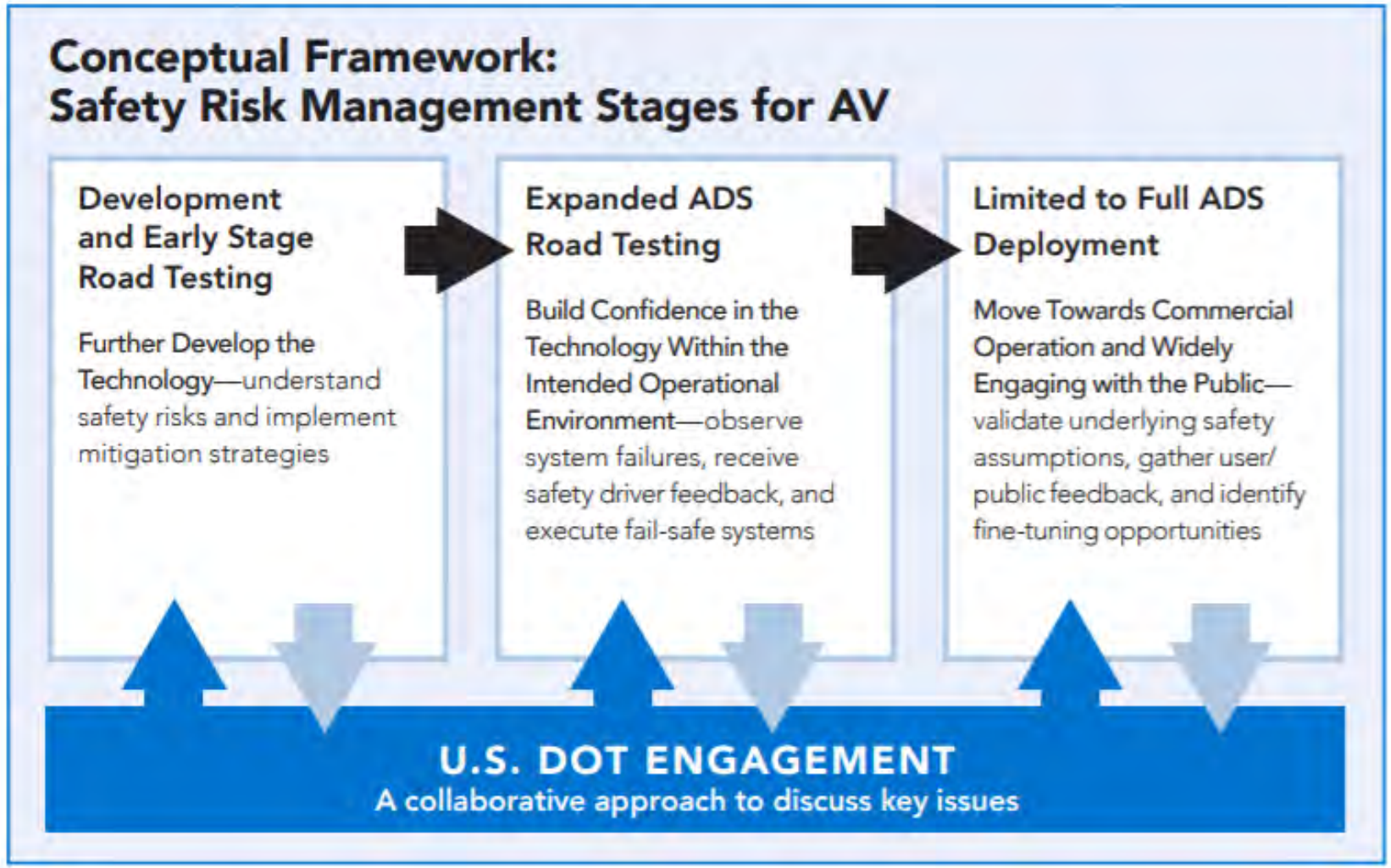
“Demonstration”

- Demonstrate the AV’s safety to policymakers and the public
  - A developer-declared period
  - Some level of oversight or transparency
  - Consistent with the stated ODD
- Verification and validation (routine) can inform
- Demonstration activities can occur in:
  - Simulation
  - Closed courses
  - Public roads, with or without a safety driver

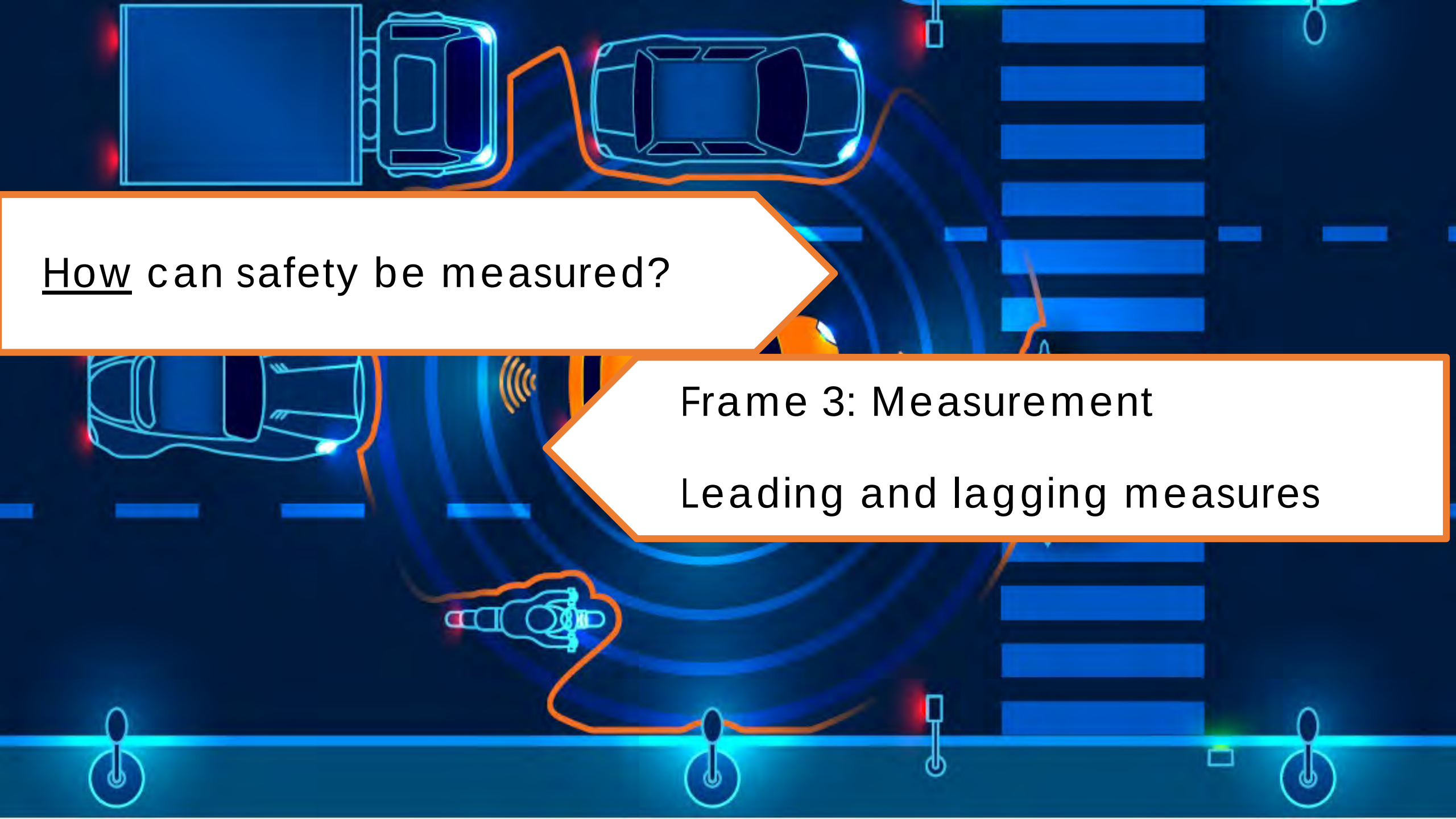
© RAND Corporation, 2019

RAND	**Development**	**Development into Demonstration**	**Demonstration Into Early Deployment**

DOT



NHTSA. Automated Vehicles 3.0: Preparing for the Future of Transportation. 2018.



<u>How</u> can safety be measured?

Frame 3: Measurement

Leading and lagging measures

Safety Frame 3: Measurement

Leading Measures

For example….

Disengagements

Infractions

Roadmanship

Lagging Measures

For example….

Crashes

Injuries

Deaths

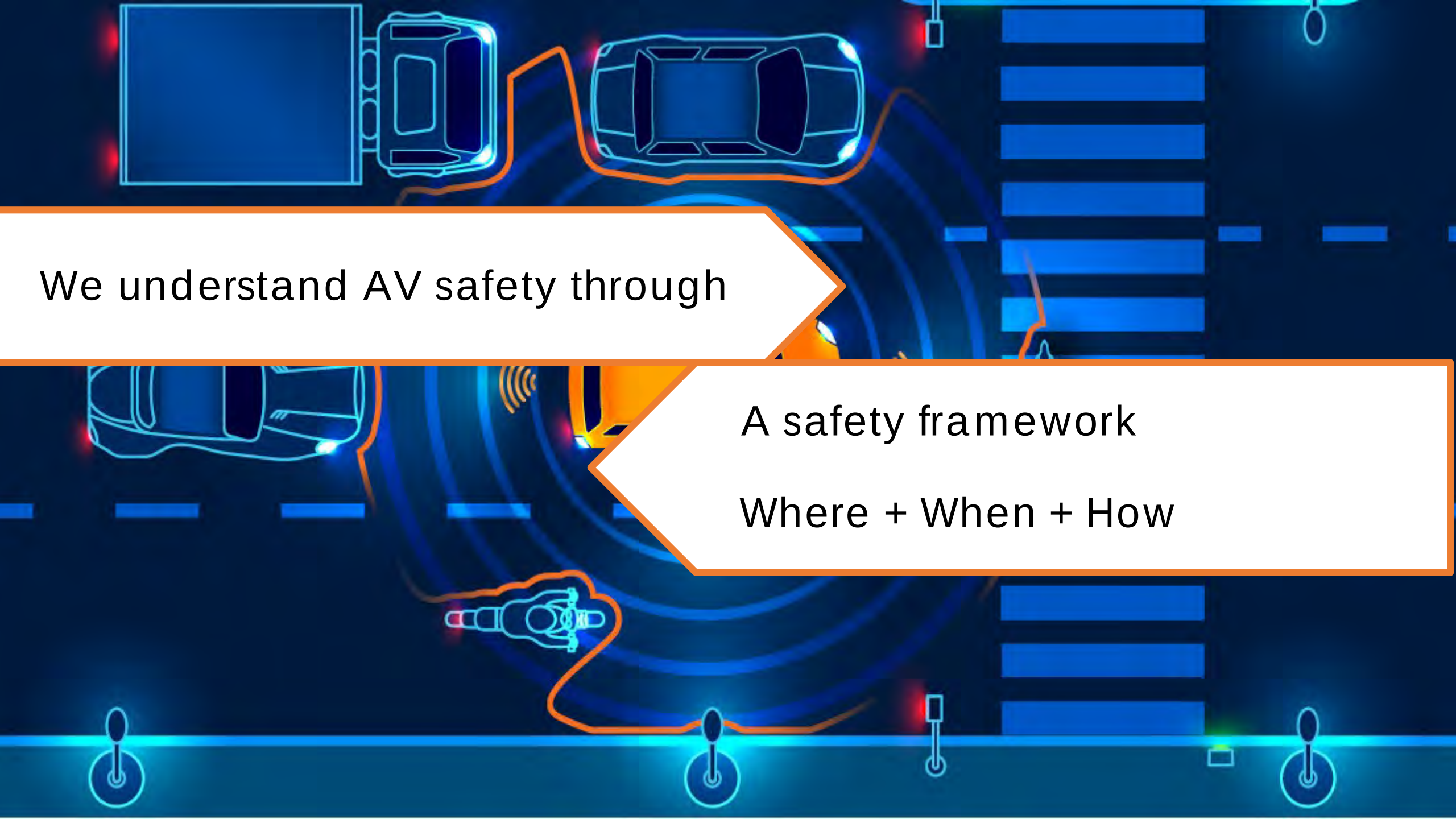
© RAND Corporation, 2019

Roadmanship

- The ability to drive on the road safely without creating hazards and responding well to the hazards created by others

- Such a measure does not currently exist
  - Safety envelope violations as an option. But how is the envelope defined?
    - Safety behavior rules comprising the Responsibility Sensitive Safety (RSS) as an option

© RAND Corporation, 2019



We understand AV safety through

A safety framework

Where + When + How

A Safety Framework

Stage	Setting	Leading measures			Lagging measures
		Infractions	Roadmanship	Disengagement+	Outcome
Development	Simulation	●	●	N/A	●
	Closed course	⊛	⊛	○	⊛
	Public roads	●	●	○	⊛
Demonstration	Simulation	●	●	N/A	●
	Closed course	⊛	⊛	⊛	⊛
	Public roads	⊛	⊛	⊛	⊛
Deployment	Simulation				
	Closed course				
	Public roads	●	●	N/A	●

Public not at risk
Public at risk
● Measure of public safety
⊛ Events that generate measures are likely informative as case-studies rather than feeding into exposure-based rates (e.g., infraction rate per 100,000 vehicle miles traveled).
○ Measure does not reflect public safety
N/A Not available

+ This column assumed that, in the closed course and public road settings, a safety driver is available (either in the vehicle or remotely). If a safety driver is not present, this entire column would be N/A.

RAND Science, Technology, and Policy Program

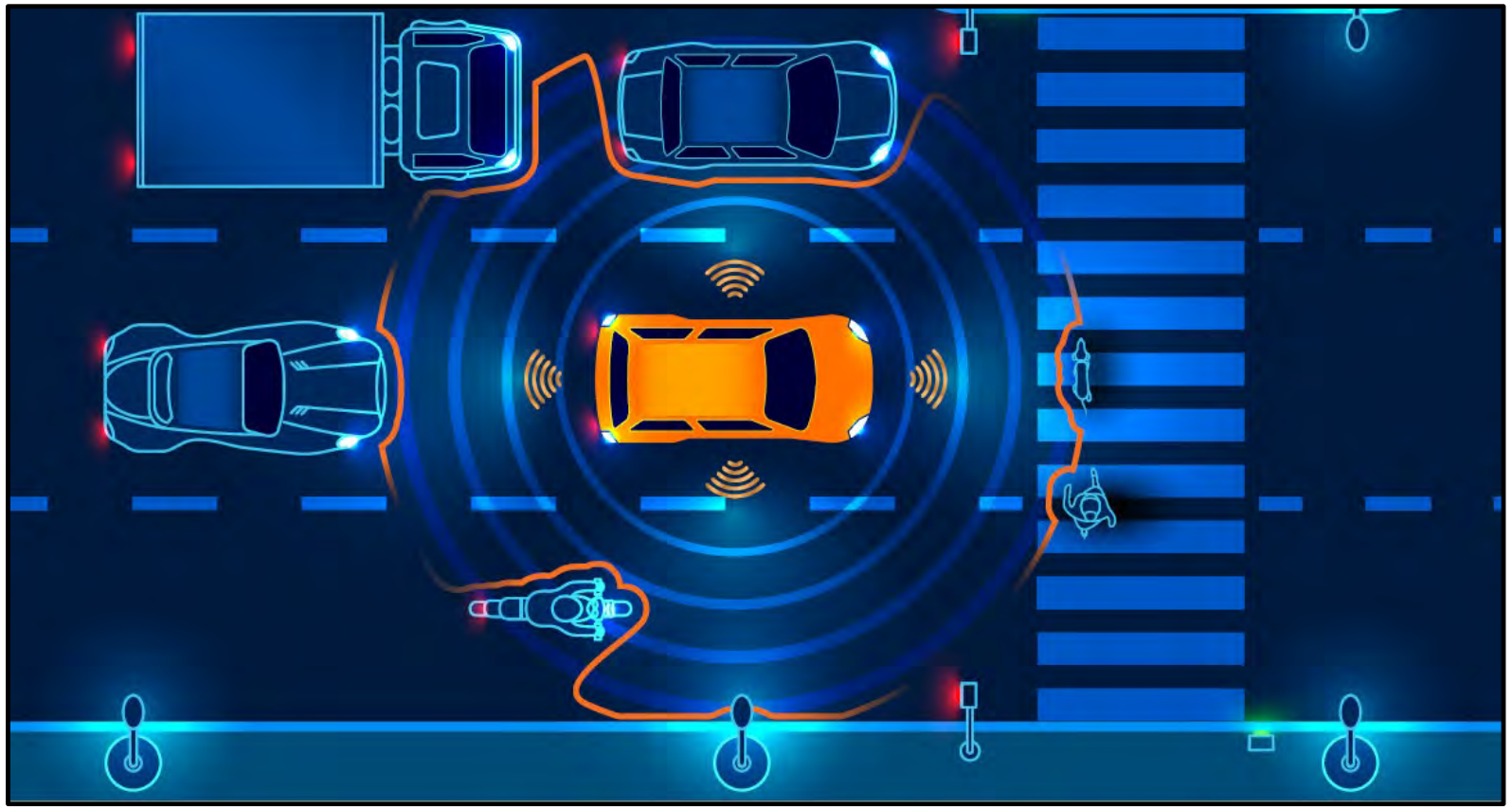
© RAND Corporation, 2019

RAND Recommendations beyond the framework

- A formal definition of roadmanship is needed
- Safety events (e.g., crashes) should be evaluated as case studies
- Protocols for information sharing should be developed and used
- A common Operational Design Domain taxonomy is needed
- A designated demonstration period can be used for benchmarking and communicating about safety
- Research is needed into how to measure and communicate AV safety in the context of frequent updates

© RAND Corporation, 2019

https://www.rand.org/pubs/research_reports/RR2662.html



Thank you

Marjory Blumenthal: marjory@rand.org
Laura Fraade-Blanar: lblanar@rand.org
James Anderson: janderso@rand.org

Lessons from the Nuclear Risk-Informed Assessments

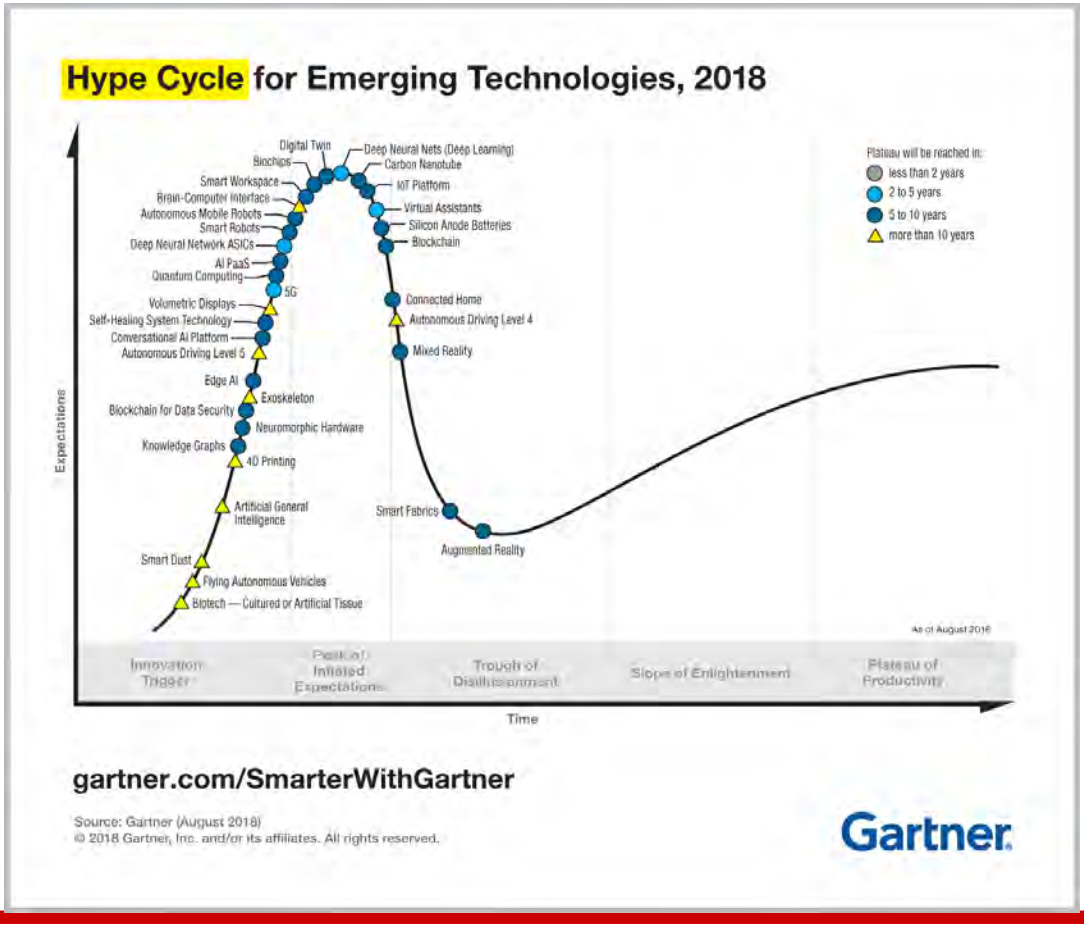
Mohammad Modarres
Center for Risk and Reliability
University of Maryland

Topics

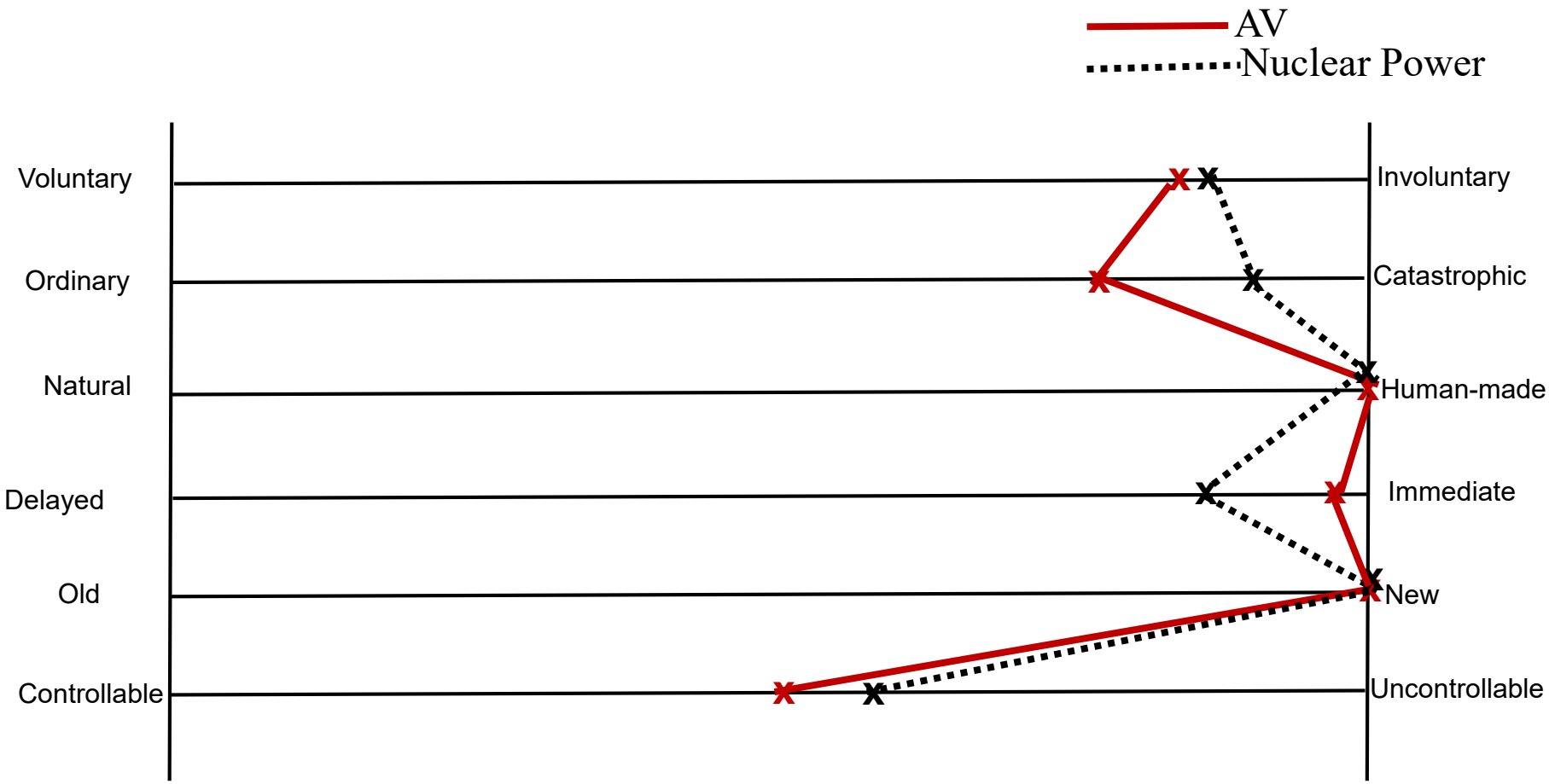
- Similarities and differences of safety and risk characteristics of AVs vs. nuclear technologies
- A quick history of safety considerations in the nuclear industry
- Emergence of "risk-informed" safety assessment
- What can we learn from nuclear safety experience
- Conclusions

Hype Cycle

- New technologies AVs and Nuclear included experience the so-called "Hype Cycle"



A Psychometric Risk Profile Comparison of Risks from AVs and Nuclear Power



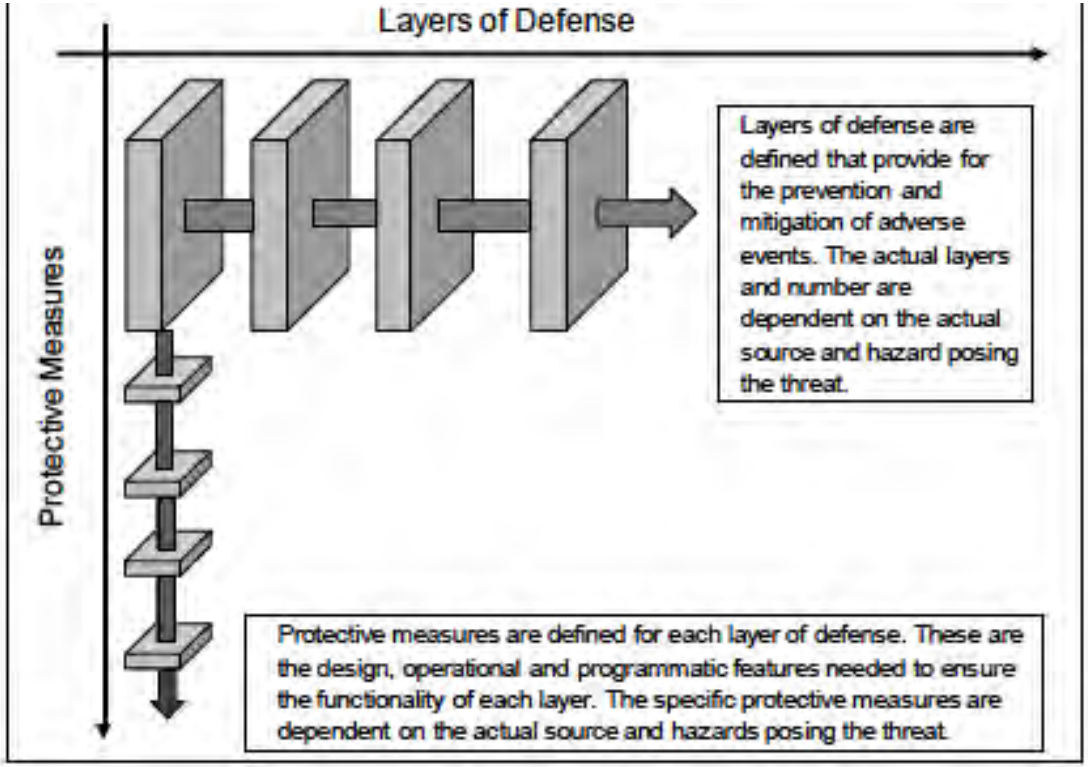
Some Nuclear Safety History

- U.S. Atomic Energy Act of 1946 rested atomic technology and military applications with Government

- U.S. Atomic Act of 1954 ended the government's monopoly and allowed peaceful uses provided that: " . . . a *reasonable assurance* exists that such uses would not result in undue risks to the health and safety of the public"

Defense-in-Depth (DiD) Became A Safety Design Principle

DiD evolved into a collection of design and operating reqirements to overcome lack of precise knowledge



NEI, Modernization of Technical Requirements, Draft 9/2018

Defense-in-Depth (Cont.)

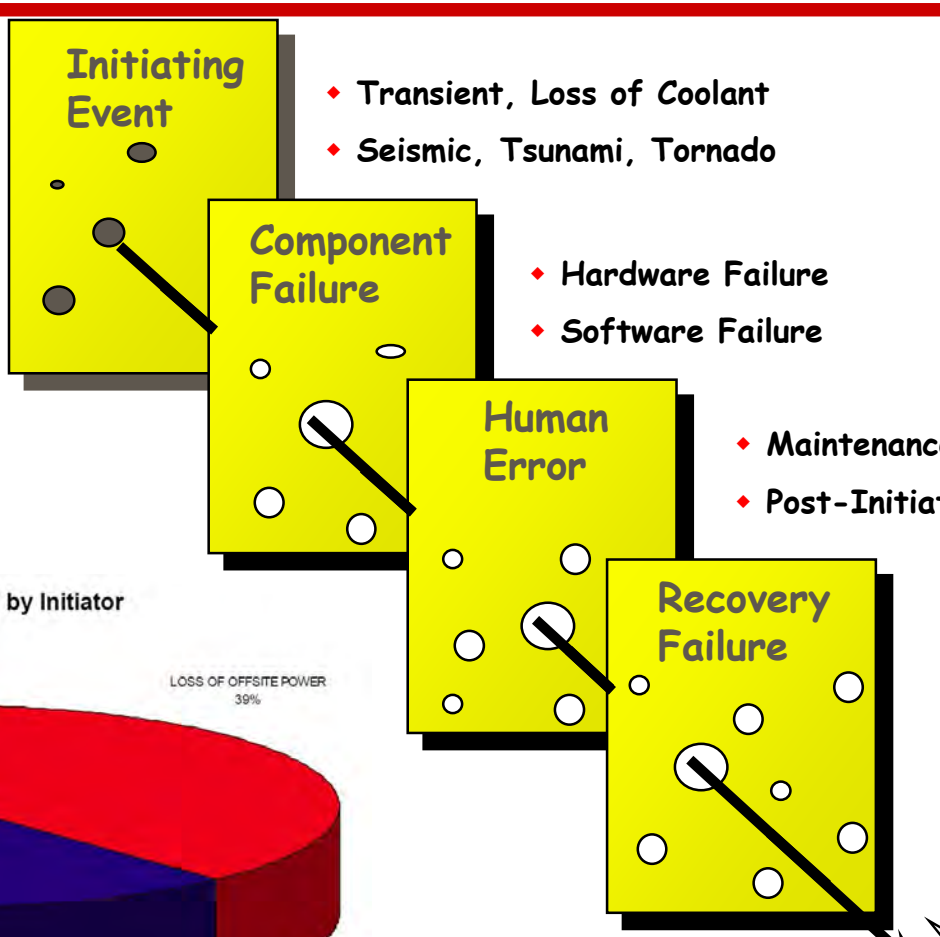
Acceptance criteria needed to measure adequacy of DiD

- Withstand a fixed set of accident scenarios *judged* by experts as most significant adverse events or the so-called "Design Basis Accidents (DBAs)"
- Assumed a plant that could handle the DBAs, it will handle any other accident
- Reasonable assurance was interpreted as conformance to the body of regulations on the basis of DiD.
- Acceptances criteria measured deterministically with conservative methods, tools and bounds

Emergence of Probabilistic Risk Assessment (PRA)

- In the mid-1960s, concerns such as containment integrity under loss of reactor coolant paved the way for use of PRA to address the shortcomings of the DBAs
- PRA was to model more realistic accident scenarios
- PRA was meant to answer: What can go wrong?, How likely is it? What are its consequences?
- The landmark WASH-1400 study commissioned by the AEC (later NRC) in 1972-1975, developed the concept, practice and realistic examples of PRA

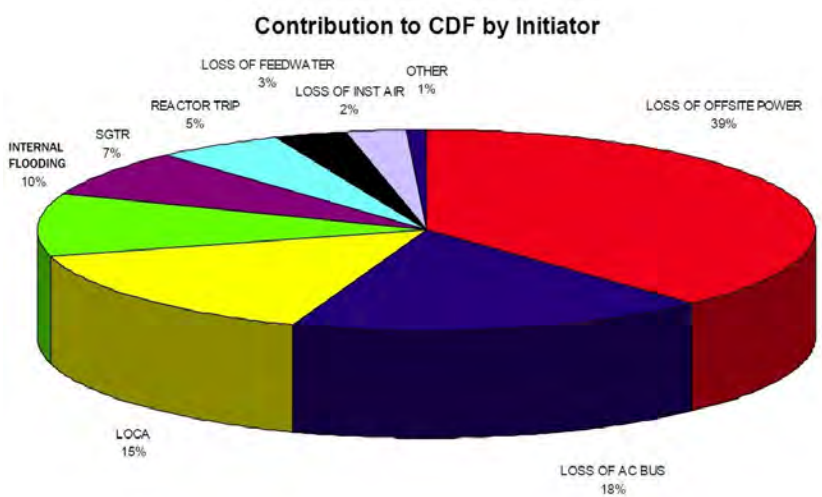
Key Elements of a PRA



- Transient, Loss of Coolant
- Seismic, Tsunami, Tornado

- Hardware Failure
- Software Failure

- Maintenance/Design Errors
- Post-Initiator Errors



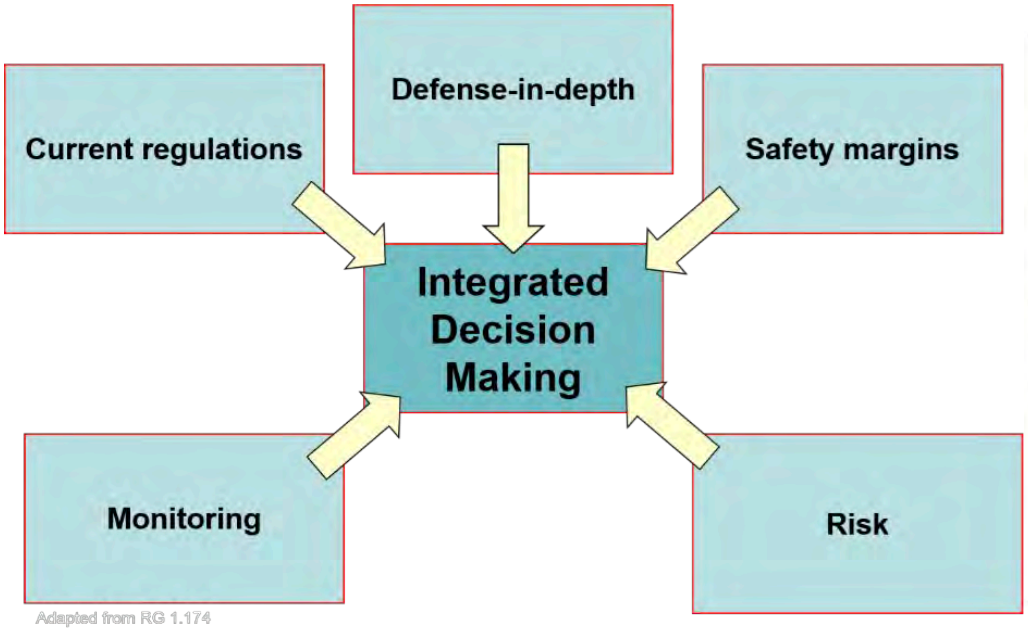
Source: Nuclear Regulatory Commission

Pre- & Post-WASH1400

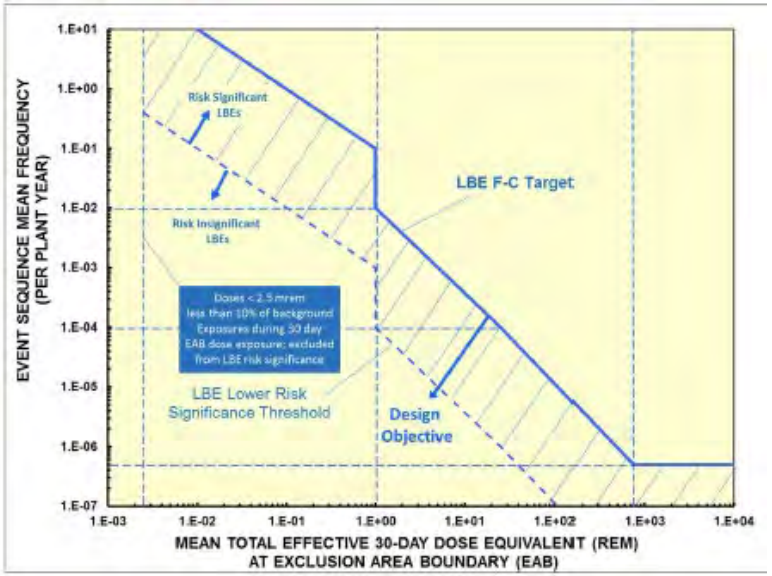
- Pre:
  - Protect again large loss of coolant
  - Core damage is unlikely < 10^{-8} per year
  - Consequences are disastrous
- Post:
  - Small loss of coolant and transients are more important
  - Core damage is more likely than believed ~5×10^{-5}
  - Consequences are significantly smaller
  - Support systems and human actions are very important
- Based on political and technical factors NRC in late 1978 withdrew its support of PRA
- TMI accident a few month later in March 1979 was consistent with WASH1400 conclusions

Risk-Informed Regulation

- NRC developed a set of qualitative safety goals and qualitative (probabilistic) safety objectives
- NRC developed a PRA Policy Statement and reformed its safety regulation to "risk-informed"



Adapted from RG 1.174



Lessons of Risk-Informed Approach that Applies to AV Safety?

- Formal PRA models can provide important realistic static and dynamic scenarios and contributors to accident risks in design and operation of AVs
- The PRA models can be updated through streams of sensor data, weather and road conditions, state of the vehicle and the entire fleet of related vehicles
- PRAs may serve in support of risk management and policy decision making to predict, avoid and mitigate road accidents
- PRA can learn by updating its risk models with near-miss events and specialize itself to a specific car, driver and region
- Data on significant near miss events can be shared among manufactures

Risk-Informed Autonomous Action

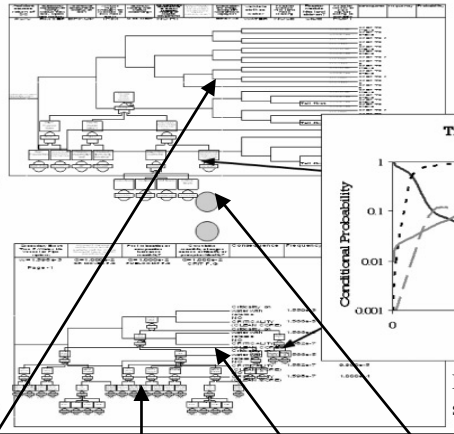
Decision Module

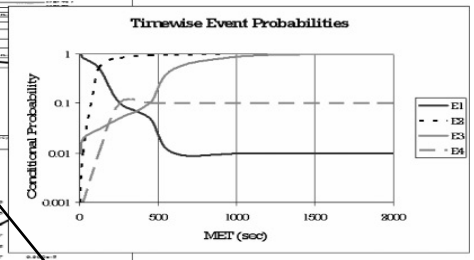
Dynamic Probabilistic Scenario Generator/Simulator

Risk-Informed Assessment Module

Policy/ Insurance Decisions

Operator Behavior Module





From: Mike Franke: quasi-dynamic PRA structure for space reactor

Analytics and Deep Learning Module

Data Processing/Filtering Module

Conclusions

- Old methods of safety analysis may be insufficient for complex technologies such as AVs
- Major accidents could prove disastrous to the vitality of the industry
- Risk-informed performance-based approaches could characterize all uncertainties including engineering ones into the operation, policy and regulation of AVs
- Risk-informed methods empower innovation and lead to better design, adequate safety features and sound policy

Thank you!

Questions?

Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions

Dr. Roger L. McCarthy, P.E.

26 April 2019

roger@mccarthyengineering.com

©McCarthy Engineering

130+ years since Karl Benz

Company History

Benz Patent Motor Car: The first automobile (1885–1886)

- The major features of the two-seater vehicle, which was completed in 1885, were the compact high-speed single-cylinder four-stroke engine installed horizontally at the rear, the tubular steel frame, the differential and three wire-spoked wheels. The engine output was 0.75 hp (0.55 kW).

https://www.daimler.com/company/tradition/company-history/1885-1886.html

©McCarthy Engineering

Greatest Engineering Achievements OF THE 20TH CENTURY

Welcome!
How many of the 20th century's greatest engineering achievements will you use today? A car? Computer? Telephone? Explore our list of the top 20 achievements and learn how engineering shaped a century and changed the world.

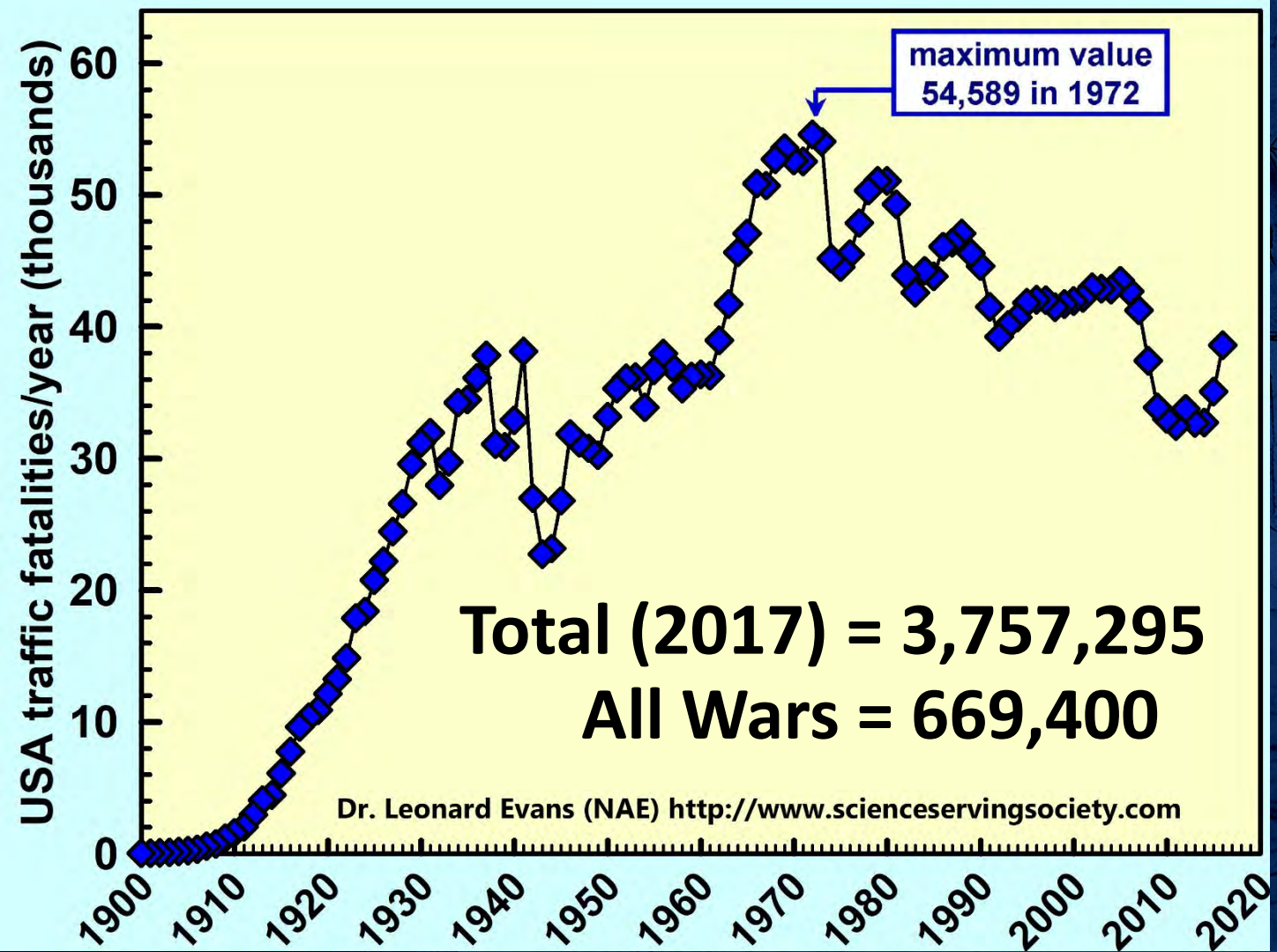
1. Electrification
2. Automobile
3. Airplane
4. Water Supply and Distribution
5. Electronics
6. Radio and Television
7. Agricultural Mechanization
8. Computers
9. Telephone
10. Air Conditioning and Refrigeration
11. Highways
12. Spacecraft
13. Internet
14. Imaging
15. Household Appliances
16. Health Technologies
17. Petroleum and Petrochemical Technologies
18. Laser and Fiber Optics
19. Nuclear Technologies
20. High-performance Materials

LinkEngineering

Greatest Achievements

http://www.greatachievements.org/

©McCarthy Engineering



During this same period we fought:

WW I = ~116K
+
WW II = ~400K
+
Korea = ~53K
+
Vietnam = ~90K
+
Gulf War = ~.4K
+
Peace (?) Keeping = ~10K

Include Disease & Accidents!

Safety promise of “self-driving”

- ~94% of the US vehicular accidents have as the “critical event” one or more “driver critical reasons,”
  - But the study did NOT define theses “reasons” as “causes”
- “Automated vehicles have the potential to save thousands of lives, driving the single biggest leap in road safety that our country has ever taken,” - U.S. Transportation Secretary Anthony Foxx
  - True, but only for the USA (and possibly China)
    - Important: US + China = ~25% world’s auto deaths
  - Because the US is so far behind the rest of the world
- NHTSA issued (9/2016) a “Federal Policy for safe testing and deployment of automated vehicles”

©McCarthy Engineering

Not all “self-driving” is equal

- Formal taxonomy of autonomous vehicle operation created (2014) by the US Society of Automotive Engineers: SAE International's J3016-201609
- Adopted by the US NHTSA (10/2016)
- Also note “Guidelines for Safe On-Road Testing of SAE Level 3, 4, and 5 Prototype Automated Driving Systems (ADS)” (SAE J3018_201503)

©McCarthy Engineering

Level	Name	Narrative definition	DDT: Sustained lateral and longitudinal vehicle motion control	DDT: OEDR	DDT fallback	ODD
Driver performs part or all of the *DDT* [Dynamic Driving Task]						
0	No Driving Automation	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*Driver*	*Driver*	n/a
1	Driver Assistance	The *sustained* and *ODD*-specific execution by a *driving automation system* of either the *lateral* or the *longitudinal vehicle motion control* subtask of the DDT (but not both simultaneously) with the expectation that the *driver* performs the remainder of the *DDT*.	*Driver* and *System*	*Driver*	*Driver*	Limited
2	Partial Driving Automation	The *sustained* and *ODD*-specific execution by a *driving automation system* of both the *lateral* and *longitudinal vehicle motion control* subtasks of the *DDT* with the expectation that the *driver* completes the *OEDR* subtask and *supervises* the *driving automation system*.	***System***	*Driver*	*Driver*	Limited
ADS ("*System*") performs the entire *DDT* (while engaged)						
3	Conditional Driving Automation	The *sustained* and *ODD*-specific performance by an *ADS* of the entire DDT with the expectation that the *DDT fallback-ready user* is *receptive* to *ADS*-issued *requests to intervene*, as well as to *DDT performance-relevant system failures* in other *vehicle* systems, and will respond appropriately.	*System*	***System***	*Fallback-ready user (becomes the driver during fallback)*	Limited
4	High Driving Automation	The *sustained* and *ODD*-specific performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	***System***	Limited
5	Full Driving Automation	The *sustained* and unconditional (i.e., not *ODD*-specific) performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	**Unlimited**

"self-driving" SAE J3016_201609 categories

Tesla 2019/04*

*https://techcrunch.com/2019/04/22/tesla-autonomy-day-is-here-heres-how-to-watch/, https://gearpatrol.com/2019/02/26/the-state-of-autonomous-driving-in-2019-what-to-know/

Google 2017**

**https://www.thedrive.com/tech/15848/waymo-is-already-running-cars-with-no-one-behind-the-wheel

Levels of Autonomy

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) AUTOMATION LEVELS

Full Automation

0	1	2	3	4	5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Source: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

California was the first state with autonomous vehicle testing regulations

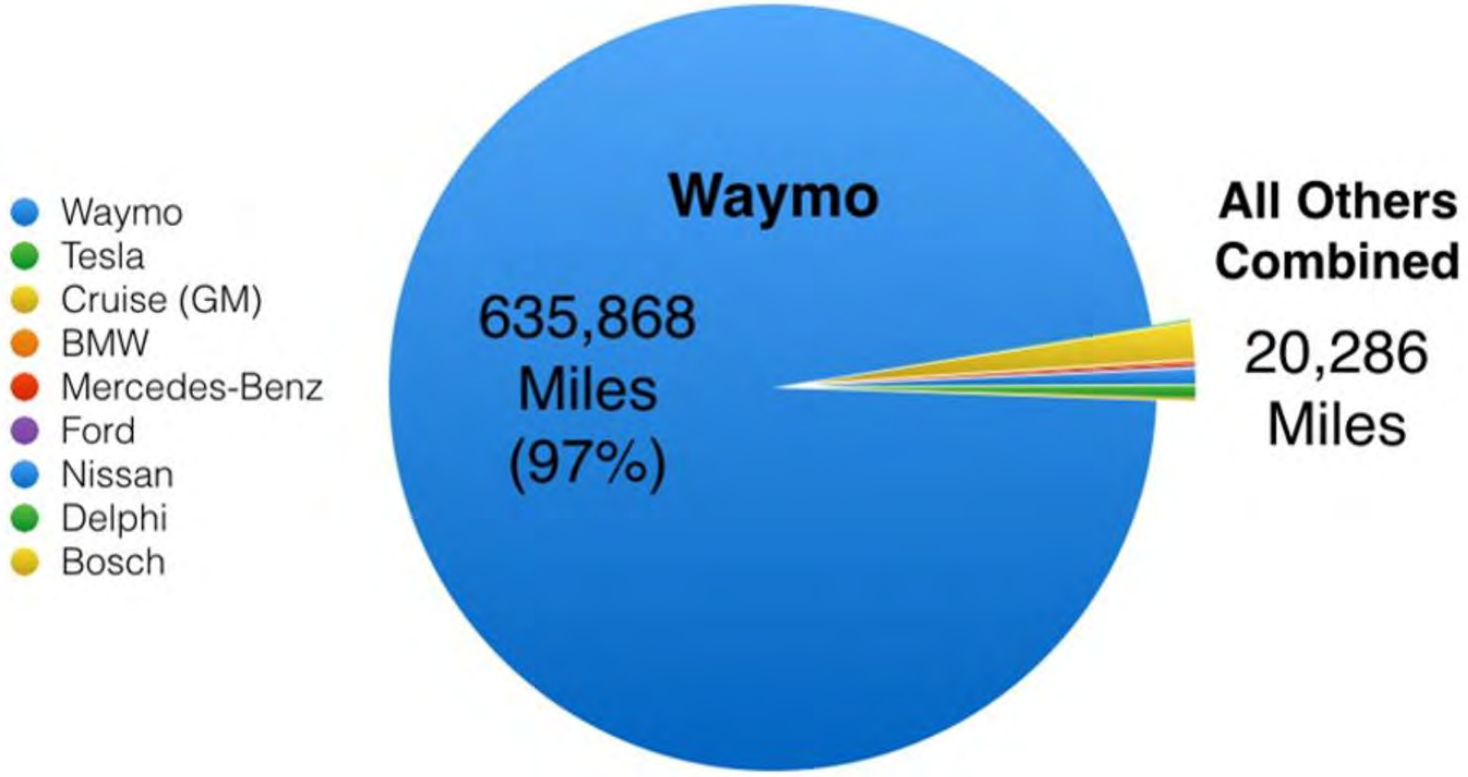
- Title 13, Division 1, Chapter 1
  - Article 3.7 – Testing of Autonomous Vehicles
- The autonomous vehicles testing regulations, which require a driver, were effective on September 16, 2014.
- Required every autonomous mile, accident, and disengagement to be reported

©McCarthy Engineering

CA regulation

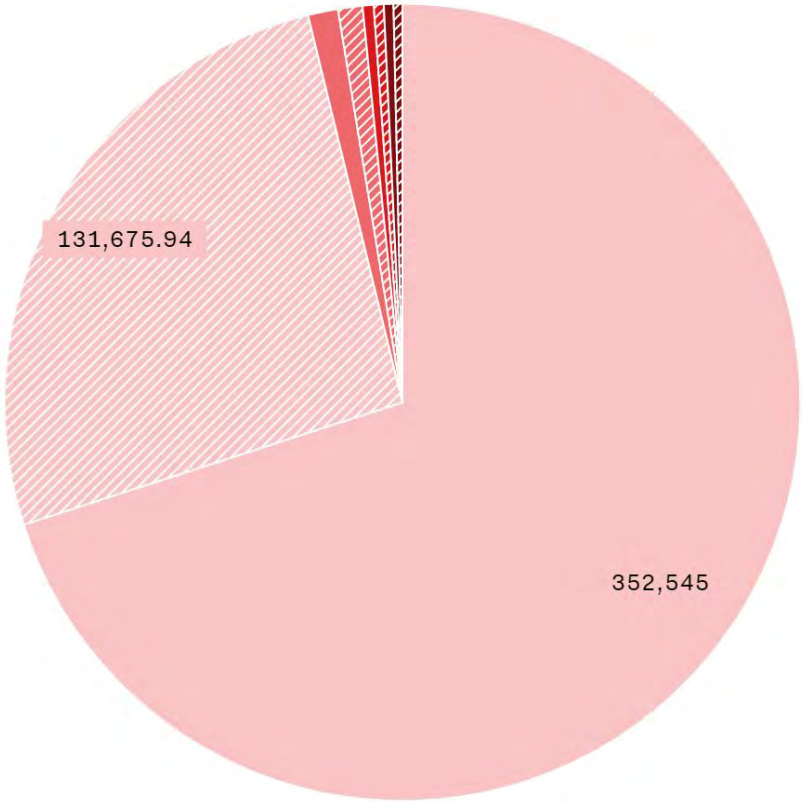
- § 227.02. Definitions
- (a) “Autonomous mode” is the status of vehicle operation where technology that is a combination of hardware and software, remote and/or on-board, performs the dynamic driving task, with or without a natural person actively supervising the autonomous technology’s performance of the dynamic driving task. An autonomous vehicle is operating or driving in autonomous mode when it is operated or driven with the autonomous technology engaged.
- (b) “Autonomous test vehicle” is a vehicle that has been equipped with technology that is a combination of both hardware and software that, when engaged, performs the dynamic driving task, but requires a human test driver or a remote operator to continuously supervise the vehicle’s performance of the dynamic driving task.
  - (1) An autonomous test vehicle does not include vehicles equipped with one or more systems that provide driver assistance and/or enhance safety benefits but are not capable of, singularly or in combination, performing the dynamic driving task on a sustained basis without the constant control or active monitoring of a natural person.
  - (2) For the purposes of this article, an “autonomous test vehicle” is equipped with technology that makes it capable of operation that meets the definition of Levels 3, 4, or 5 of the SAE International’s Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, standard J3016 (SEP2016), which is hereby incorporated by reference

©McCarthy Engineering

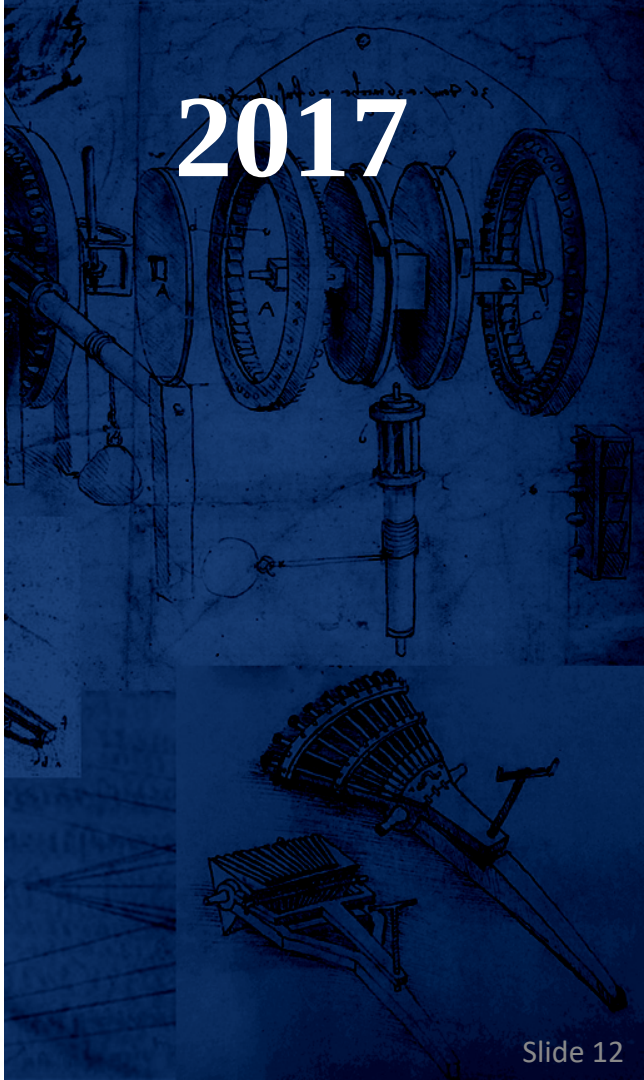


Autonomous Miles on California Public Roads in 2016

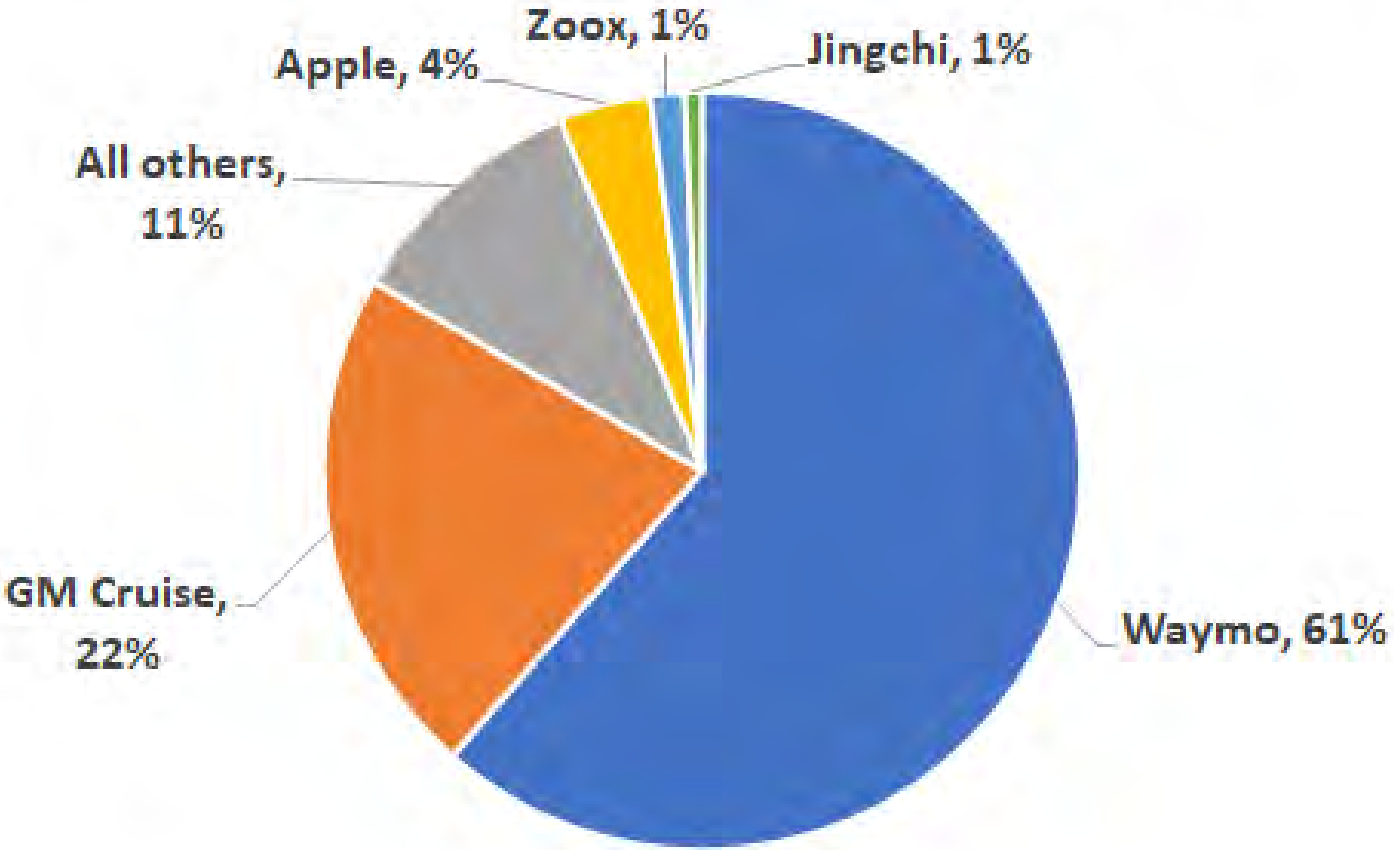
AUTONOMOUS MILES DRIVEN IN CALIFORNIA FROM 12/16-11/17

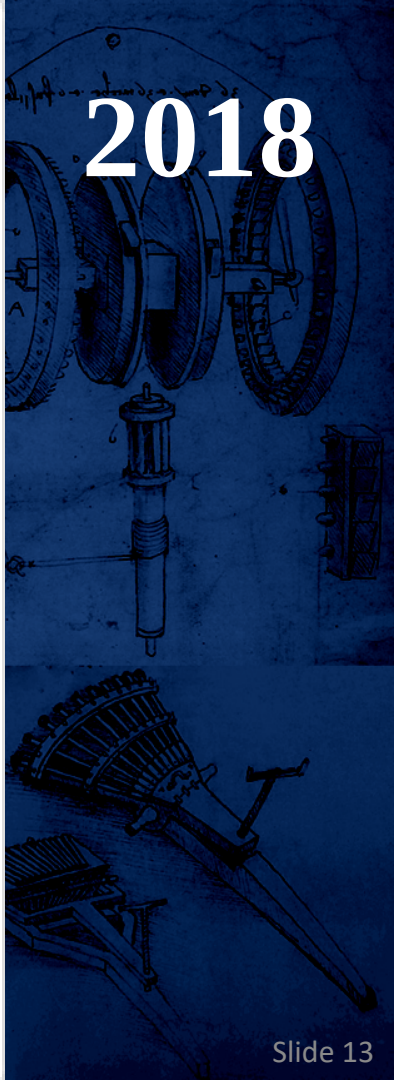


Waymo GM/Cruise Drive.ai Nissan Zoox Bosch Baidu Aptiv

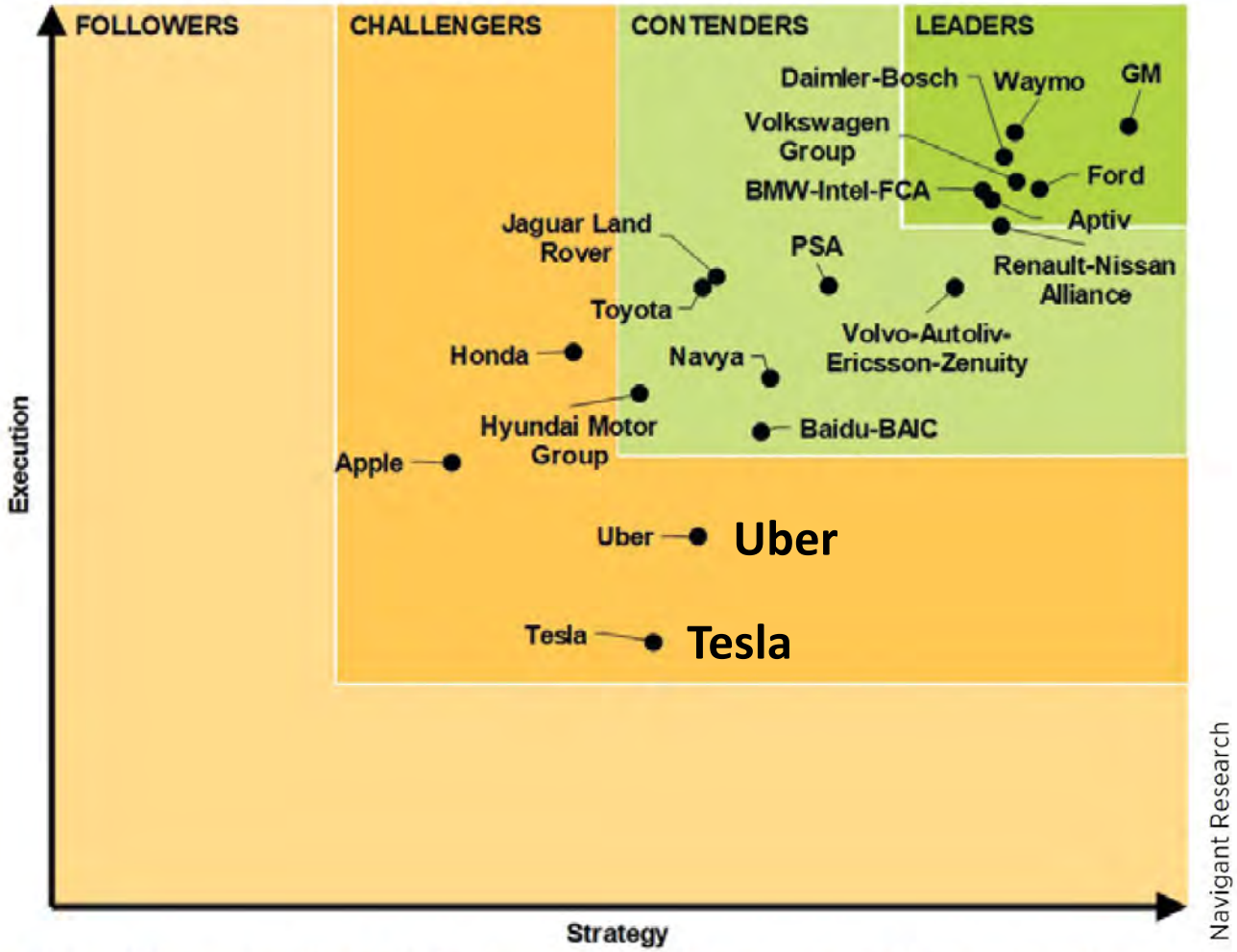


2018: 2.05 MIllion California Autonomous Miles





©McCarthy Engineering

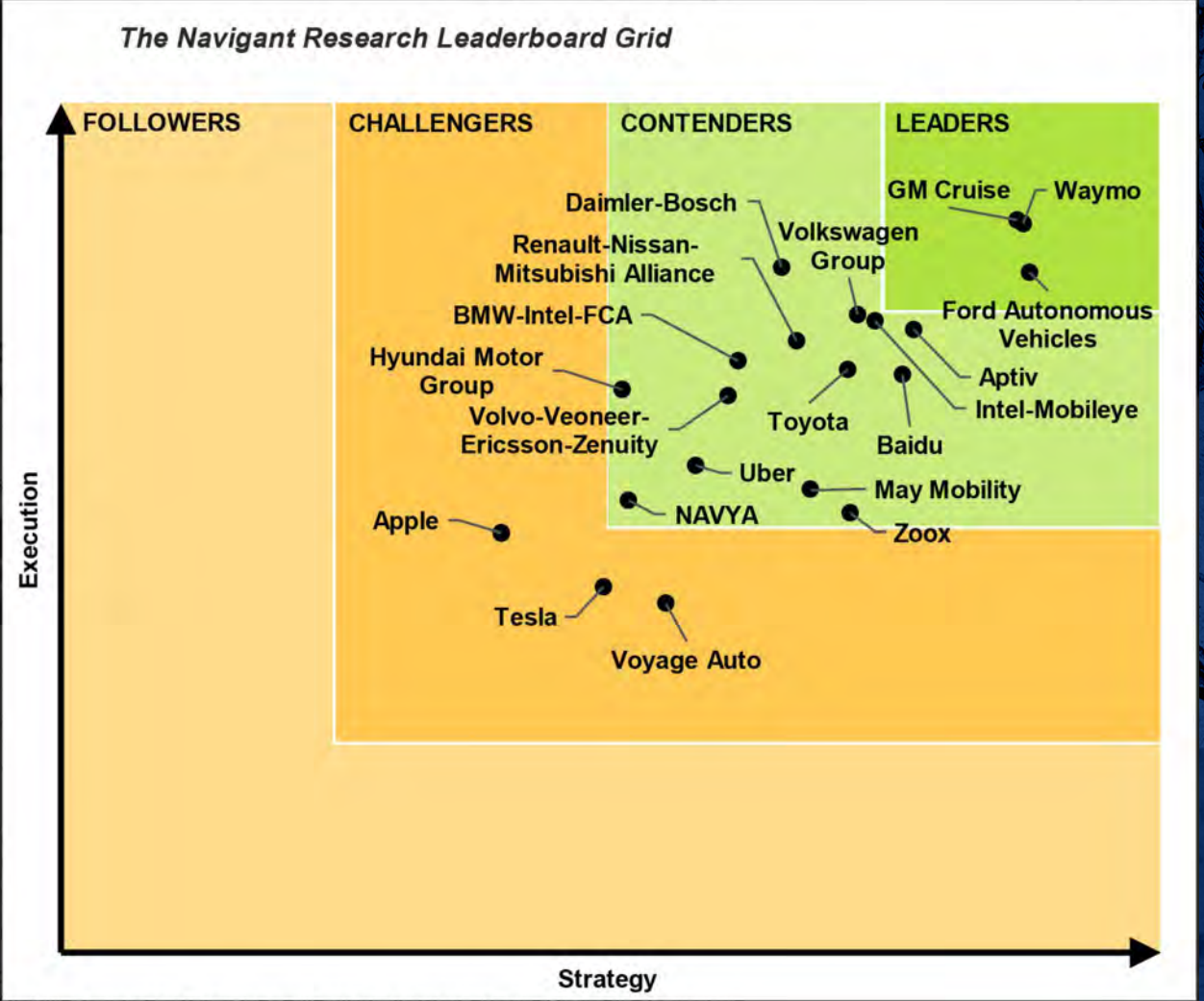


GM and Waymo top the 2018 Navigant Research Automated Driving Leaderboard.

2017

Navigant is a billion Dollar technology Consulting firm with Approximately 5,000+ Employees headquartered In Chicago

From article in March 2018 SAE Journal Autonomous Vehicle Engineering



Navigant Research's 2019 automated driving leaderboard. *(Navigant)*

2018

Google California autonomous record

Table 5

Crash and injury rates for conventional vehicles and self-driving vehicles.

Vehicle type	Rates per million vehicle miles of travel			Injuries per crash
	Crashes	Injuries (nonfatal)	Fatalities	
Conventional vehicles	1.9 **(4.1*)**	0.77	0.01	0.41
Self-driving vehicles	9.1	3.29	0	0.36

Google/Waymo 2016 CA **12.6** 8/.635868* (12/15-11/16)

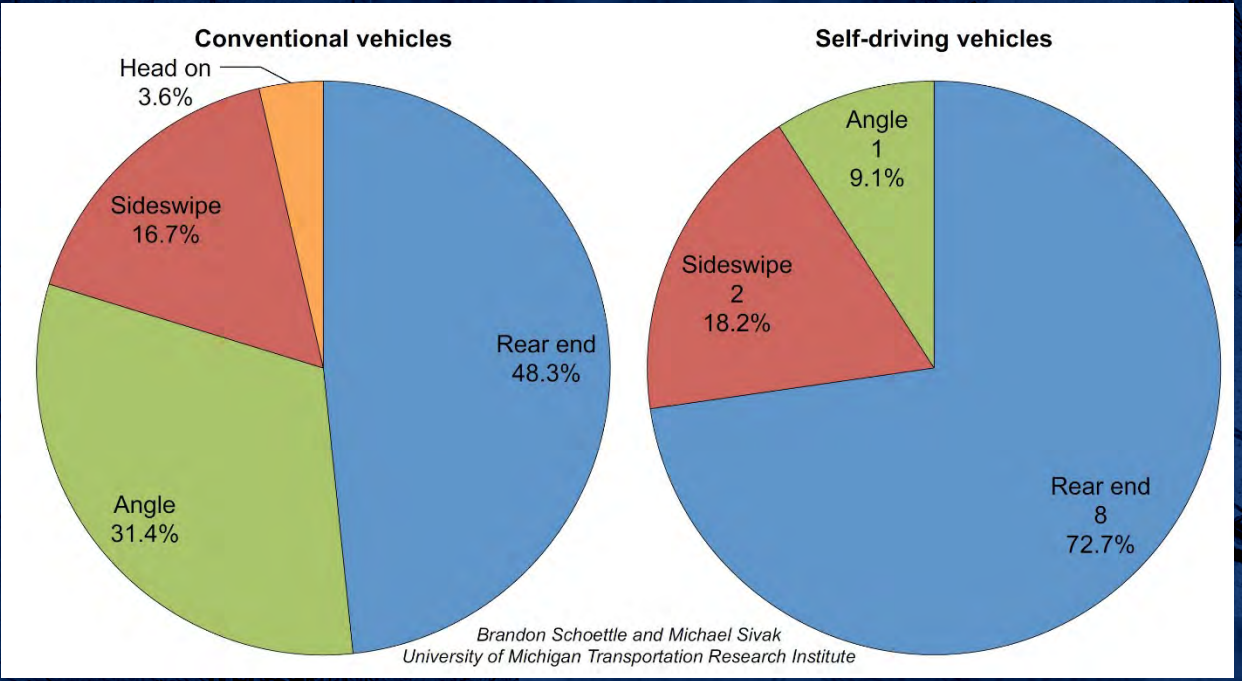
The 2016 crash rate for Google/Waymo was 3X the adjusted* (for under reporting) crash rate of conventional vehicles

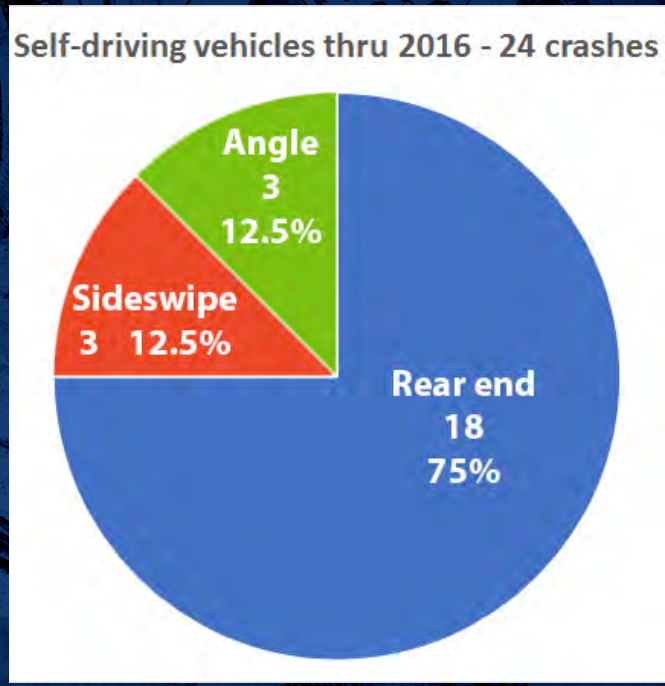
Table 5 from: UMTRI-2015-34, pg. 11

* https://www.dmv.ca.gov/portal/wcm/connect/946b3502-c959-4e3b-b119-91319c27788f/GoogleAutoWaymo_disengage_report_2016.pdf?MOD=AJPERES

©McCurdy Engineering

California self-driving accidents 2015-16

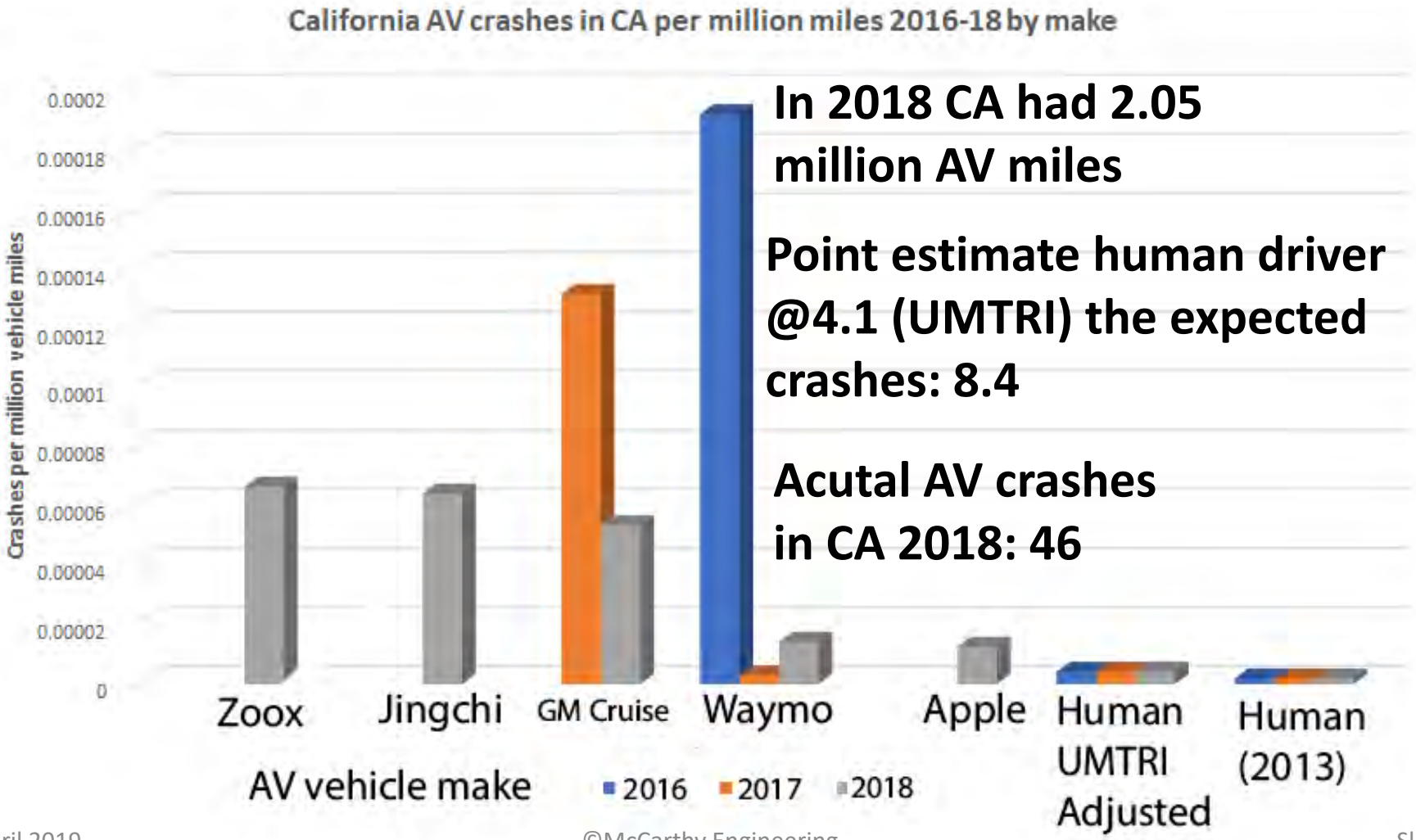




from UMTRI-2015-34, pg. 9

Based on 11 crashes

©McCarthy Engineering



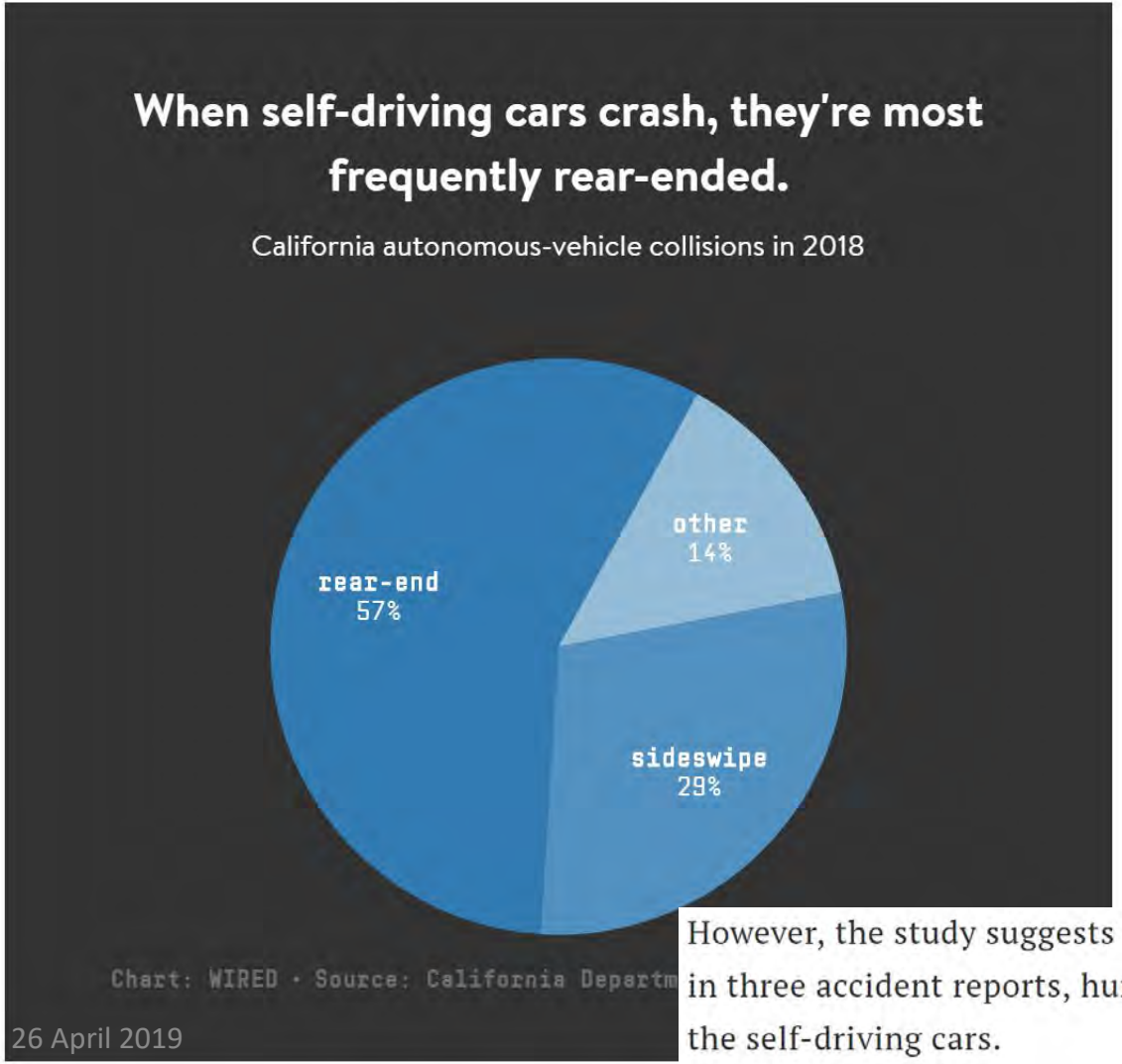
In 2018 CA had 2.05 million AV miles

Point estimate human driver @4.1 (UMTRI) the expected crashes: 8.4

Acutal AV crashes in CA 2018: 46

©McCarthy Engineering

Unexpected AV behavior results in read end collisions

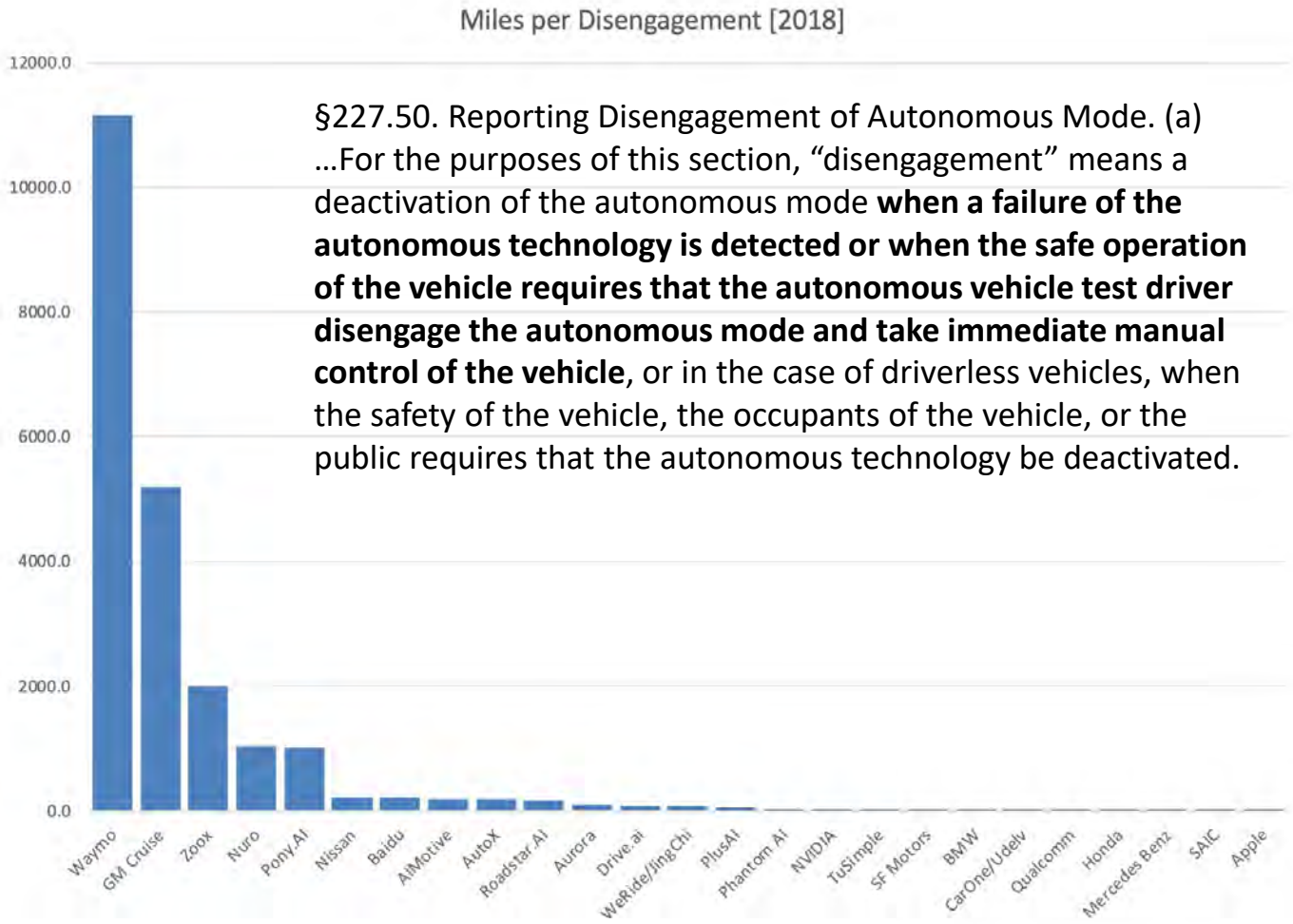


However, the study suggests that humans are still the biggest problem. In fact, in three accident reports, humans were found to have attacked or climbed atop the self-driving cars.

Why do autonomous vehicles have more crashes?

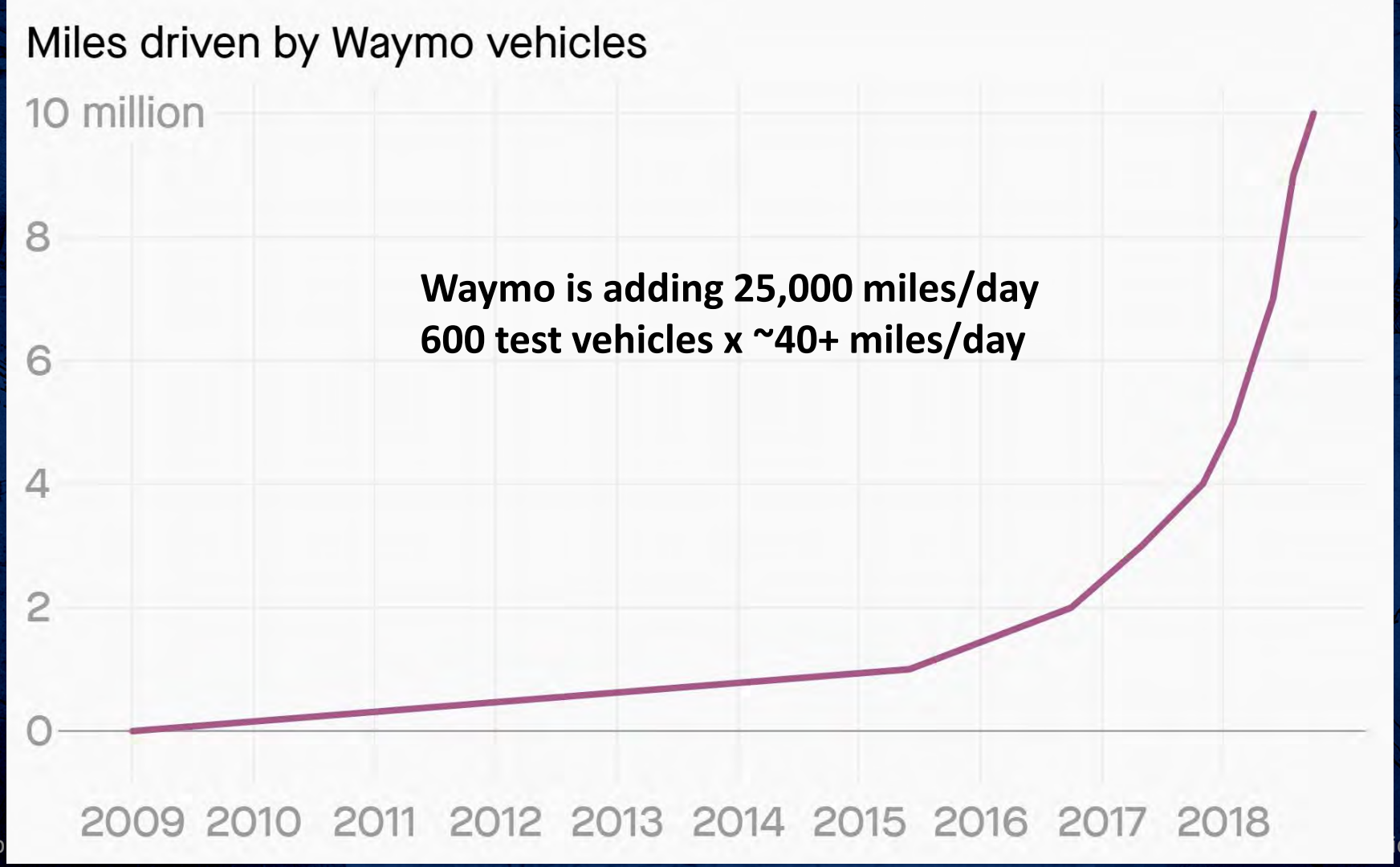
- Particularly when virtually all the crashes are the fault of the other driver
- Most of the autonomous vehicle accidents are being struck from the rear by a following vehicle
- Whose driver had not properly anticipated the conservatism of the autonomous vehicle's slow operation.
- Regulators need to be prepared to see dramatically high reported crash rates in the autonomous vehicle fleets

©McCarthy Engineering



§227.50. Reporting Disengagement of Autonomous Mode. (a) …For the purposes of this section, "disengagement" means a deactivation of the autonomous mode **when a failure of the autonomous technology is detected or when the safe operation of the vehicle requires that the autonomous vehicle test driver disengage the autonomous mode and take immediate manual control of the vehicle**, or in the case of driverless vehicles, when the safety of the vehicle, the occupants of the vehicle, or the public requires that the autonomous technology be deactivated.

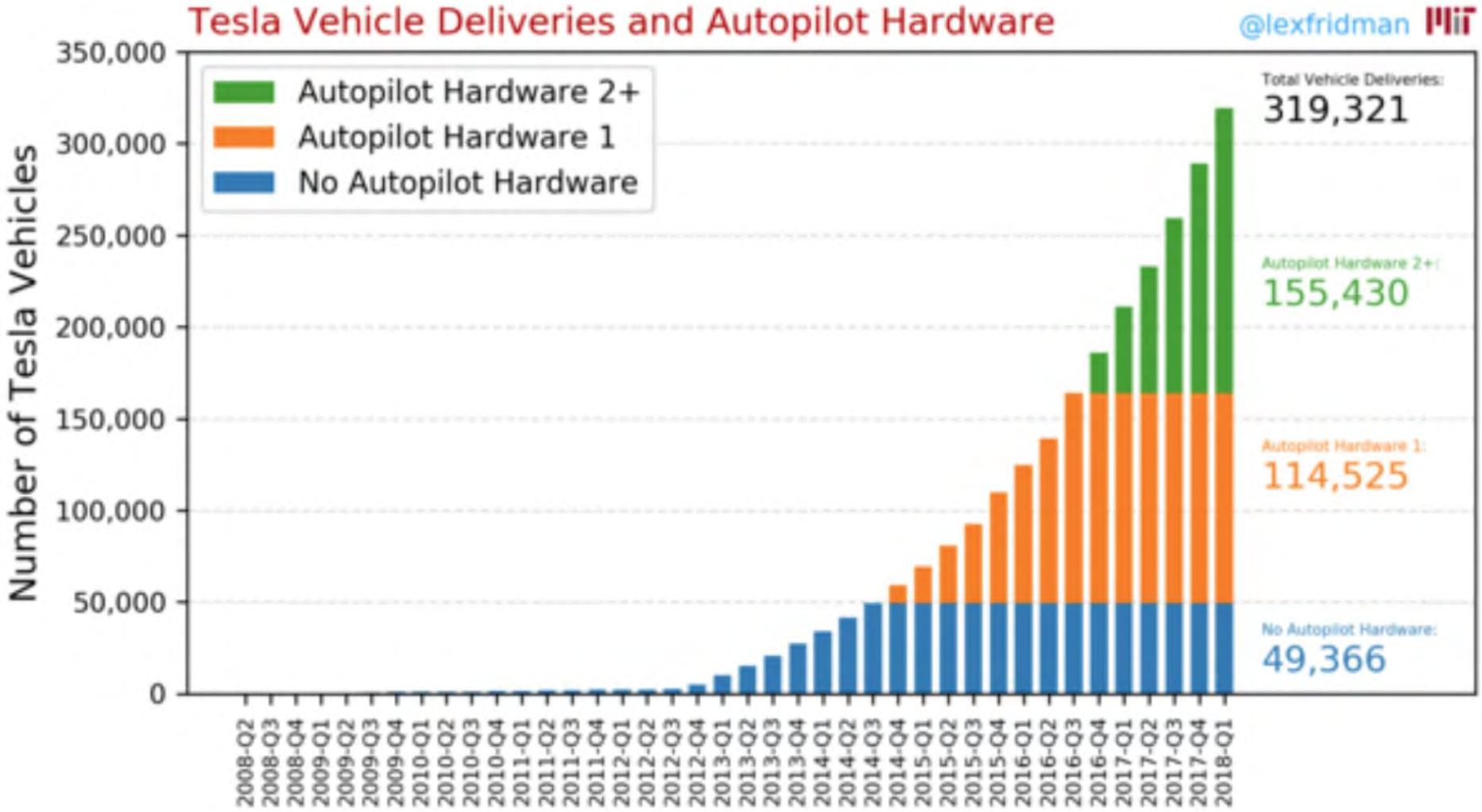
Miles per disengagement or the period between December 2017 and November 2018

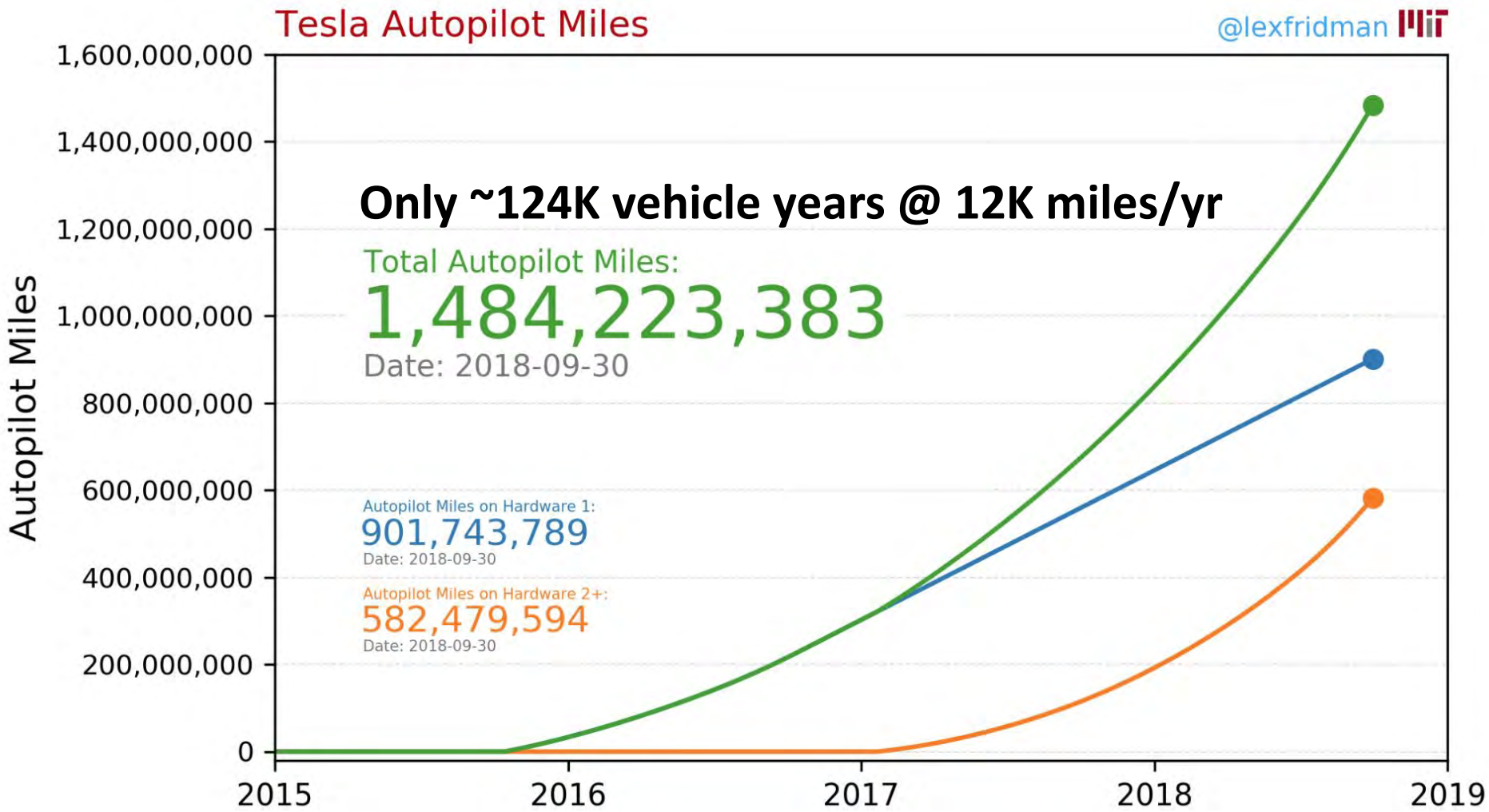

Miles driven by Waymo vehicles
10 million
8
6
4
2
0
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
Waymo is adding 25,000 miles/day
600 test vehicles x ~40+ miles/day

Tesla “autopilot”

- Tesla rolled out it “autopilot” feature in 14 October 2015
- The “autopilot” mode of the current Tesla vehicles is only level 2 “self-driving”
  - not classed as an “autonomous” vehicle
  - Otherwise Telsa would have to report in CA
- BUT - there are now probably ~350,000 Tesla’s with some “auto pilot” capability and probably less than a thousand truly autonomous vehicles
- Much larger Tesla fleet might permit the detection of an incremental change in crash risk from incremental change of vehicle automation

©McCarthy Engineering


Tesla Vehicle Deliveries and Autopilot Hardware
@lexfridman
Autopilot Hardware 2+
Autopilot Hardware 1
No Autopilot Hardware
Total Vehicle Deliveries:
319,321
Autopilot Hardware 2+:
155,430
Autopilot Hardware 1:
114,525
No Autopilot Hardware:
49,366
Number of Tesla Vehicles
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
2008-Q2
2008-Q3
2008-Q4
2009-Q1
2009-Q2
2009-Q3
2009-Q4
2010-Q1
2010-Q2
2010-Q3
2010-Q4
2011-Q1
2011-Q2
2011-Q3
2011-Q4
2012-Q1
2012-Q2
2012-Q3
2012-Q4
2013-Q1
2013-Q2
2013-Q3
2013-Q4
2014-Q1
2014-Q2
2014-Q3
2014-Q4
2015-Q1
2015-Q2
2015-Q3
2015-Q4
2016-Q1
2016-Q2
2016-Q3
2016-Q4
2017-Q1
2017-Q2
2017-Q3
2017-Q4
2018-Q1


Tesla Autopilot Miles
@lexfridman
MIT
Only ~124K vehicle years @ 12K miles/yr
Total Autopilot Miles:
1,484,223,383
Date: 2018-09-30
Autopilot Miles on Hardware 1:
901,743,789
Date: 2018-09-30
Autopilot Miles on Hardware 2+:
582,479,594
Date: 2018-09-30
Autopilot Miles
1,600,000,000
1,400,000,000
1,200,000,000
1,000,000,000
800,000,000
600,000,000
400,000,000
200,000,000
0
2015
2016
2017
2018
2019

Tesla “autopilot”

- Tesla has great connected intelligence, data capture, and Internet capabilities on the vehicle
- In May 2017 Tesla warned owners that unless they “opt out” their Tesla will start sending short anonymous video clips of their driving to the manufacturer
- Internet connection notifies Tesla of crash events with airbag deployment
- As well as how many miles are being driven
- Tesla knows more about its vehicle fleet experience than any other manufacturer.

©McCarthy Engineering

Tesla “autopilot”

- The currently available Tesla autopilot crash data is not promising
  - contrary to the “hype” of the manufacturer
- First known “autonomous” driving US fatality in May of 2016
- “Unable to distinguish the white truck against the brightly lit sky, the self-driving system failed to apply the brakes.”
- Tesla accident experience made public in the safety investigation by the NHTSA

©McCarthy Engineering

“Tesla team” statements

- **In response to 7 May 2016 fatal crash of Joshua Brown whose Tesla Model S drove into the side of a tractor trailer in the “autopilot” mode**
- “We learned yesterday evening that NHTSA is opening a preliminary evaluation into the performance of Autopilot during a recent fatal crash that occurred in a Model S. This is the first known fatality in just over 130 million miles where Autopilot was activated.”*
- *https://www.tesla.com/blog/tragic-loss?utm_campaign=Blog_063016&utm_source=Twitter&utm_medium=social

©McCarthy Engineering

NHTSA investigation of Brown Crash

- AFTER PROBING TESLA'S DEADLY CRASH, FEDS SAY YAY TO SELF-DRIVING (Headline of "WIRED" magazine)*
- "A safety-related defect trend has not been identified at this time and further examination of this issue does not appear to be warranted"
- " the agency exculpated Tesla, and then some. It crunched the numbers to find that among Tesla cars on the road, those carrying its Autosteer technology, which can keep the car within clear lane markings, crashed 40 percent less frequently than those without."
- **Not quite true. Tesla crunched that number, and the NHTSA didn't endorse it, but quoted it, and the damage was done.**

*https://www.wired.com/2017/01/probing-teslas-deadly-crash-feds-say-yay-self-driving/

©McCarthy Engineering

Tesla “autopilot”

After the fatal crash Elon Musk made numerous claims about Tesla safety: “Indeed, if anyone bothered to do the math (obviously, you did not) they would realize that of the over 1M auto deaths per year worldwide, approximately half a million people would have been saved if the Tesla autopilot was universally available. Please, take 5 mins and do the bloody math before you write an article that misleads the public.”

©McCarthy Engineering

Tesla “autopilot”

- Tesla rolled out it “autopilot” feature in 14 October 2015
- Two months later there was fatal Tesla S crash on 20 January 2016 involving Gao Yaning in Handan, China while using the “autopilot” feature
- The Tesla S traveling at full speed exhibited no braking or evasion slammed into the back of a slow moving, large orange street sweeper partially in the high-speed left lane
- In an emailed statement, Tesla said… it had not been able to determine whether Autopilot was active at the time of the Handan accident
- “The company declined to say when it learned of the fatality in China, or whether it had reported the crash to United States safety officials”

©McCarthy Engineering

January 2016 Fatal Tesla “autopilot” crash in China

EVENTUALLY Tesla owns up

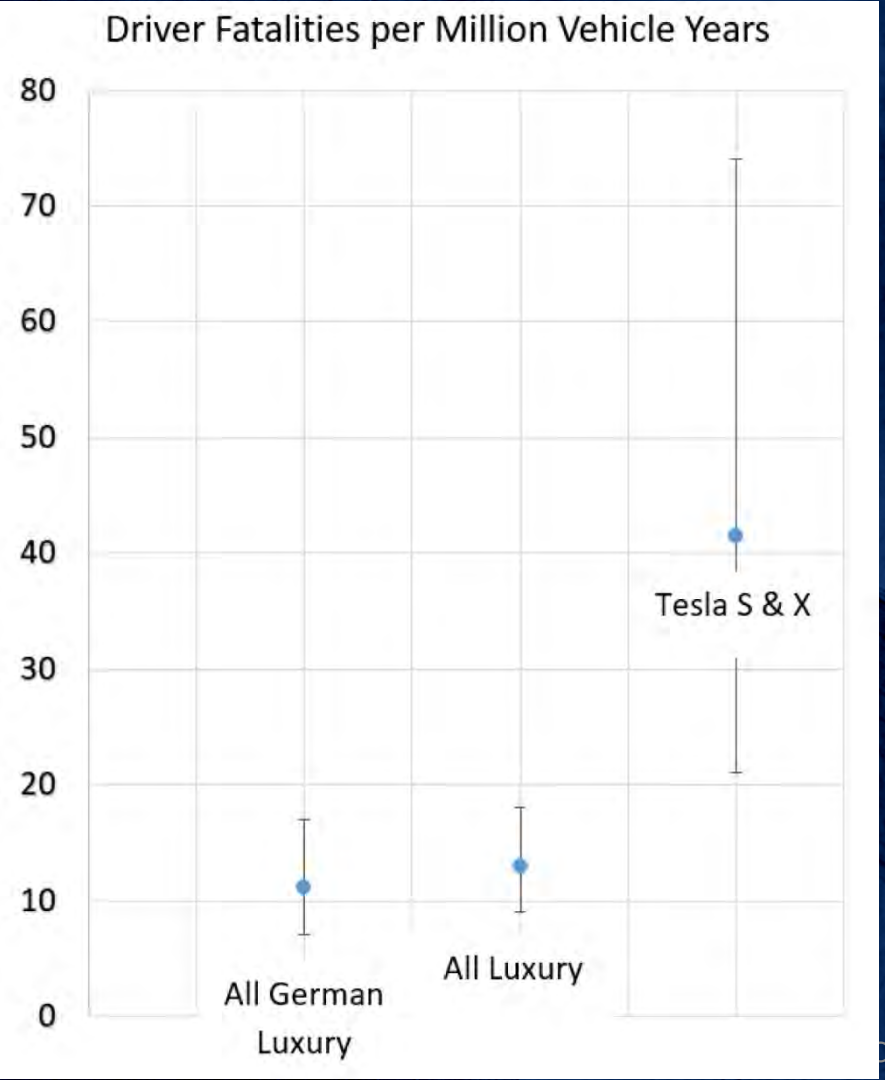
- **Tesla Admits Autopilot Feature Led to Fatal China Crash in 2016**
- (Yicai Global) Feb. 28 [2018] -- Electric carmaker Tesla Inc. has admitted that its self-driving feature was responsible for the collision that caused the death of a 23-year-old Chinese man more than two years ago.
- **https://www.yicaiglobal.com/news/tesla-admits-autopilot-feature-led-fatal-china-crash-2016**

©McCarthy Engineering

Tesla “autopilot”

- Review of Tesla crash data proves it is Elon Musk, and not the commentators, who are mathematically challenged
- When comparative fatal crash rates are computed: “Conclusion: Autopiloted Teslas have twice the fatal-crash rate of human-piloted Teslas”
- But what about the injury rate?
- Conventional vehicles have a 27% lower airbag deployment crash rate than Teslas on autopilot

©McCarthy Engineering



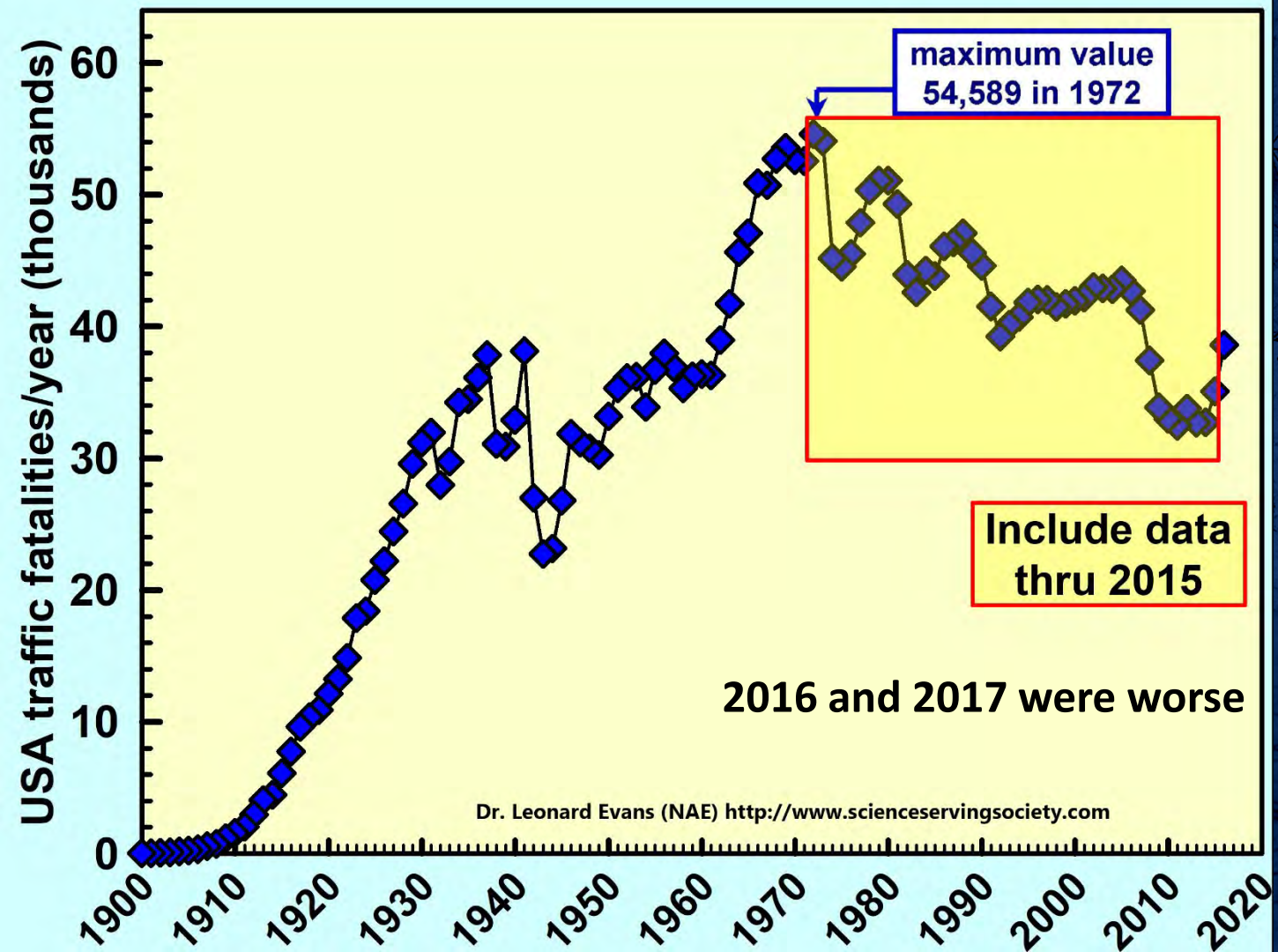
Result from manually correcting Tesla codes in FARS

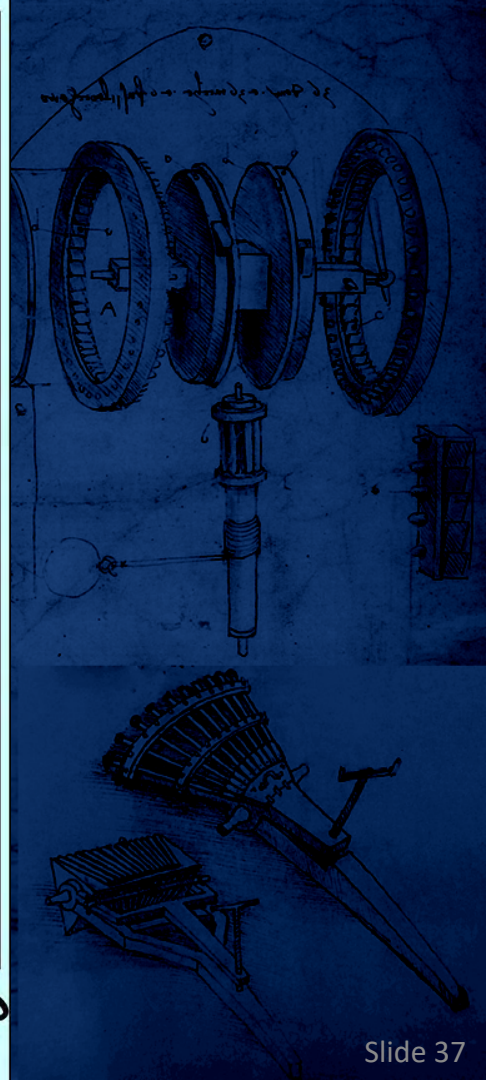
https://medium.com/@MidwesternHedgi/teslas-driver-fatality-rate-is-more-than-triple-that-of-luxury-cars-and-likely-even-higher-433670ddde17

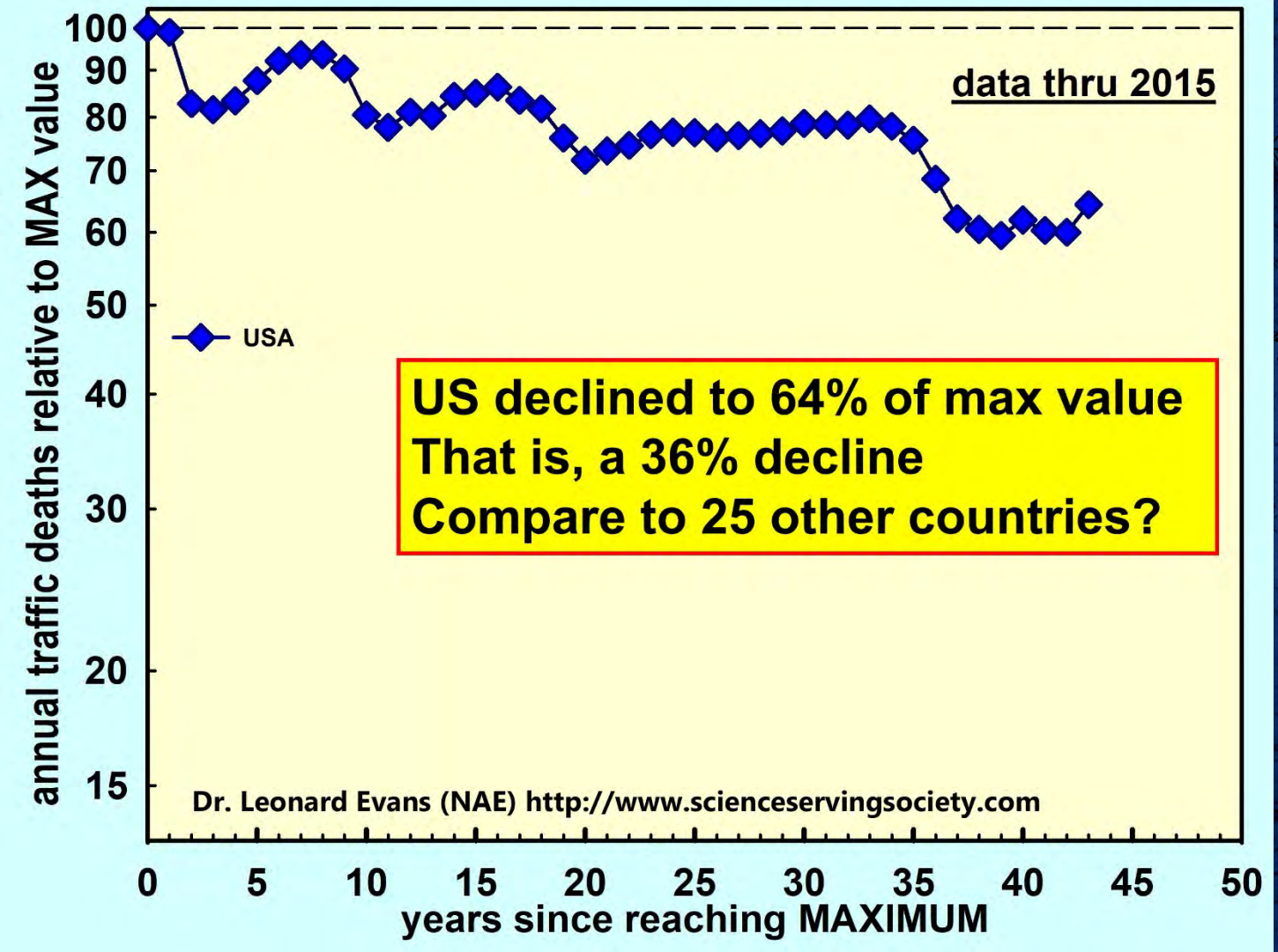
Inconceivable the NHTSA would repeat the Tesla Statistic

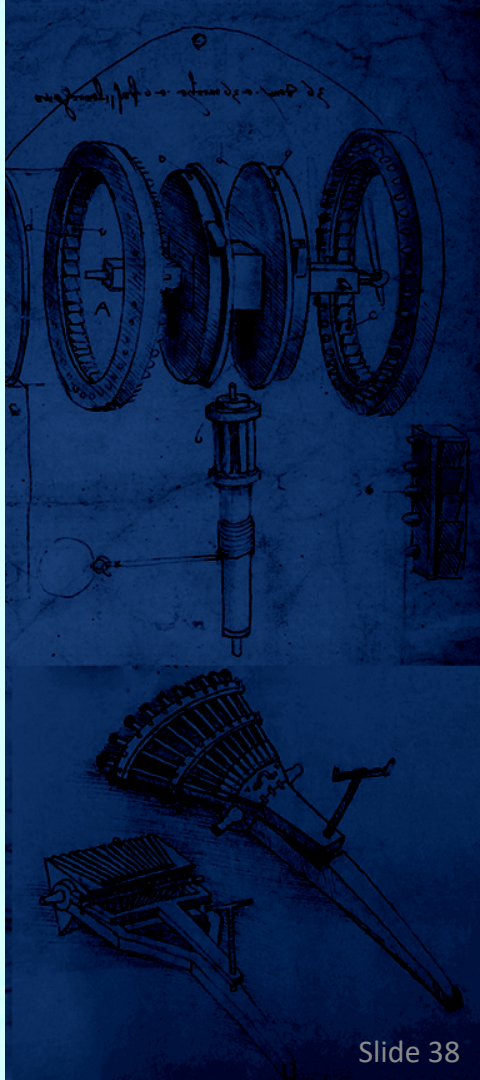
Until you realize the NHTSA has a problem

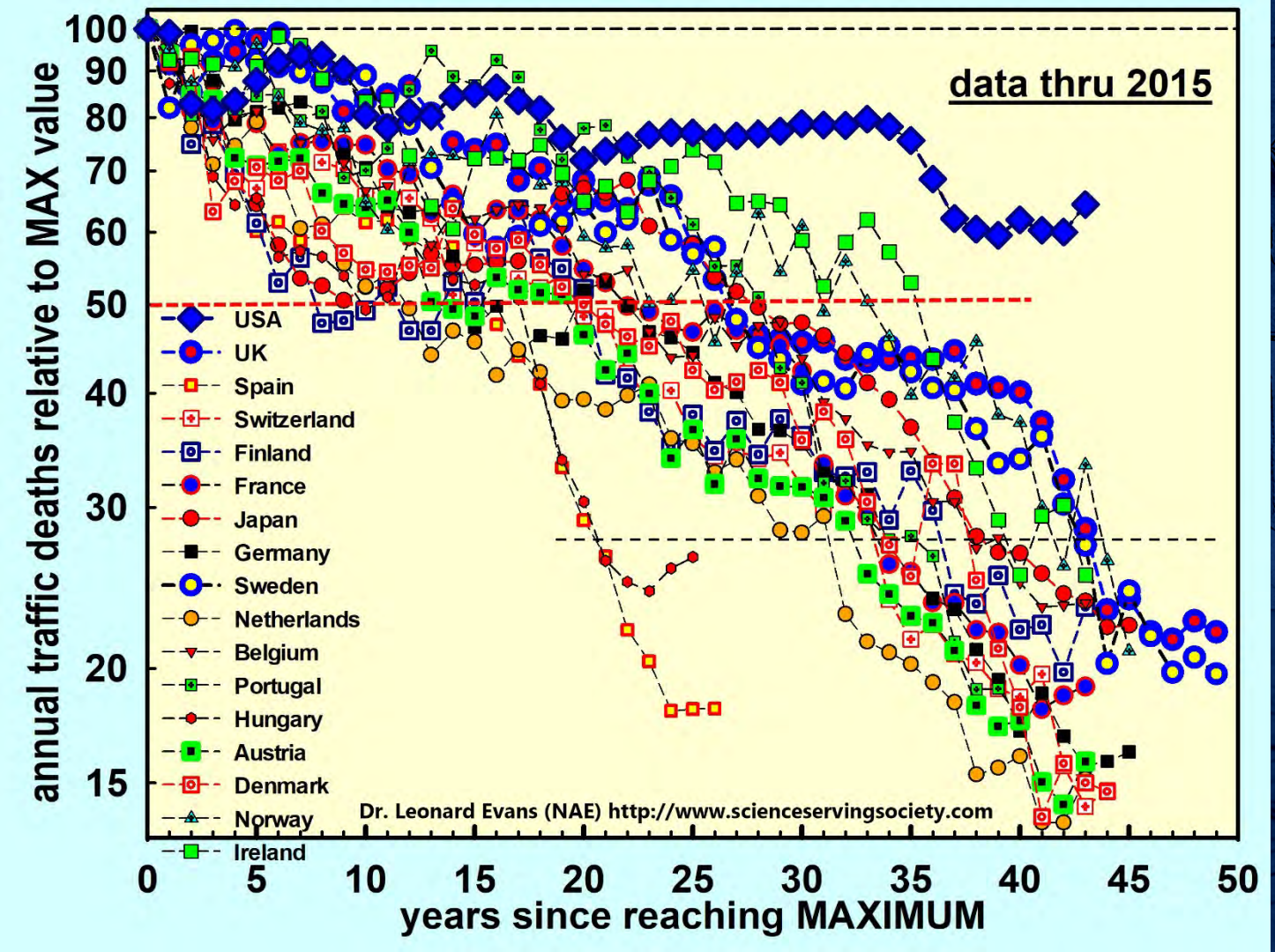
©McCarthy Engineering


USA traffic fatalities/year (thousands)
0
10
20
30
40
50
60
1900
1910
1920
1930
1940
1950
1960
1970
1980
1990
2000
2010
2020
maximum value
54,589 in 1972
Include data
thru 2015
2016 and 2017 were worse
Dr. Leonard Evans (NAE) http://www.scienceservingsociety.com




data thru 2015
USA
US declined to 64% of max value
That is, a 36% decline
Compare to 25 other countries?
Dr. Leonard Evans (NAE) http://www.scienceservingsociety.com
annual traffic deaths relative to MAX value
100
90
80
70
60
50
40
30
20
15
0
5
10
15
20
25
30
35
40
45
50
years since reaching MAXIMUM

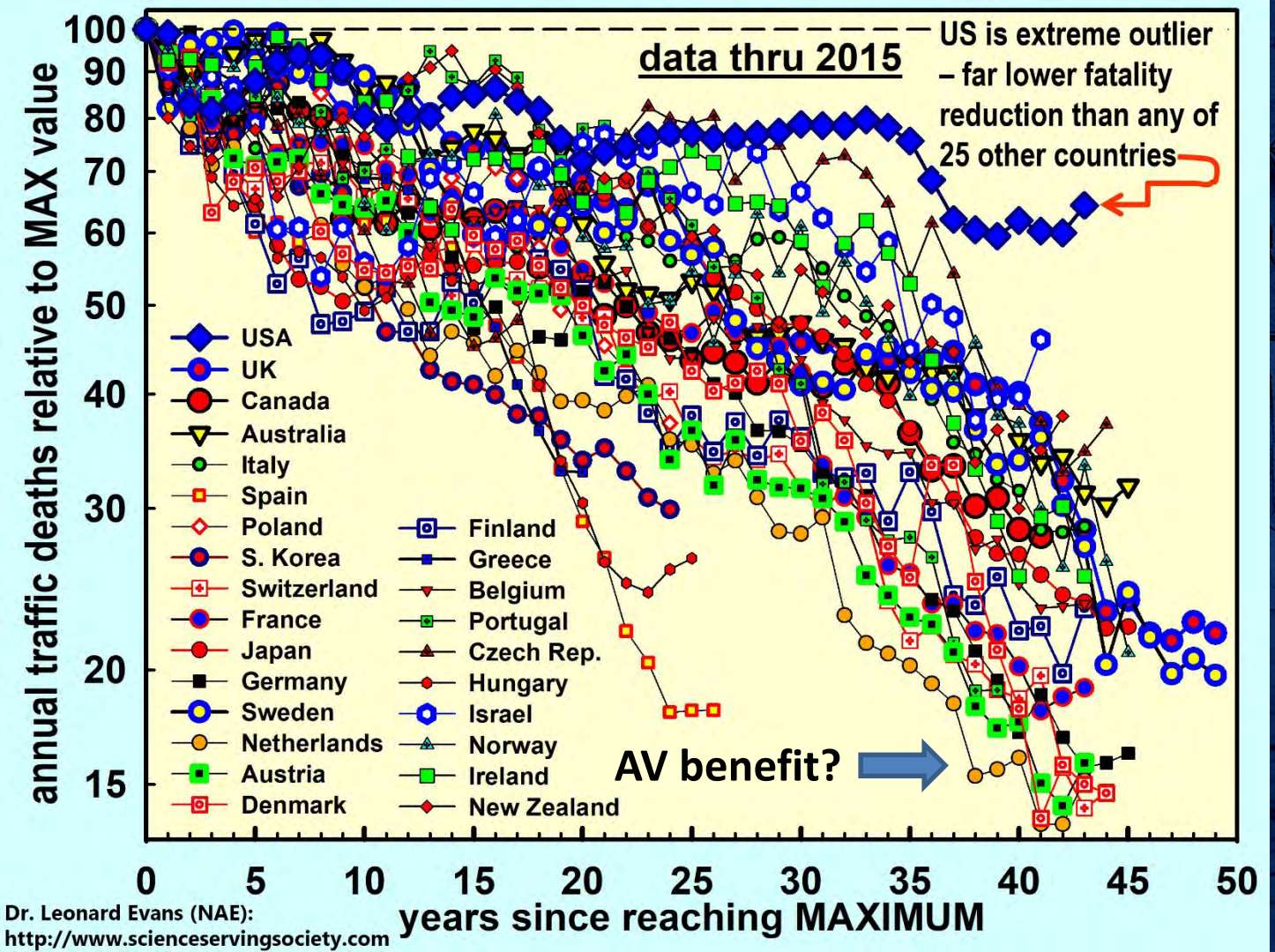




Low hanging fruit??

Where is our NHTSA?

No study of this Success???



Dr. Leonard Evans (NAE):
http://www.scienceservingsociety.com

Dr. Evans: It's not the "National Highway Traffic Safety Administration"

"National Vehicle Safety Administration"

Why is the US so bad?

- **The NHTSA is obsessed with vehicle safety rather than driver behaviors**
  - **I believe an unfortunate legacy of its creation**
- **Driver behaviors are far more important to safety**
  - **Our permissible blood alcohol of .08 is a disgrace**
  - "A .05% BAC legal limit is the most common and found in … Argentina, Australia, Austria, Belgium, Finland, France, Germany, Greece, Hong Kong, Israel, Italy, South Africa, Spain, Switzerland, Thailand, Taiwan, Turkey, and others"

©McCarthy Engineering

As bad as this is, it is about to get worse

- **“EU lists 11 car safety systems to become mandatory from 2021”**
  - Advanced emergency braking
  - Alcohol interlock installation facilitation
  - Drowsiness and attention detection
  - Event (accident) data recorder
  - Emergency stop signal
  - Full-width frontal occupant protection crash test and improved seatbelts
  - Head impact zone enlargement for pedestrians and cyclists, as well as safety glass
  - Intelligent speed assistance
  - Lane keeping assist
  - Pole side impact occupant protection
  - Reversing camera or detection system

©McCarthy Engineering

The future

- "The notion that they [autonomous vehicles] are today safer than humans is pure myth," said Steve Shladover at California PATH, a transportation research arm of UC Berkeley. "They're not even close to the capabilities of human drivers."
- A higher crash rate is currently observed in every mode of automated driving
  - And we have visited Tesla's fatal crash rate
- Instead of AVs, the biggest safety impact could be made by developing the driver "assistance" technologies as a gradual path to full AV
- AND bringing our insane driving regulations in conformance with the rest of the world.

©McCarthy Engineering

Questions?

©McCarthy Engineering

IEEE Guide to Autonomous Vehicle Technology

Coming Q4 2018! 7-course online training program from IEEE

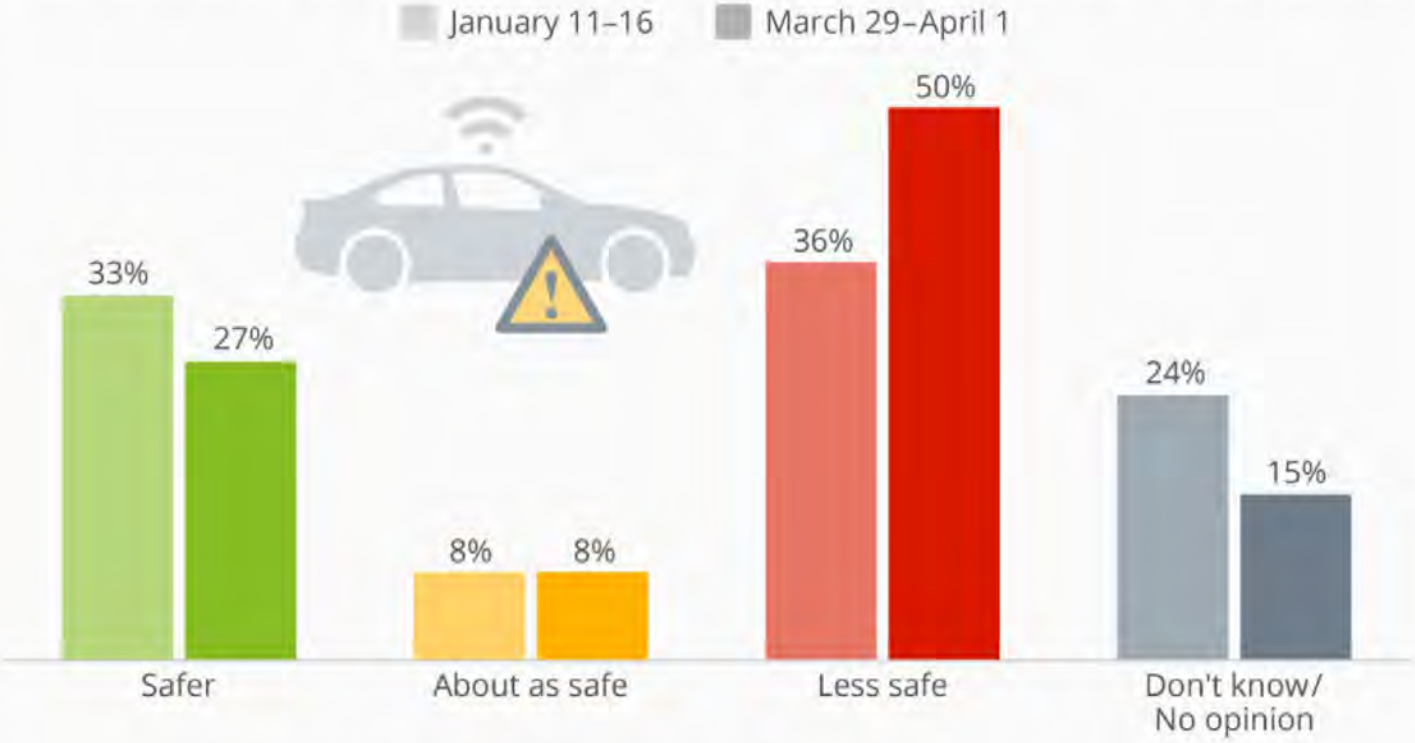
IEEE Guide to Autonomous Vehicle Technology is a seven-course program that covers foundational and practical applications of autonomous, connected, and intelligent vehicle technologies.

For more information or to pre-order this course program, completed the interest form at http://bit.ly/2PN6PqB to be connected with an IEEE Content Specialist.

©McCarthy Engineering

Fatal Accidents Damage Trust in Autonomous Driving

Would you say that self-driving cars are more or less safe than vehicles driven by humans?



Based on two polls among roughly 2,000 U.S. adults, each with a margin of error of +/-2%

@StatistaCharts

Source: Morning Consult

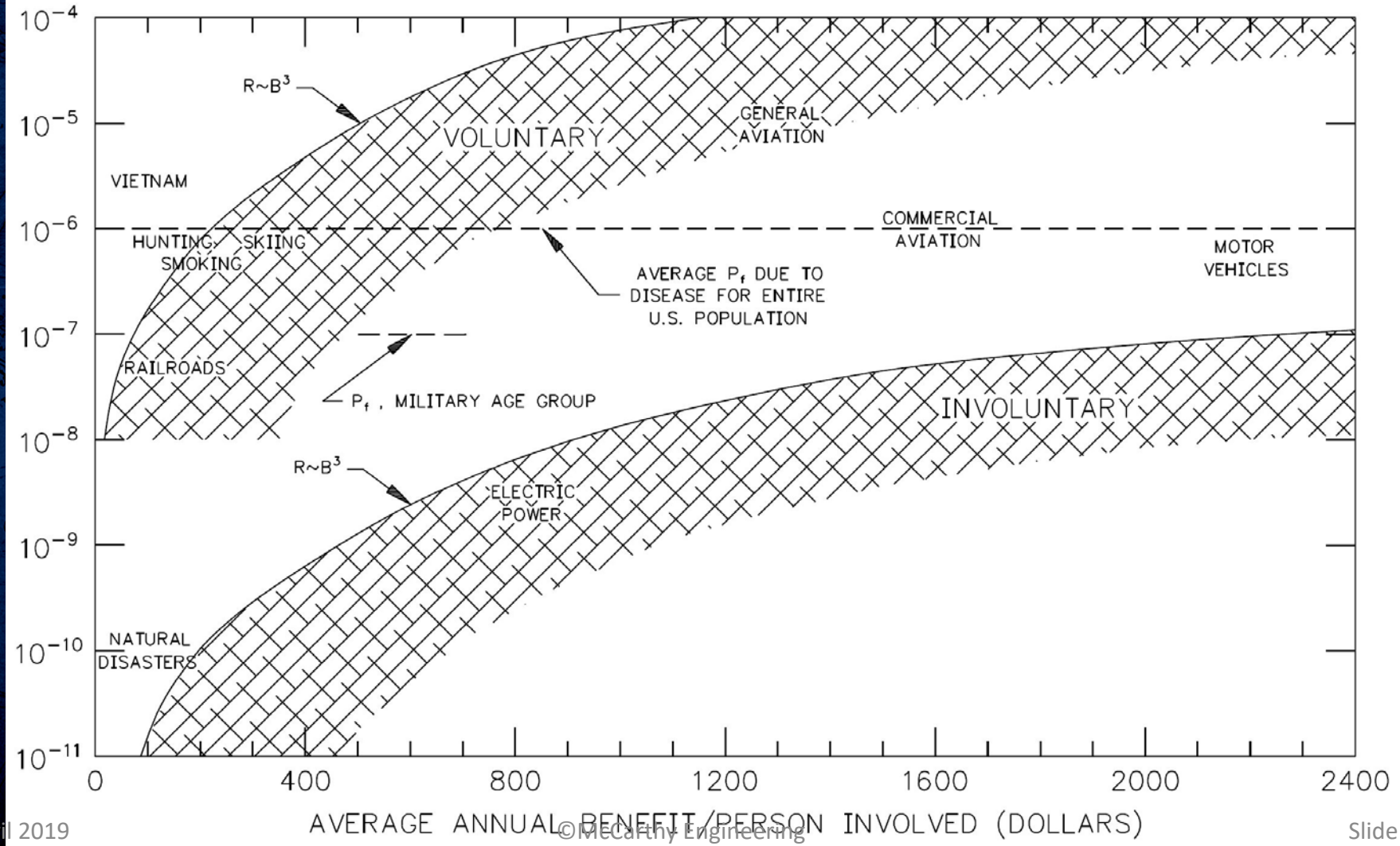
statista

Published 16 April 2018

How Safe Is Safe Enough for Self-Driving Vehicles (SDVs)?

- Two risk-acceptance criteria emerged: the *tolerable risk* criterion, which indicates that SDVs should be four to five times as safe as HDVs, and
- The *broadly acceptable risk* criterion, which suggests that half of the respondents hoped that the traffic risk of SDVs would be two orders of magnitude lower than the current estimated traffic risk.

©McCarthy Engineering



© McCarthy Engineering

Tesla crash US 101 in Silicon Valley 23 Mar 18

The driver had the problem before

©McCarthy Engineering

Autopilot crash US 101 on 23 March 2018

©McCarthy Engineering

Autopilot status 3 weeks ago*

- Musk, 47, started selling full self-driving as an $8,000 option in October 2016.
- Tesla then suffered a series of setbacks, including departures of top Autopilot managers and engineers.
- Owners who paid thousands of dollars for the options filed a class-action lawsuit, alleging they were deceived into buying a feature that didn't exist.

*https://www.bloomberg.com/news/articles/2018-10-19/tesla-drops-self-driving-option-buyers-have-been-unable-to-use

©McCarthy Engineering

Challenges for autonomous vehicles

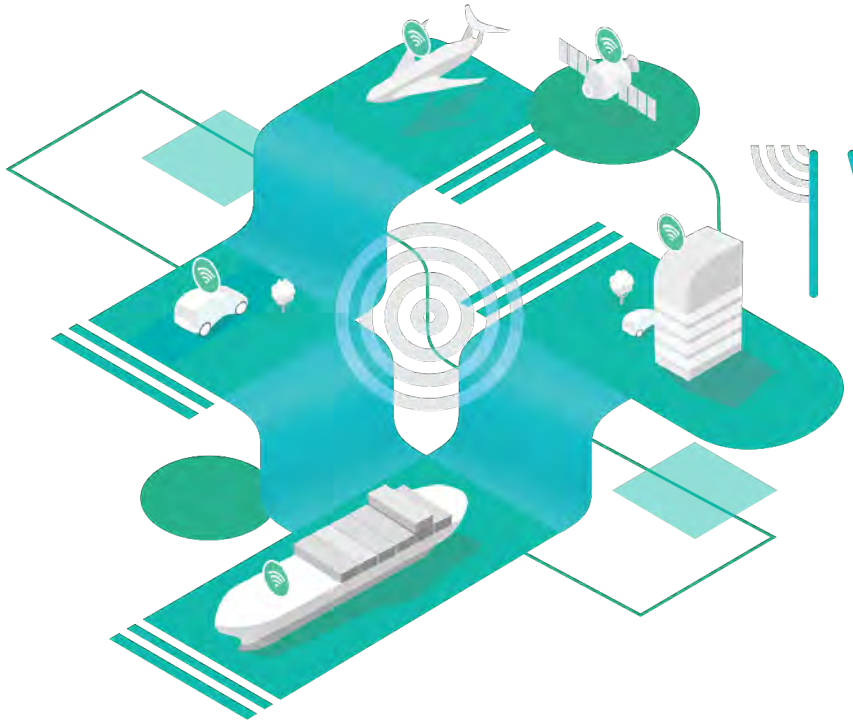
- The Google self-driving technology requires an "intricate" and detailed map about prospective routes involving "vastly more effort" than Google maps and are "an order of magnitude more complicated."
- This requirement poses implications for its introduction in countries, such as China, where "for reasons related to security, government regulations mandate that public maps cannot be more accurate than 50 meters"

©McCarthy Engineering

Challenges for autonomous vehicles

- the autonomous vehicle is the ideal suicide bomber
- criminals escaping in an autonomous vehicle would be free to shoot at their pursuers
- In the US he most frequent preference was for no self-driving (45.8%), followed by partially self-driving (38.7%), with completely self-driving being the least preferred (15.5%).“
  - 75 percent of Chinese said they would likely ride in a self-driving car

©McCarthy Engineering



Highlights of the First International Workshop on Autonomous Systems Safety, Reliability, and Security

Ali Mosleh
Distinguished Professor
Evelyn Knight Chair in Engineering
Director, The B. John Garrick Institute for the Risk Sciences
University of California, Los Angeles

Presented at Workshop on Risk Analysis of of Autonomous Cars
April 26, 2019

NTNU
Norwegian University of Science and Technology

The B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

DNV·GL

The Research Council of Norway

ROLLS ROYCE

Introductory Remarks

The First International Workshop on Autonomous Systems Safety (IWASS-1) was recently held in Trondheim Norway, co-sponsored by UCLA and Norwegian University of Science and Technology (NTNU). The objective of the workshop was to identify common challenges related to safety, reliability and security (SRS) of autonomous systems, and propose possible solutions for those challenges. A white paper distributed to the attending 40 experts from academia, industry, and governmental agencies, proposed the following topics as the focus of the workshop: How to make the case for autonomous system SRS; (b) Approaches to modeling and analysis of autonomous systems SRS; (c) Risks and benefits of human being in the loop; and (4) Issues in establishing safety standards, oversight, regulations, and liability. Two and half days of plenary presentations and discussions by four breakout groups on these subjects resulted in preliminary conclusions presented at the end of the workshop. This talk will summarize the key findings of IWASS-1 and provide a personal perspective on the challenges in assuring Safety, Reliability, and Security of autonomous system.

IWASS

- Gathered key experts in autonomous systems safety.
- Aimed to identify common challenges related to safety, reliability, and security (SRS) of autonomous systems.
- Discuss and propose possible solutions for the identified challenges.

Main sponsors:

NTNU
Norwegian University of Science and Technology

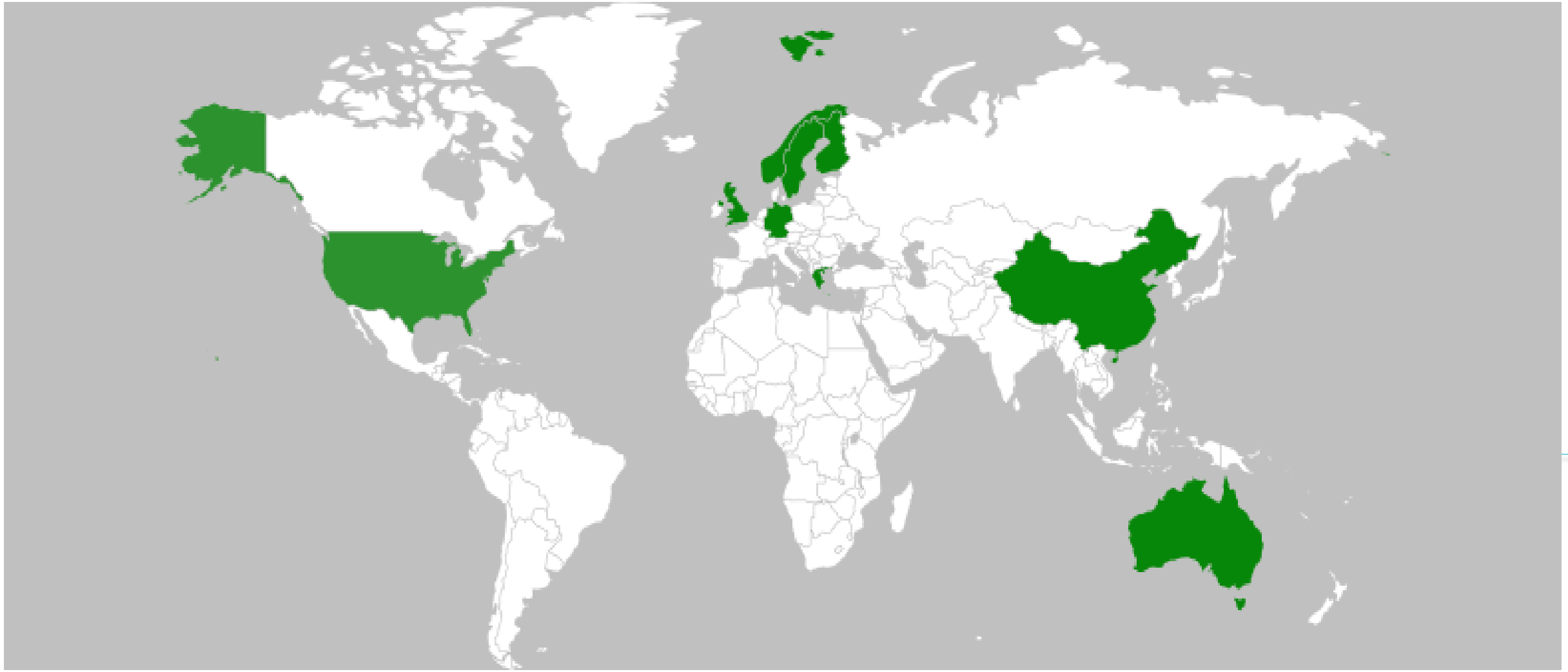
The B. John Garrick Institute for the Risk Sciences
UCLA ENGINEERING

The Research Council of Norway

DNV·GL

ROLLS ROYCE

Origin of participants



Participation

- 35 invited experts, 15 observers
  - Design Engineers
  - Service Providers
  - Operators
  - Risk, Safety, and Security Analysts
  - Regulators
  - Law and ethics specialists
  - Human behavior specialists
  - Philosophers
- Organizations
  - Industry
  - Government Agencies
  - Universities and Research Center
- Sectors
  - Land Transport
  - Aviation
  - Maritime
  - Defense

Key Topics

- Making the case for autonomous system Safety, Reliability and Security (SRS)
- Modeling and analysis methods for assessing autonomous system
- Human in the loop – benefits and risks
- Dealing with complexity of integrated systems of Software–Hardware–Human
- Safety standards, oversight, regulations, ethics and liability

Presentations

- Raised many important challenges, research questions, and perspectives:
  - Qualification, verification and validation approaches
  - Human factors in autonomy and research directions
  - Ethics and trust in autonomy
  - Application areas
    - autonomous cars and buses,
    - UAS,
    - intelligent marine systems
  - Risk issues related to safety and cybersecurity
  - Regulatory challenges and guidance for approval of autonomous ships

Breakout sessions

- Group 1 – SRS methods and modeling
- Group 2 – Human factors, ethics and regulations
- Group 3 – System verification, processes and testing
- Group 4 – Intelligence and decision support

Sample questions

- It is often said that holistic approach is needed for SRS assessment of autonomous systems. What does this actually mean?
- How can we determine “acceptable risk” for autonomous systems and operations?
- Should “acceptable risk” change with level of autonomy (LoA)?

Sample questions

- What are the main challenges of to safety, reliability, and security (SRS) of autonomous systems and operations?
- What challenges are similar between the different autonomous systems, operations, and industries?
- Which type of autonomous system is most feasible to be realized in the near future? Why?

Sample questions

- A challenge in risk analysis of novel systems is to identify everything that can go wrong. How can we deal with the unknown unknowns?

- Uncertainty in sensor data is a challenge. How should this uncertainty be handled in the design and operation of autonomous systems and operations?

Sample questions

- Do autonomous systems and operations need to be “as safe as” , or “safer than” other types of systems?
- Are AI systems suitable to make ethical decisions, what would be necessary for ethical decisions?
- Who is responsible for decisions made by the autonomous system (in case of accidents)?
- How can risk assessments and risk models of autonomous systems take “ shared control “ and “adaptive autonomy” sufficiently into account in the identification of hazards and the analysis of risk?

SRS Group: Topics Covered

- System Characterization
- Metrics to support (marine, maritime, land vehicles and aerospace)
  - Safety, Reliability, Security
- Adequacy of current modelling approaches
- Hazard Identification
- Validating self-learning
- Modelling Human / hardware interfaces
- Resilience
- Simulation to demonstrate the autonomous system capability
- Real-time (operational) decision support
- Data analytics

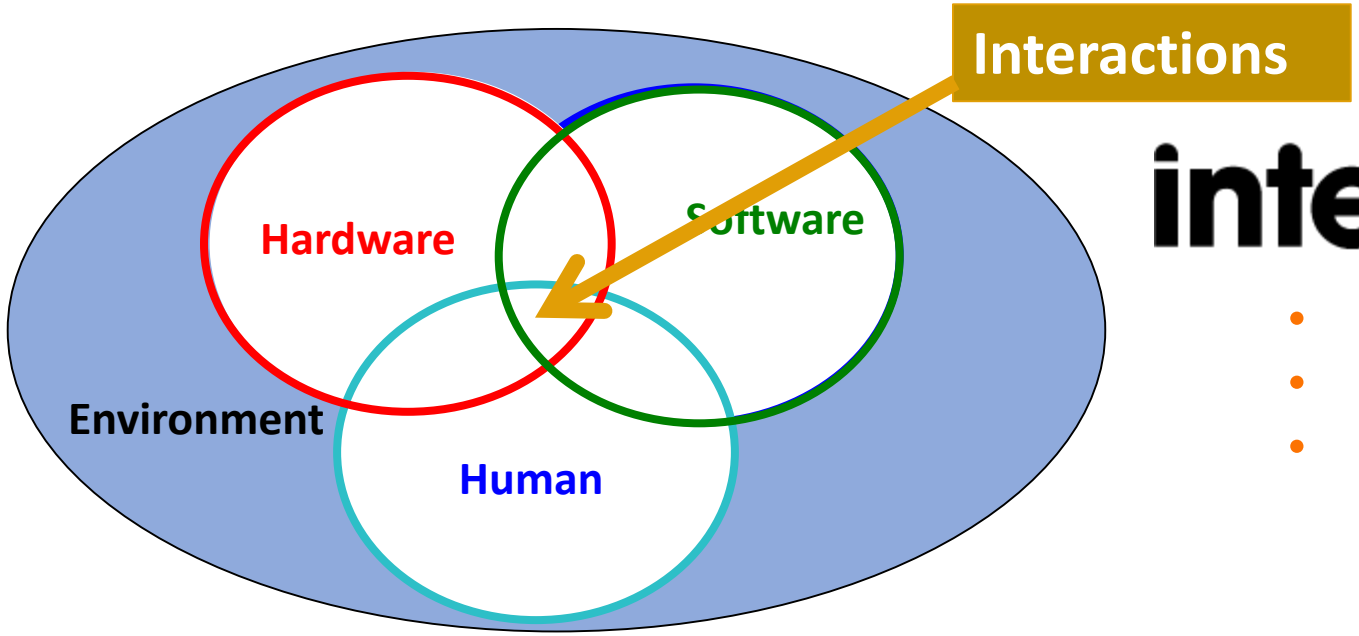
SRS Group Conclusions

- Many of the currently available methods can still play a part in supporting the safety, reliability and security of autonomous systems.
- However, many areas require new modelling techniques to be developed
  - These need to be underpinned by significant advances in understanding:
    - software failures and security
    - Identification and representation of the large number of options of environment, operation modes
- Data driven methods are inadequate to demonstrate safety

Cyber–Physical-Human (CPH) Systems

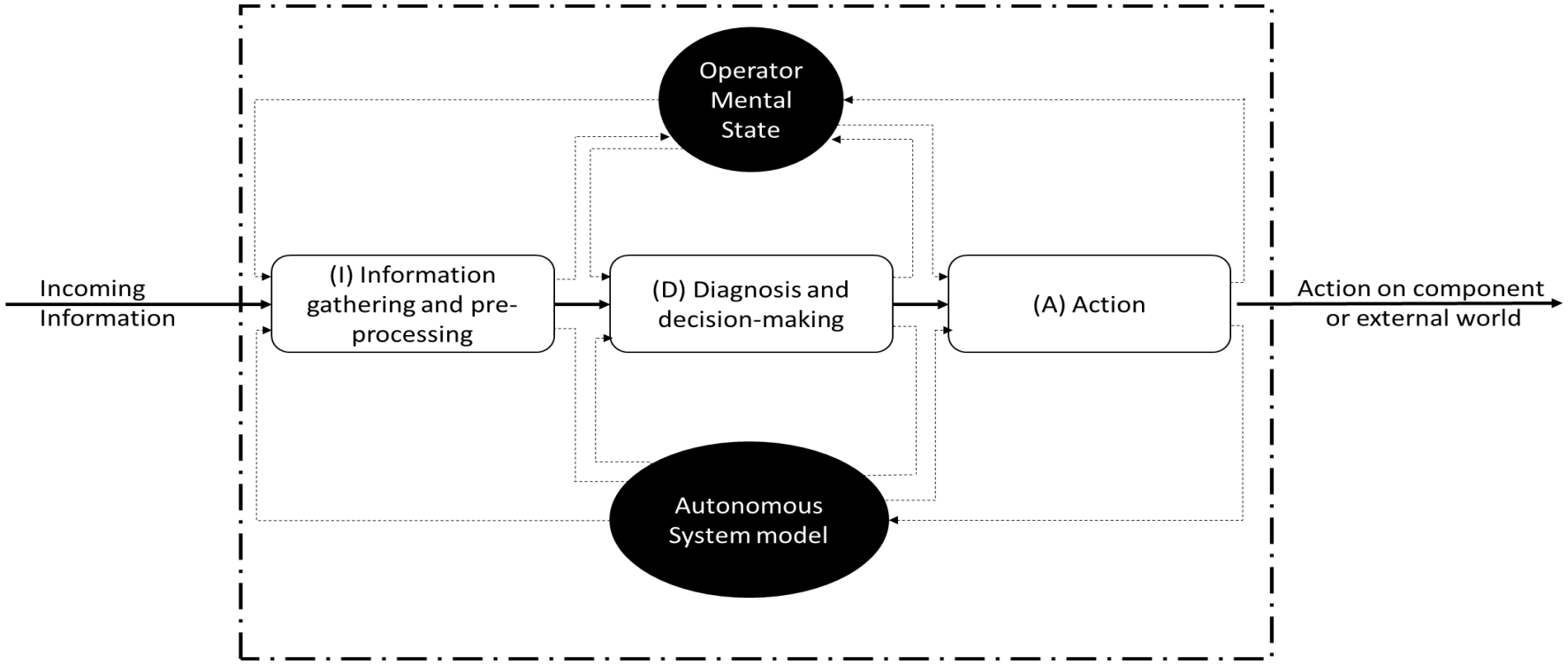
- Ultra complex, heterogeneous, distributed, open, possibly "learning systems"
- High levels of integration of the technical and social dimensions (highly interconnected socio-technical systems)
- Very high pace of development and deployment
- Higher levels of diversity of supply chain, subject to different levels of quality, reliability, and safety standards

A Major Challenge ….



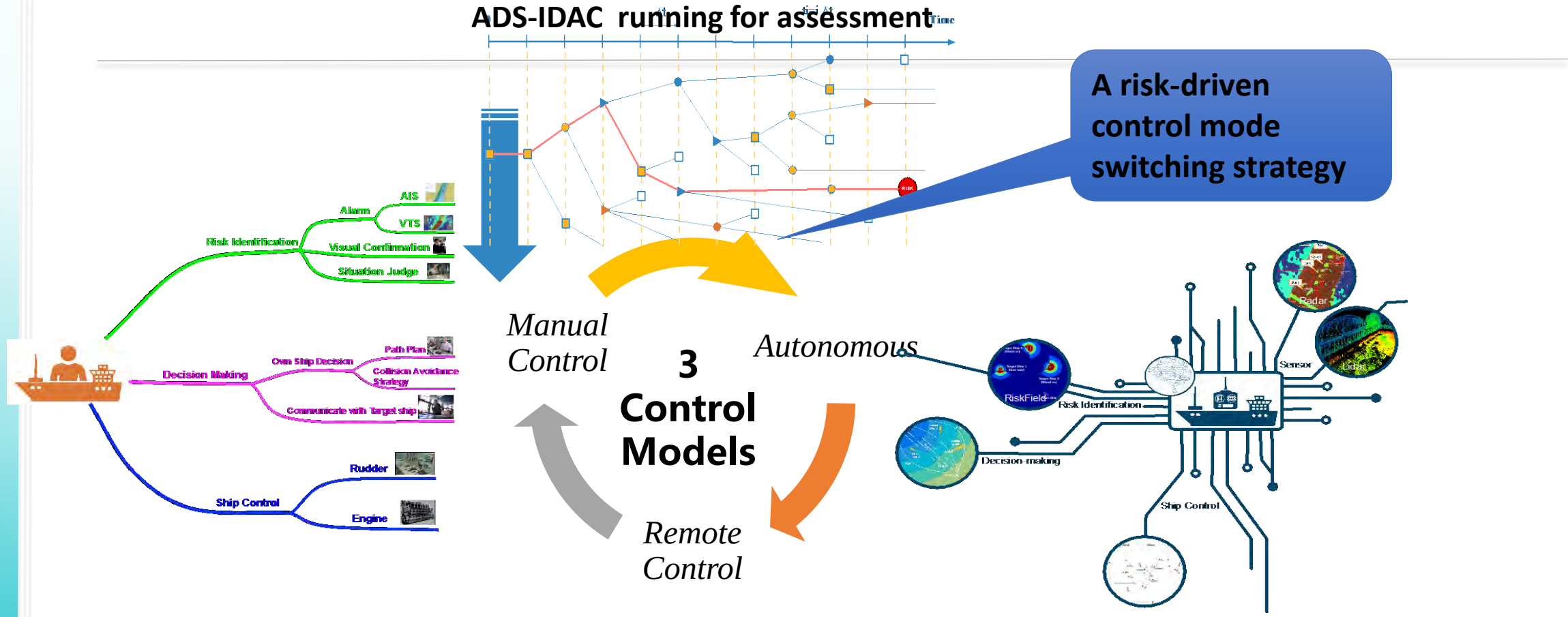
- Functional
- Physical
- Environmental

Concurrent Task Analysis



Probabilistic Simulation Approach

(Real Time Risk Based Decision Support of Unmanned Ships)



Solution Completeness and Scalability

- Computational demand / scalability
- Coverage, Scope Completeness ,
- Optimum Level of Decomposition
  - Hardware (Systems, Sub-systems, components, Parts, Failure Modes, Failure Causes …)
  - Software (Functions, Objects, Computational Routines, Line of Code,…)
  - Human (Cognitive Functions, Information Model, Task Decomposition,…)
- Interface Characterization
- Ability to Do a Graded Modeling and Analysis

My Observations

- Significant difference between incentives for service sector and system developers
- Developers overly enthusiastic and confident
- Regulators are slow and cautious
- Safety Analysts skeptical, see significant challenges
- Ethical issues are thought not to be unique to this technology
- It is often assumes that autonomous systems will be used for good purposes and to enhance the quality of life. That assumption may be unwarranted.

Outcome

The proceeding to be issued in June 2019

- Papers
- Report of the Working Groups
- Insights and Recommendations

2nd IWASS– March 2020

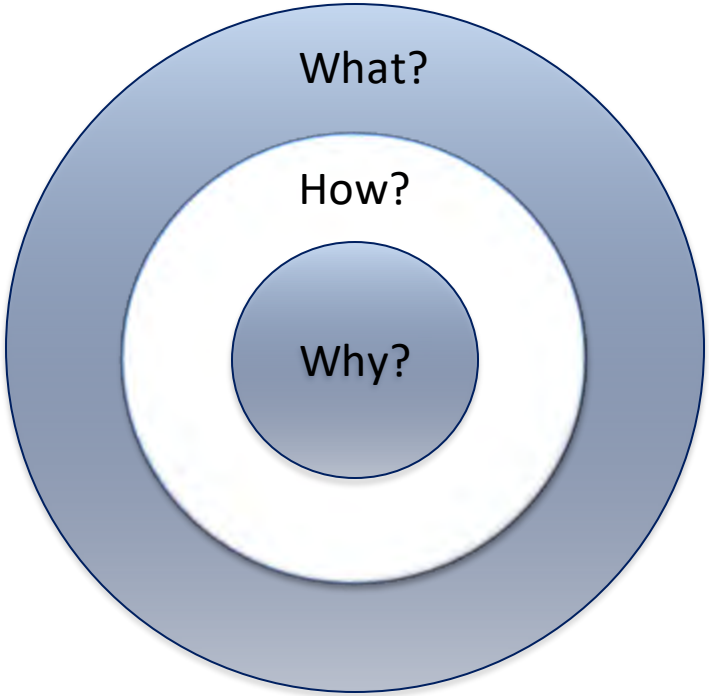
Development of dynamic safety envelopes for autonomous remotely operated underwater vehicles

Jeevith Hegde, Eirik Hexeberg Henriksen, Ingrid Bouwer Utne, Ingrid Schjølberg

Department of Marine Technology,
Norwegian University of Science and Technology (NTNU),
NO7491 Trondheim, Norway

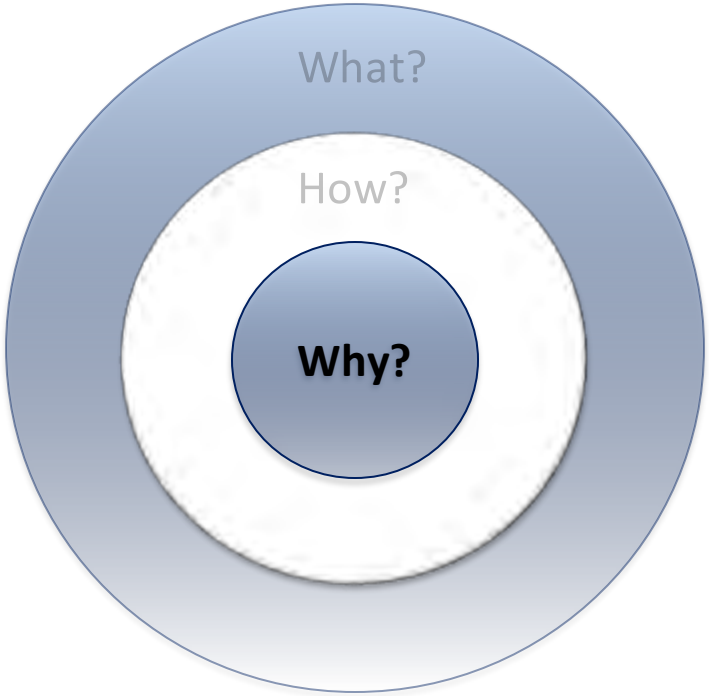
Outline

- Background
- Methods
- Laboratory setup
- Results
- Summary and future work



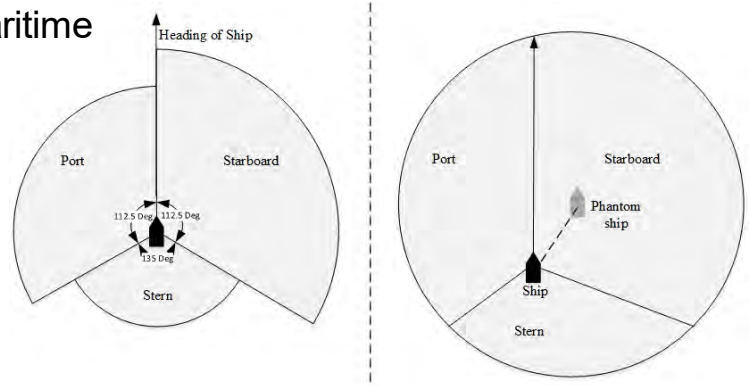
Outline

- » **Background**
- » Methods
- » Laboratory setup
- » Results
- » Summary and future work

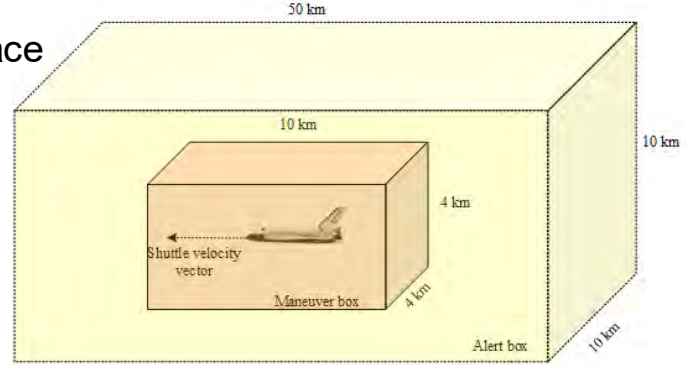


Background

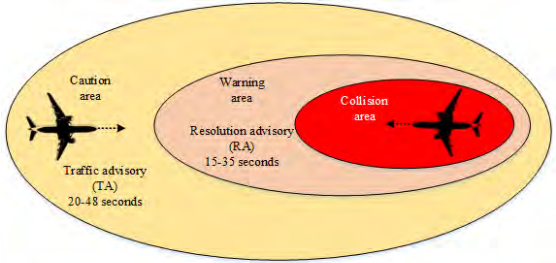
Maritime

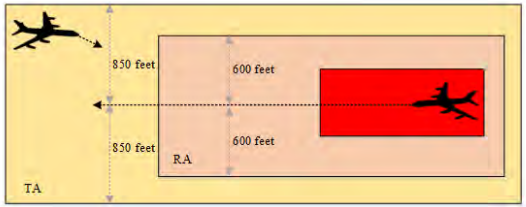


Space

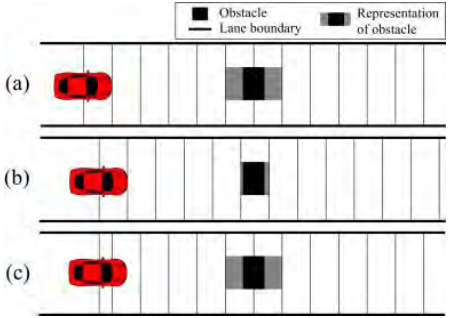


Aviation





Automotive



NTNU

Background

Collision risk indicators

+

Safety envelopes and Underwater traffic rules

+

Decision support Fuzzy logic

Dynamic safety envelopes

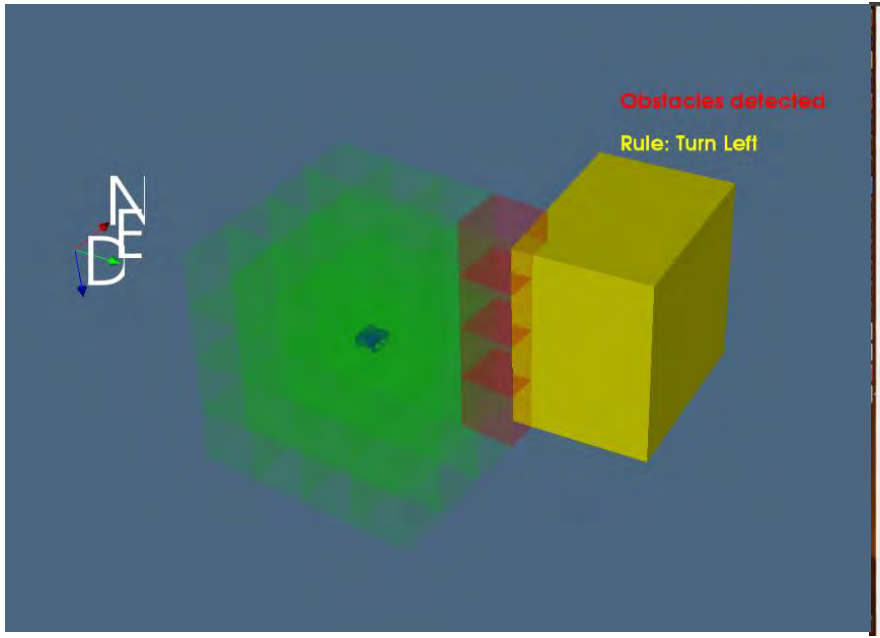
Hegde, J., Utne, I.B., Schjølberg, I., 2016. Development of collision risk indicators for autonomous subsea inspection maintenance and repair. J. Loss Prev. Process Ind. https://doi.org/10.1016/j.jlp.2016.11.002
Hegde, J., Henriksen, E.H., Utne, I.B., Ingrid, S., 2019. Development of safety envelopes and subsea traffic rules for autonomous remotely operated vehicles. Accepted by J. Loss Prev. Process Ind.
Hegde, J., Utne, I.B., Schjølberg, I., Thorkildsen, B., 2015. Application of fuzzy logic for safe autonomous subsea IMR operations, in: Safety and Reliability of Complex Engineered Systems - Proceedings - ESREL 2015. pp. 415–422.

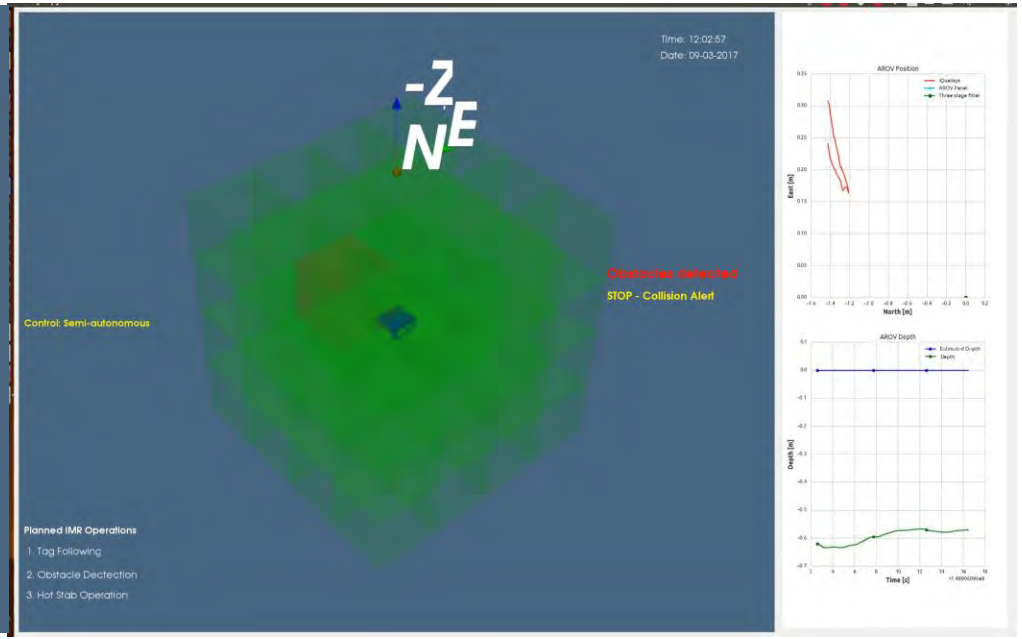
Background - Safety envelope

A 3D spatial area around the underwater vehicle forming a virtual protective barrier (in space and time) against collision with known and unknown obstacles in the subsea environment.

Hegde, J., Henriksen, E.H., Utne, I.B., Ingrid, S., 2019. Development of safety envelopes and subsea traffic rules for autonomous remotely operated vehicles. Accepted by J. Loss Prev. Process Ind.

Background - Static safety envelope

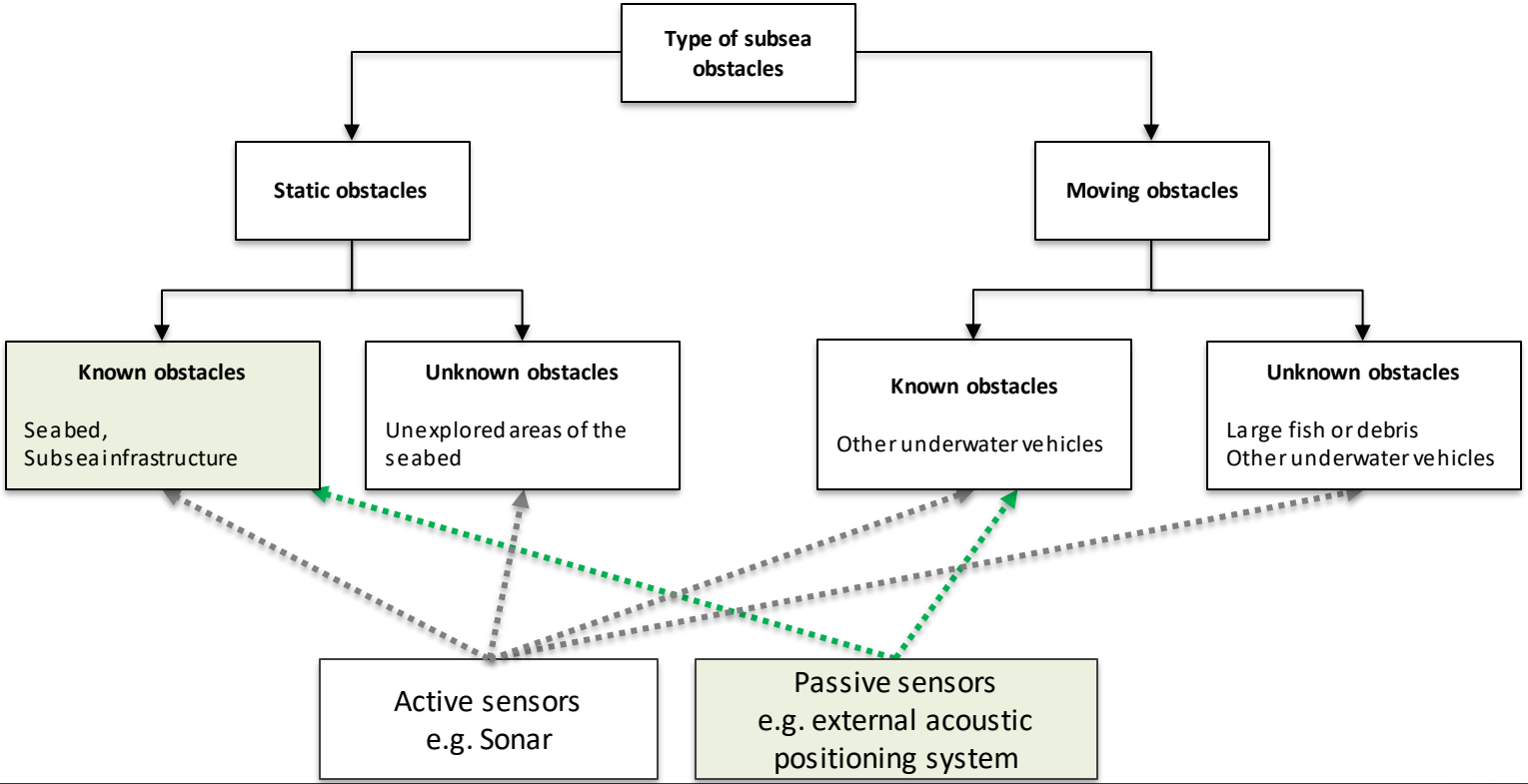




How do we make safety envelopes dynamic?

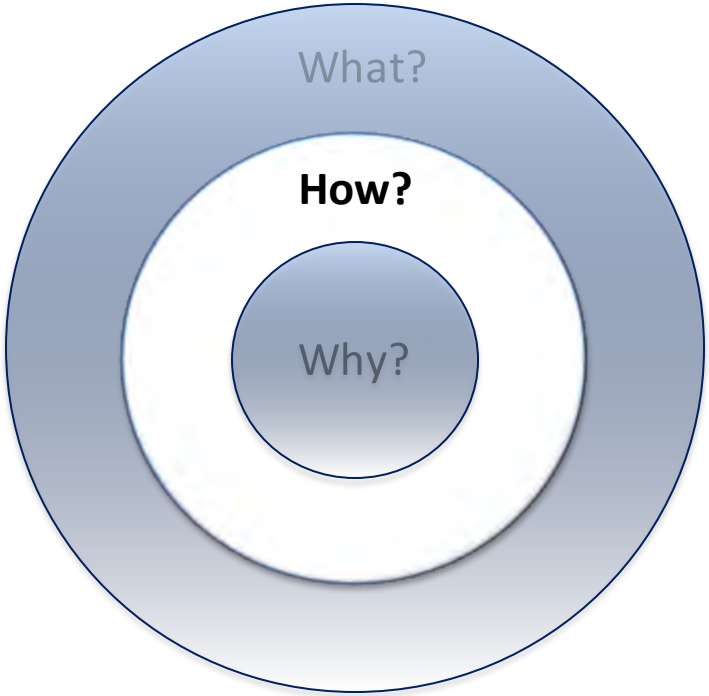
Hegde, J., Henriksen, E.H., Utne, I.B., Ingrid, S., 2019. Development of safety envelopes and subsea traffic rules for autonomous remotely operated vehicles. Accepted by J. Loss Prev. Process Ind.

Background - Scope

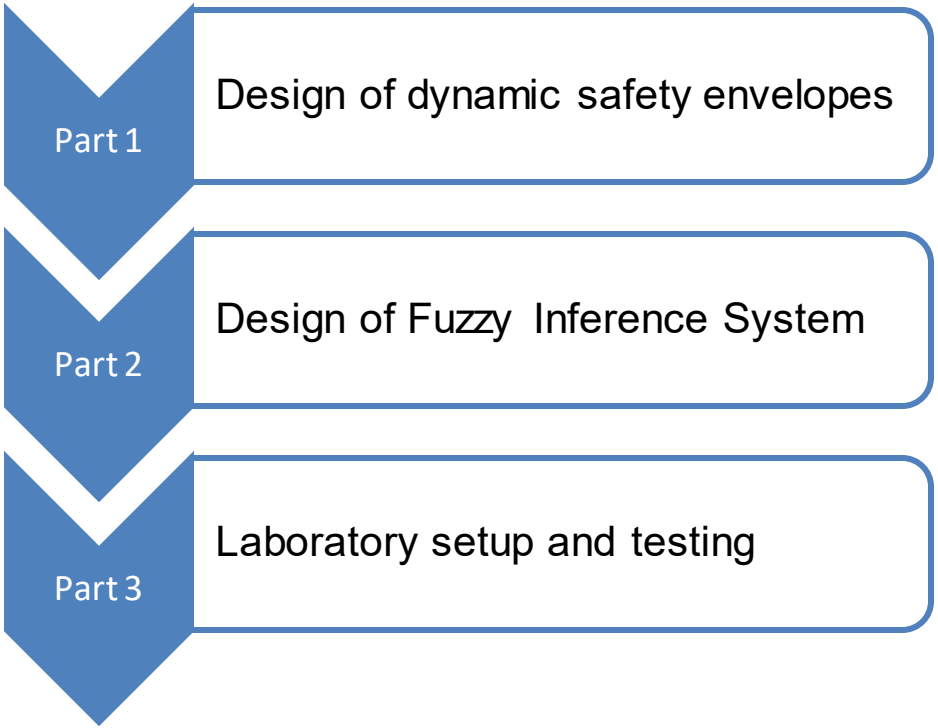


Outline

- » Background
- » **Methods**
- » **Laboratory setup**
- » Results
- » Summary and future work

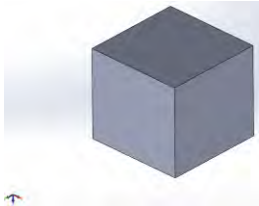


Methods

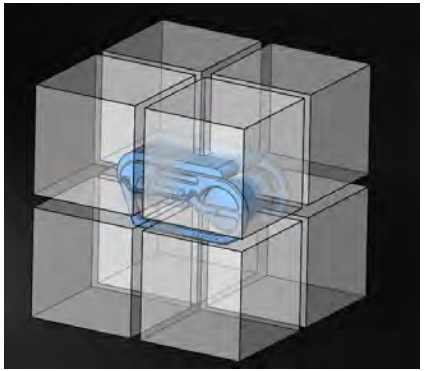

Part 1
Design of dynamic safety envelopes
Part 2
Design of Fuzzy Inference System
Part 3
Laboratory setup and testing

Methods - Design of envelopes

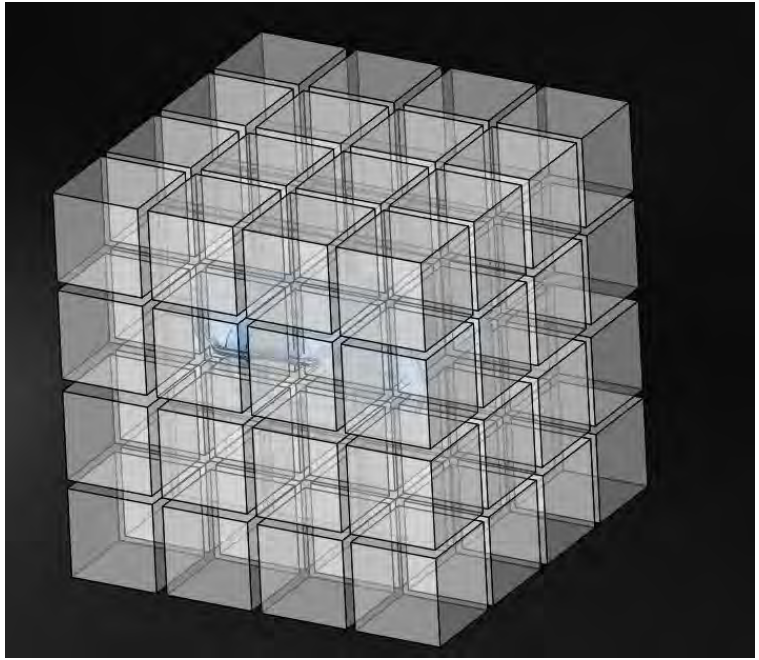
Level 0



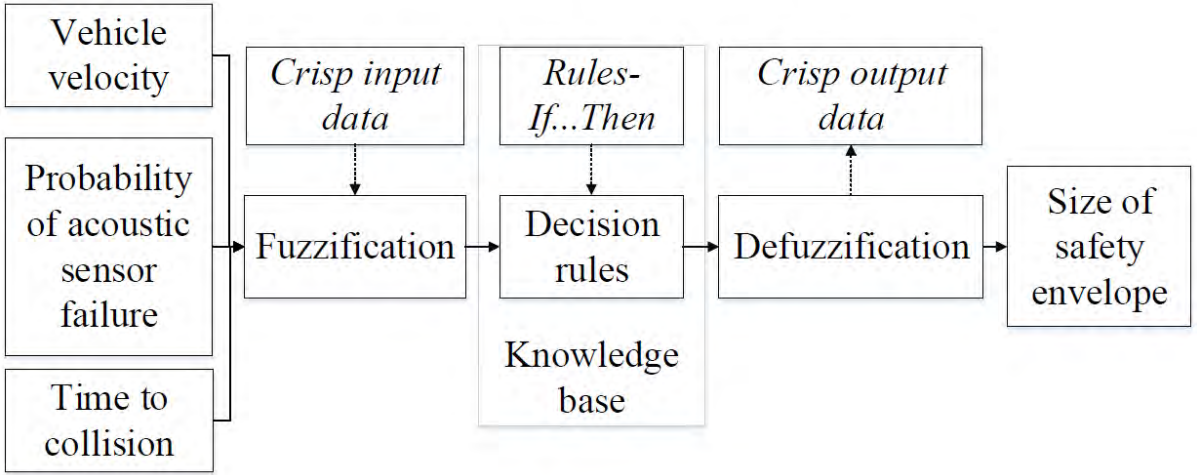
Level 1



Level 2



Methods - Fuzzy Inference System

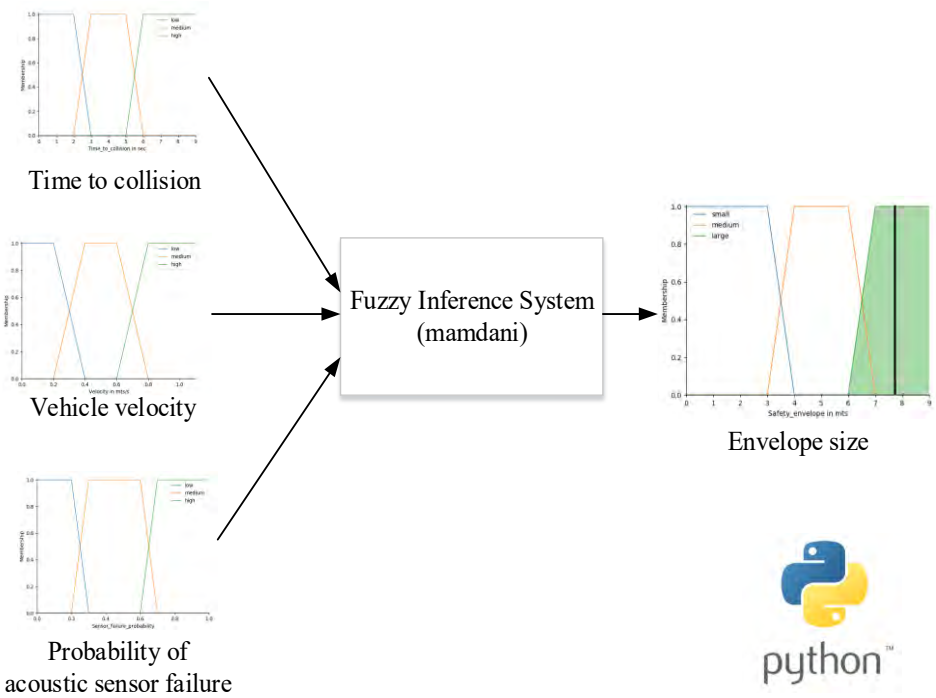


Methods - Fuzzy Inference System

Time to collision (TTC)

- $$TTC = \frac{Distance\ to\ obstacle}{Resultant\ velocity\ of\ vehicle}$$

- Low MF 0 to 3 s
- Medium MF 2 to 5 s
- High MF 5 to 10 s



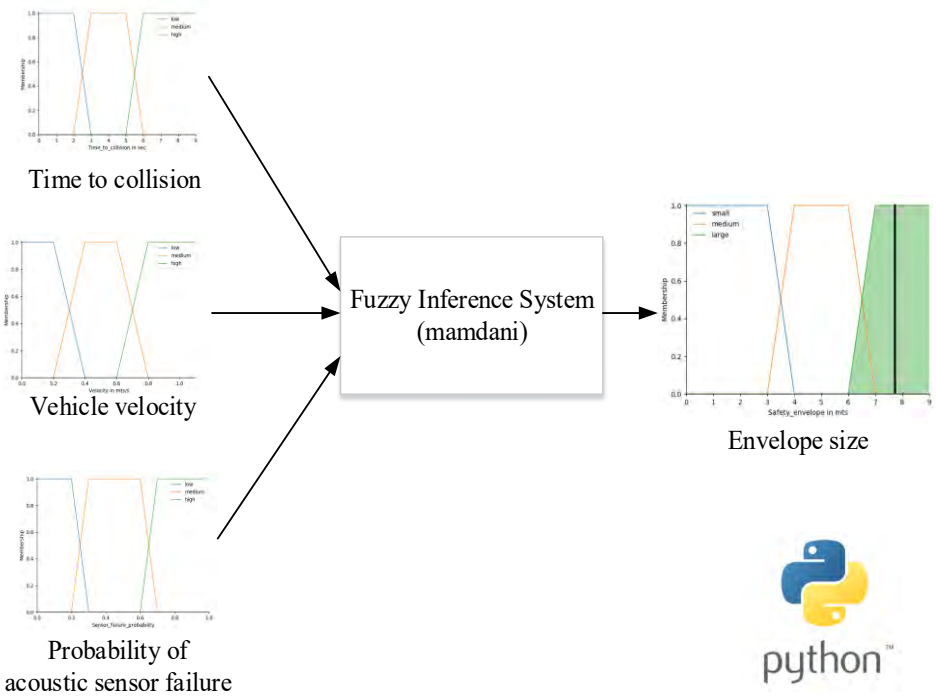
MF : Membership function

Methods - Fuzzy Inference System

Vehicle velocity

- Technical specifications of the Blue Robotics BlueROV2
- Envelope size is proportionally related to the velocity

- Low velocity MF 0 to 0.4 m/s
- Medium velocity MF 0.2 to 0.8 m/s
- High velocity MF 0.8 to 1 m/s



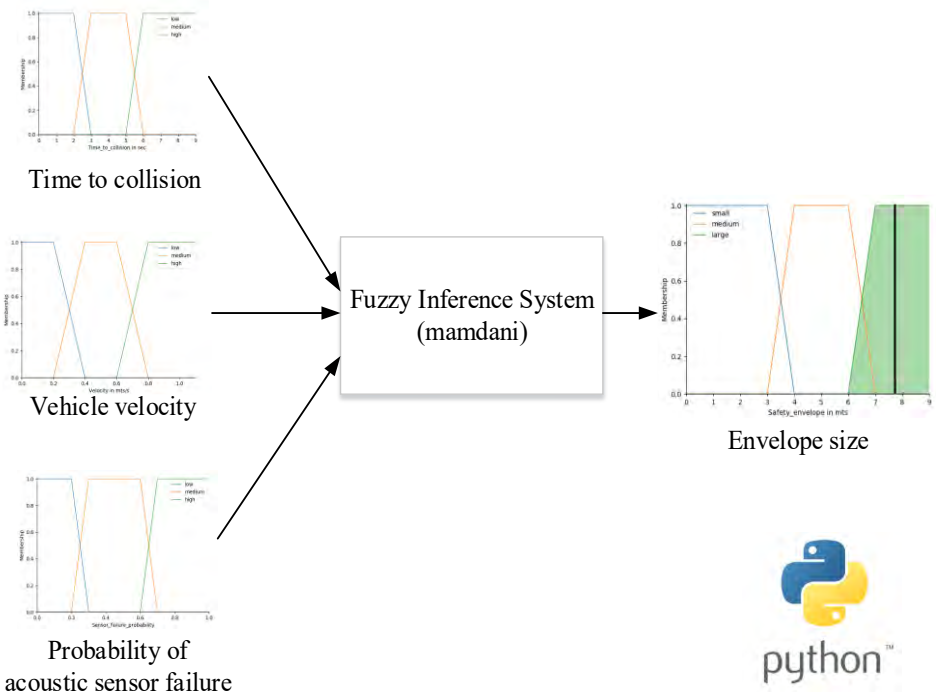
MF : Membership function

Methods - Fuzzy Inference System

Probability of acoustic sensor failure (PASF)

- Acoustic network with eight possible range (distance) measurements
- A minimum of four range values needed for reliable state estimation
- Acoustic sensor voting scheme is 4oo8

- Low MF ranges P 0 to 0.3
- Medium MF ranges P 0.2 to 0.7
- High MF ranges P 0.6 to 1



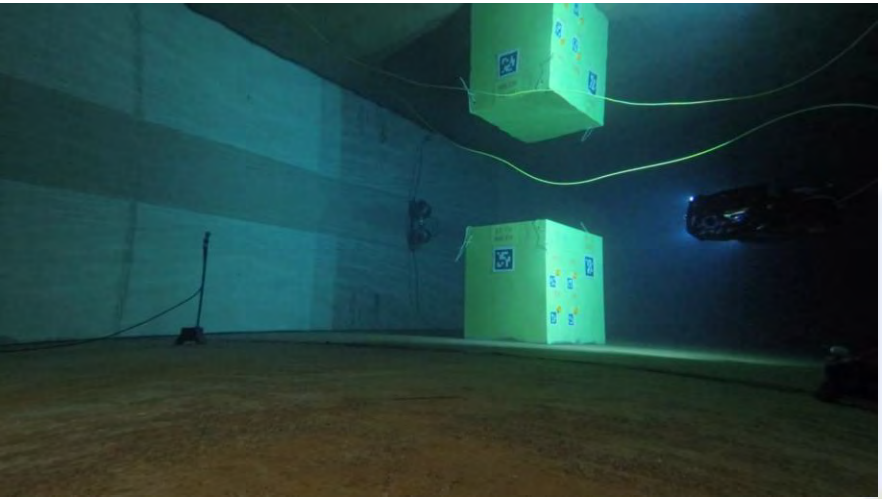
MF : Membership function

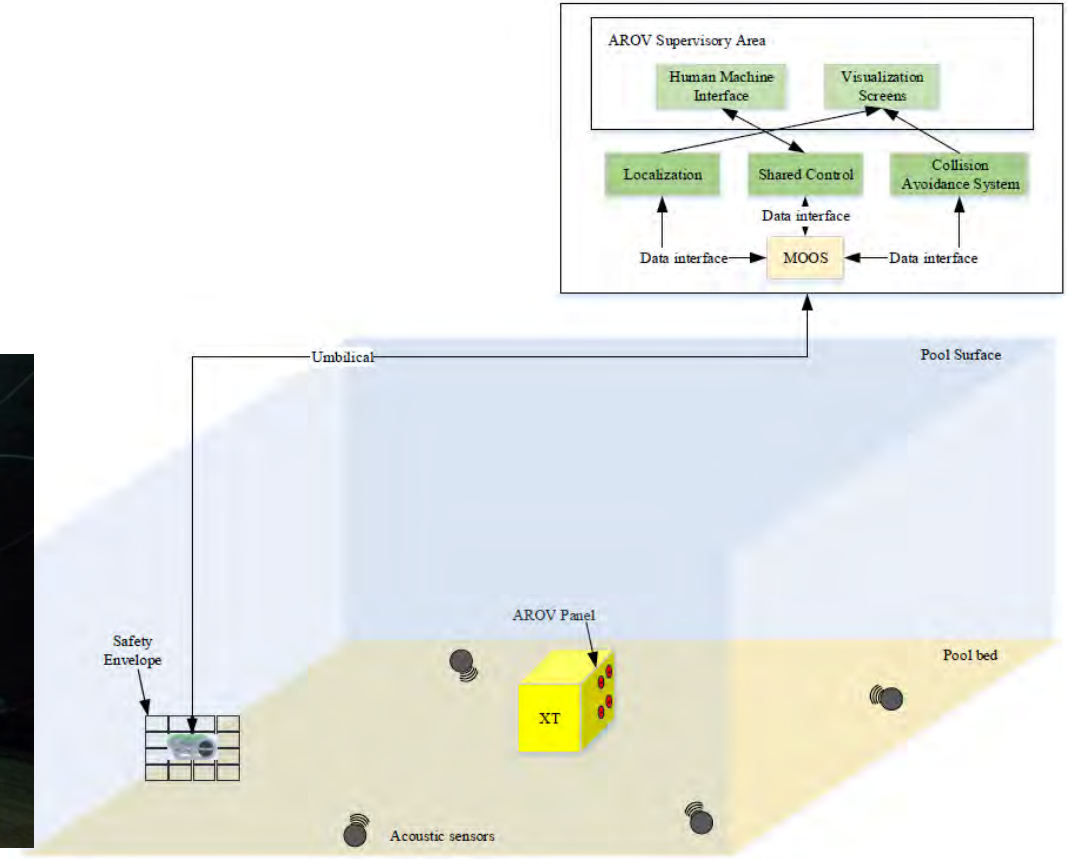
Methods - Fuzzy Rule Set

Vehicle Velocity	Probability of Acoustic Sensor Failure	Time To Collision	Size of Safety Envelope
Low	Low	Low	Large (6 – 10 mt)
Low	Low	High	Small (0 - 4 mt)

The combinations results in 27 rules

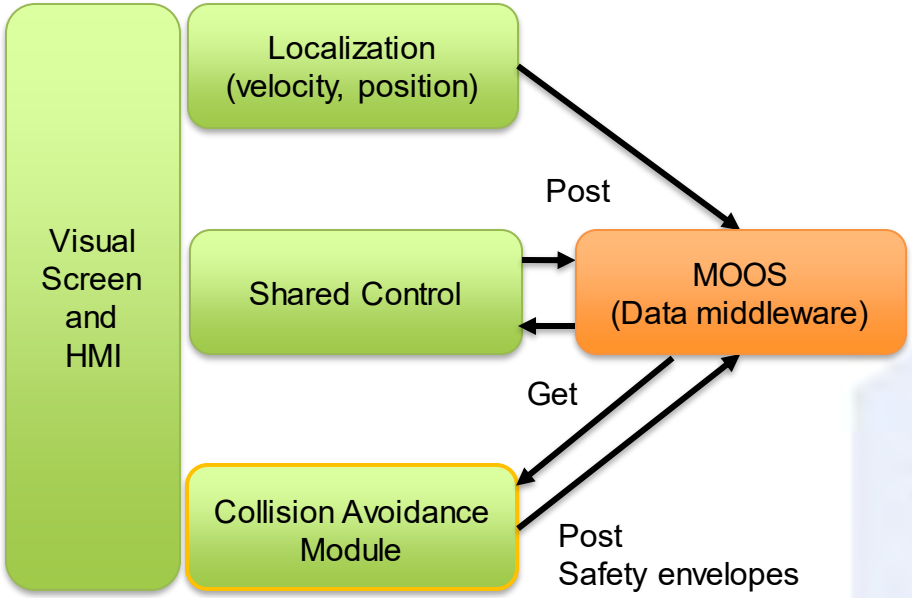
Laboratory setup

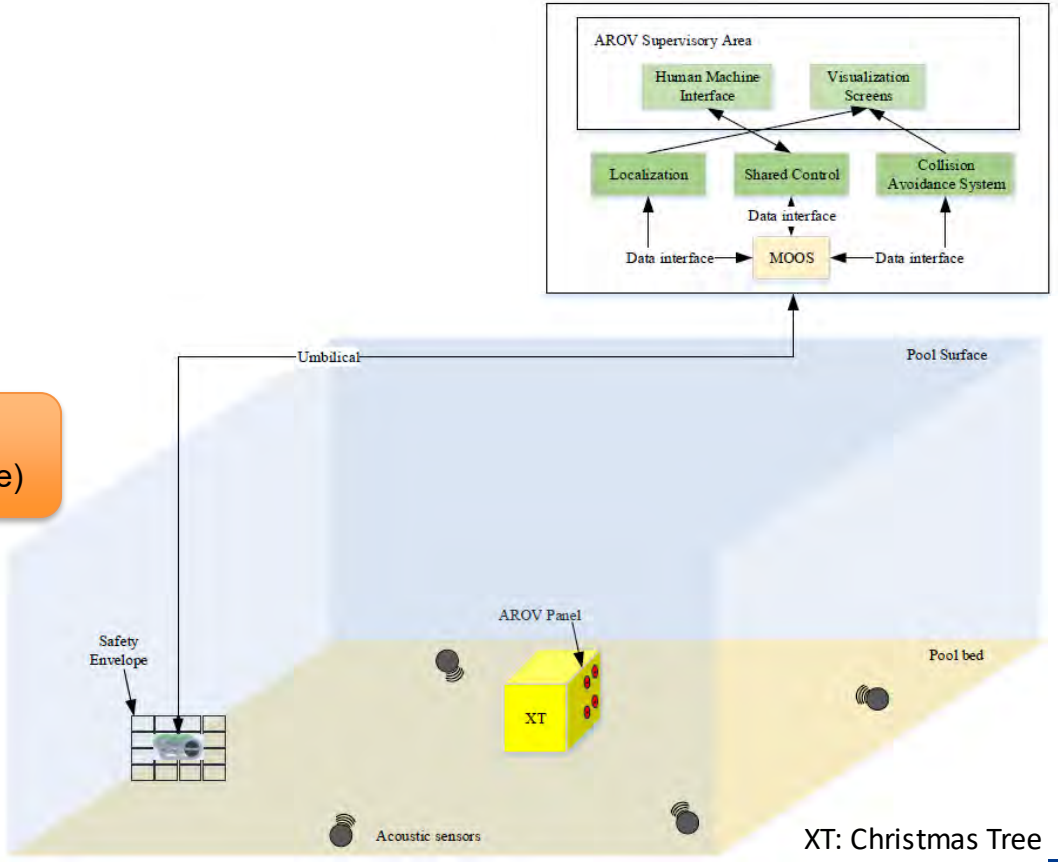




NTNU

Laboratory setup



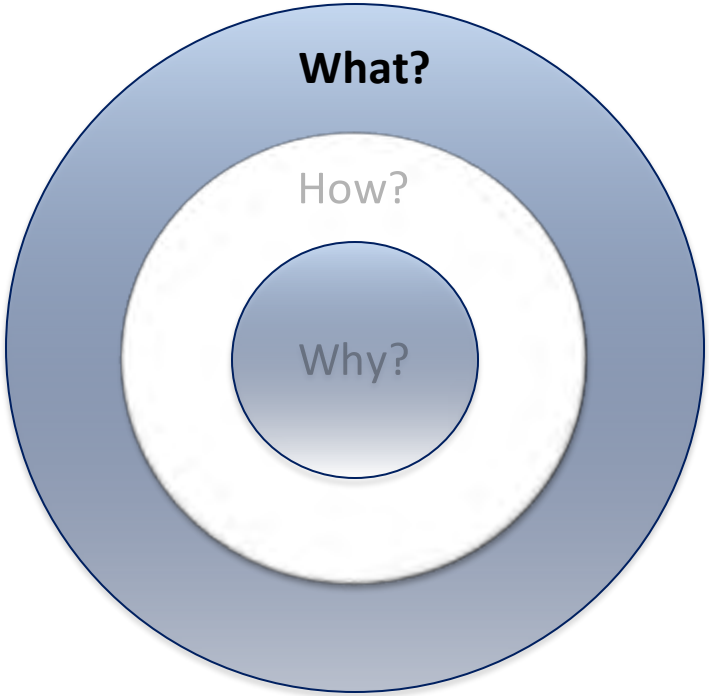


XT: Christmas Tree

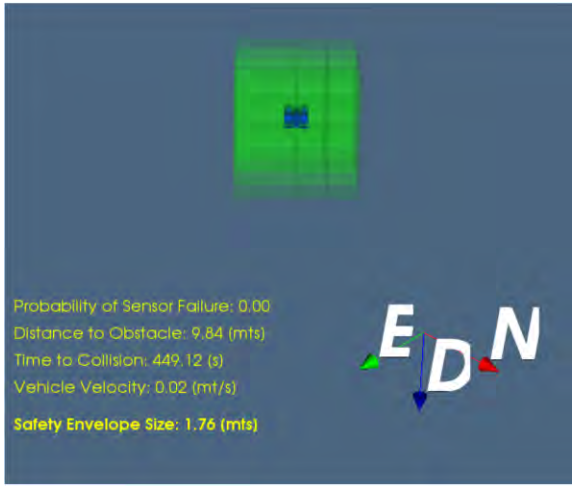
Newman, P. 2006. MOOS -Mission Orientated Operating Suite. Tech. Rep. OE2003-07. MIT Department of Ocean Engineering, Cambridge 2003.

Outline

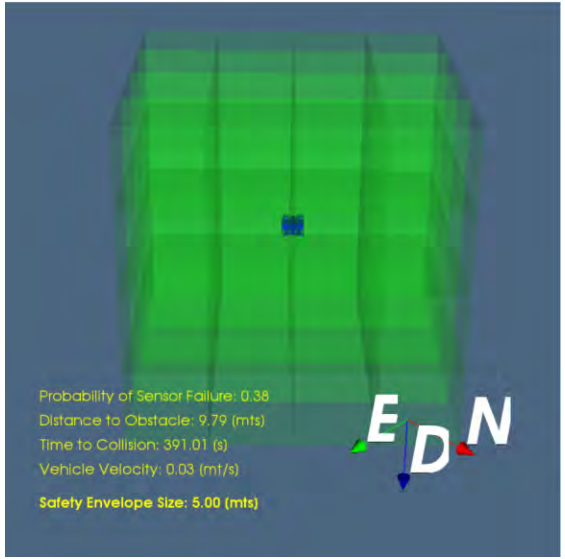
- » Background
- » Methods
- » Laboratory setup
- » **Results**
- » **Summary and future work**



Results



Data point	VV (m/s)	PASF	TTC (s)	Size of safety envelope (m)
1	0.02	0	449.12	1.76
2	0.24	0	22.12	2.49
3	0.63	0	16.52	5.00
4	0.03	0.38	391.01	5.00
5	0.25	0	18.52	2.58
6	0.20	0.12	12.69	1.83
7	0.33	0.25	5.68	3.68
8	0.36	0.25	10.56	4.11



Summary

- Proof-of-concept dynamic safety envelopes
- Proposed and tested a fuzzy inference system with three inputs
- Visualization of obstacles in an uncertain environment – digital twin
- May support the vehicle and the human supervisor in making mission critical decision

Lessons learned

Active sensors vs. passive sensors

Safety Envelopes are vehicle specific

A world visualization is important

Implementing online risk models is **Hard**

Future work

- Integrating with the subsea traffic rules module
  - From suggestion to action
- Extend the work to other underwater vehicle types
- Additional risk factors as an input to the fuzzy inference system

Oceanographic Systems Lab, Woods Hole Oceanographic Institution

Thank you for your attention!

Southampton
Management School

UNIVERSITY OF
Southampton

From autonomous underwater vehicles to unmaned marine surface vehicles: Reflections on risk models and expert judgment elicitations

Dr Mario P. Brito
Centre for Risk Research
Southampton Business School

Autonomous Underwater Vehicles and the Risk of vehicle Loss

- Autosub2 lost under the Fimbul Sea Glacier, Antarctica, 2005
- Two Hugin 6000s lost under the Wendell sea Glacier, 2019. The team was able to recover one of the AUVs. The second was permanently lost causing the end of the expedition

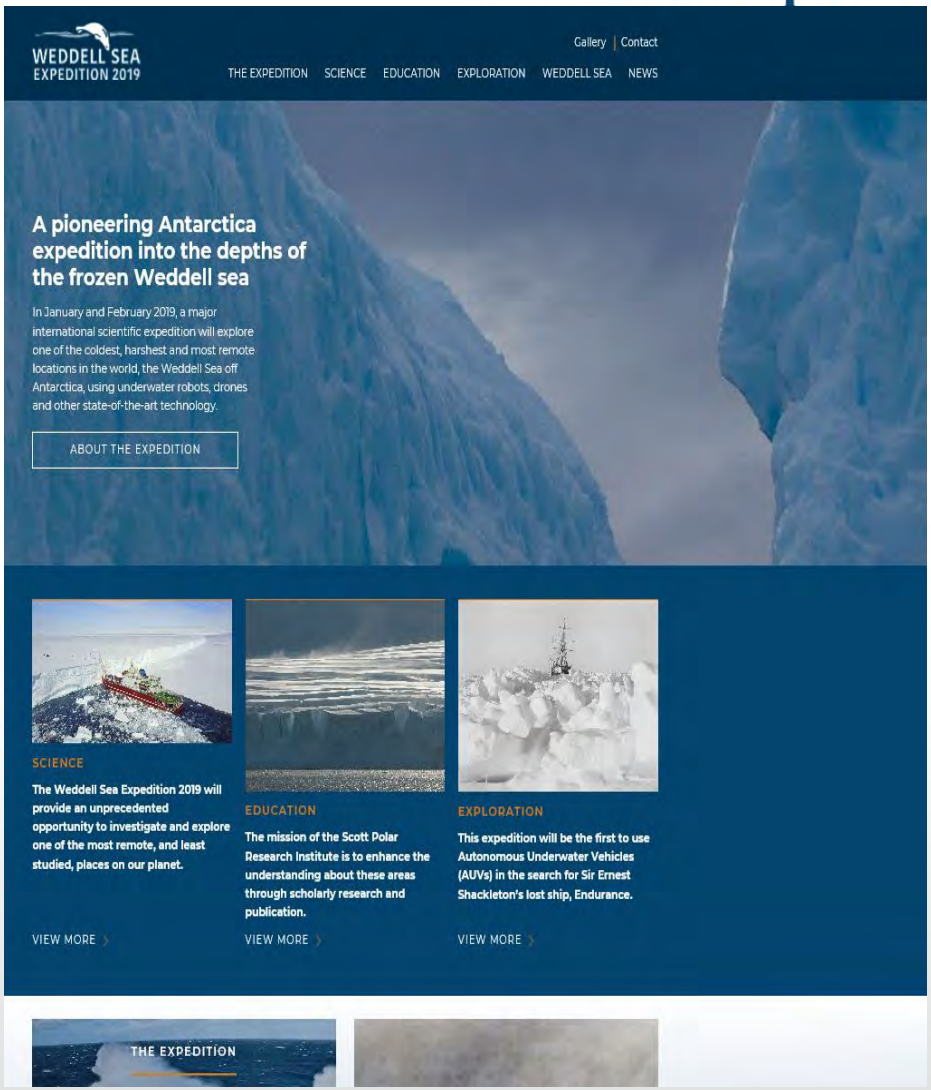
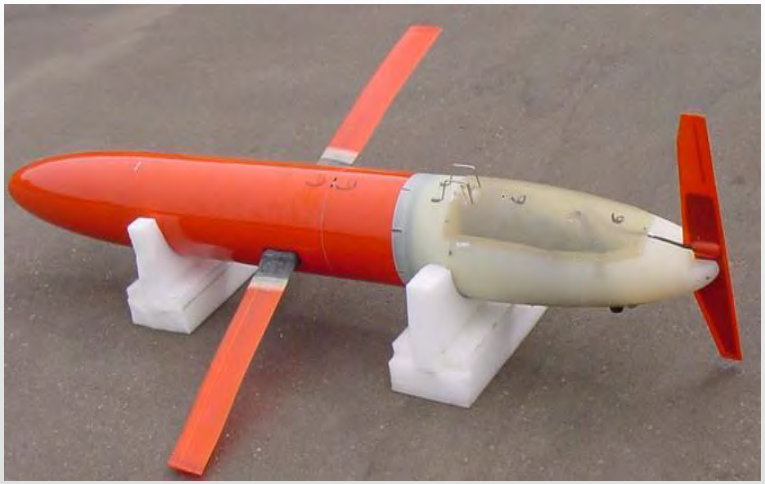


Image from the Wendell Sea Expedition webpage https://weddellseaexpedition.org/ Accessed 23/04/2019

Case study 1: Availability of significant amount of data

FP7 GROOM and SCRIPPS ocean glider reliability analysis



Non developers risk study:- FP7 Glider for Research, Ocean Observation and Science

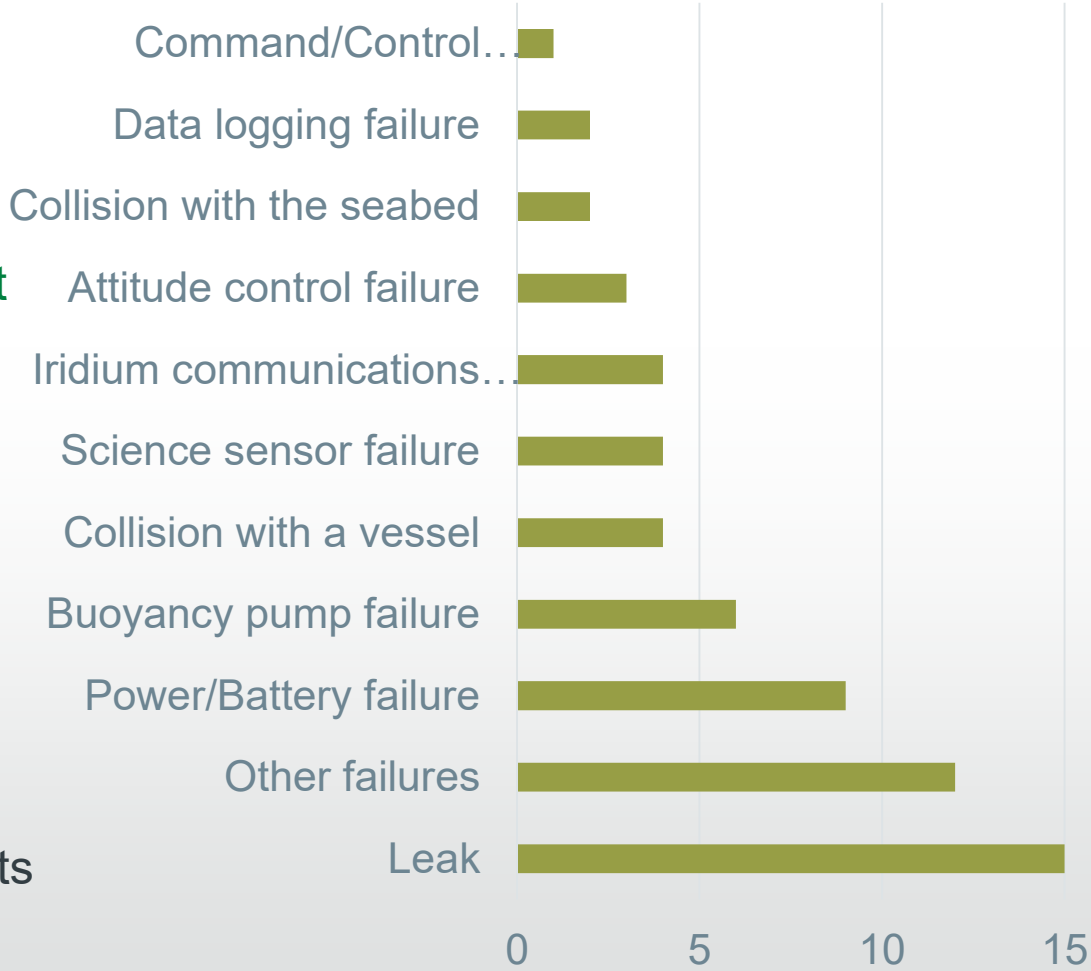
Survival analysis

The premature mission abort are 'censored'. They are included in each interval up to their last recorded age, but not counted as deaths.

The Kaplan Meier non-parametric estimator:

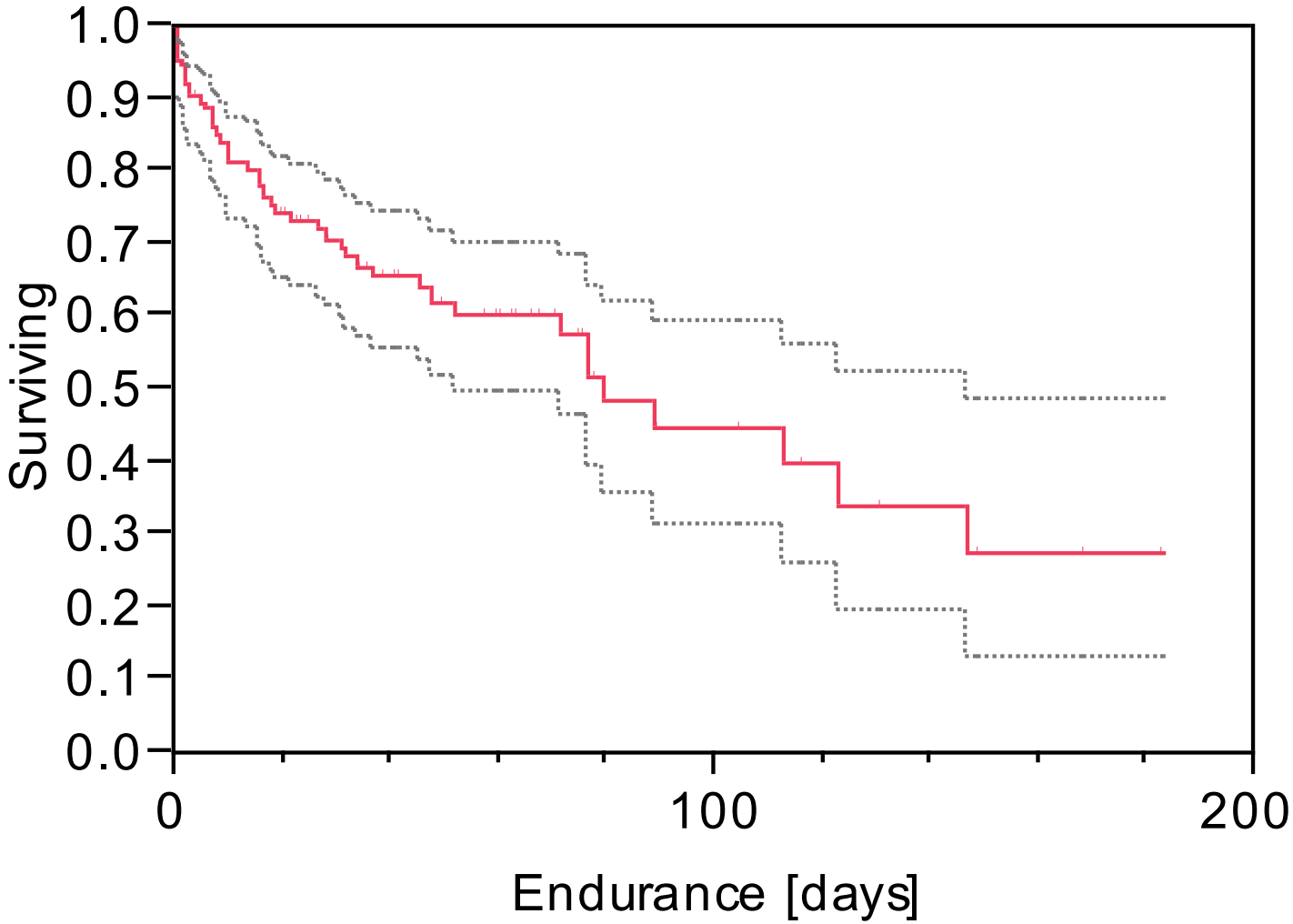
$$\hat{S}(t) = \prod_{t_i < t} \frac{n_i - d_i}{n_i}$$

n_i is the number of missions at risk, and d_i the number of aborts in each interval.



Brito, M. P., Smeed, D. A., & Griffiths, G., 2014. Underwater glider reliability and implications for survey design. Journal of Atmospheric and Oceanic Technology, 31(12), 2858-2870.

Survival analysis: Non developers

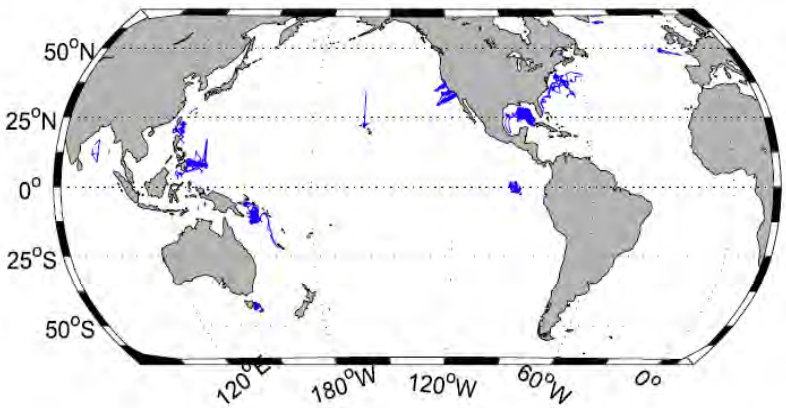


Kaplan Meier survival. In red the median, in grey the 5% and 95% confidence limit. **S(90 days) = 0.43**.

Southampton Management School

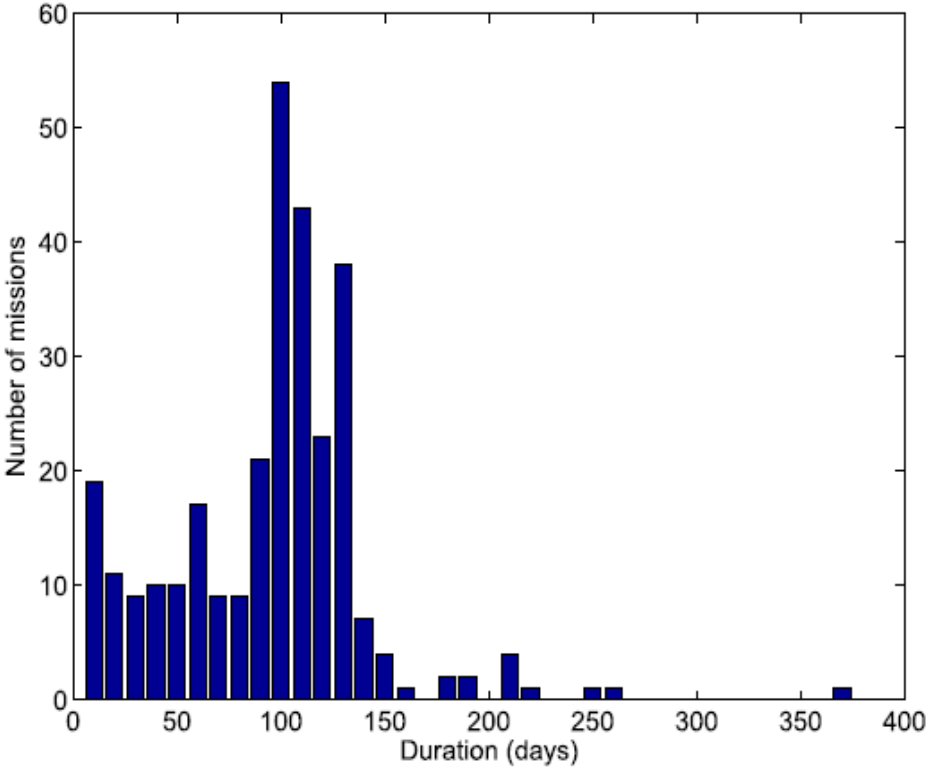
UNIVERSITY OF Southampton

Developers risk profile



Trajectories of completed missions by Spray underwater gliders since September 2004. Adapted from Rudnick et al (2016). 297 missions

Spray Underwater Glider Operations



Histogram of duration of Spray glider missions in bins every 10 days, with the first bin centered at 10 days. Adapted from Rudnick et al (2016). **S(100 days) = 0.83**.

"We were motivated by the rather grim analysis of Brito et al. (2014) to write this paper, as we believe that experienced glider operators do achieve their scientific objectives."
Rudnick et al (2016) pp. 1121.

Rudnick, D. L., R. Davis, and J. T. Sherman, 2016: Spray underwater glider operations. J. Atmos. Oceanic Technol., 33, 1113–1122,

Case study 1: Limitations and Future directions

- The effect of possible co-variates is not clear.
  - Mission depth
  - Pre-mission tests results
- The efficiency of mitigation is not captured analytically
  - How can we assess if the planned mitigation through fault correction is effective
- Anomaly detection

Dearden, R. and Ernits, J. 2013. Automated Fault Diagnosis for an Autonomous Underwater Vehicle," in IEEE Journal of Oceanic Engineering, 38, 3, pp. 484-499.
Brito, M. and Griffiths, G. 2018. Updating autonomous underwater vehicle risk based on the effectiveness of failure prevention and correction. Journal of Atmospheric and Oceanic Technology, 35, 797–808.

Southampton Management School

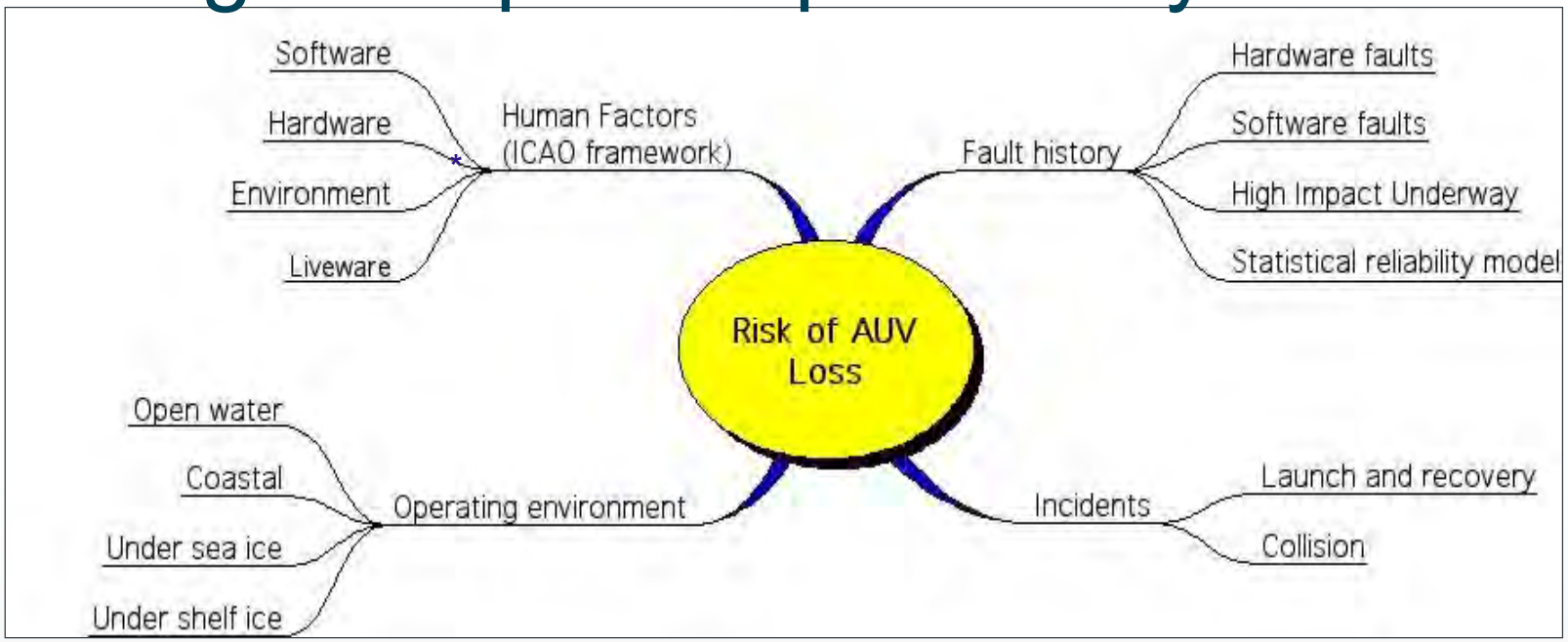
UNIVERSITY OF Southampton

Case study 2: A Modicum of experimental data and significant expert knowledge

Autosub 3 under ice programme

Natural Environment Research Council, Oceans 2025 Programme

How might we predict probability of loss?



Part A - Gather fault history, document human error and all incidents with the AUV

Part B - Set out the key features and risks of the operating environment

We postulated that combining Parts A and B could not be done through scientific methods.

* Estimated as cause of ~60% of US military UAV faults/incidents Tvaryanas et al. (2005)

Autosub Fault and Incident History

First two missions, *Discovery* 295T, July 2005.

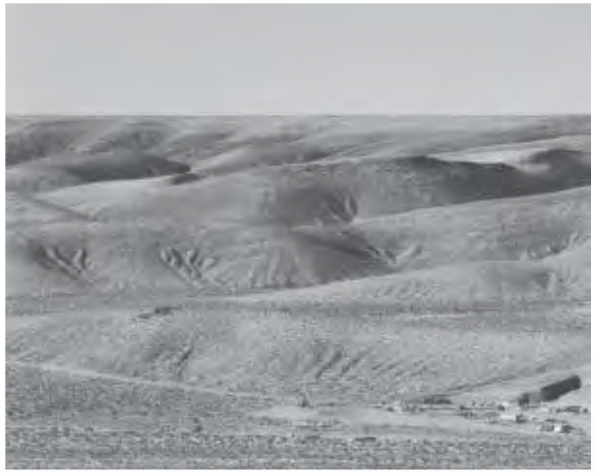
No.	Distance (km)	Fault/incident description
384	1.5	aborted (to surface) due to network failure. (Much) later tests showed general problem with the harnesses (bad crimp joints).
		Loop of recovery line came out from storage slot, long enough to tangle propeller.
385	15.2	Autosub headed off in an uncontrolled way, due to a side effect of the removal of the upwards-looking ADCP.

From its first mission in July 2005 to April 2007 Autosub3 suffered 63 faults or incidents on 29 missions, another 10 missions were fault-free.

We cannot avoid the use of Expert Judgment!

- The use of expert judgment for formal risk assessment was first introduced by the US Government. The aim was to get a group of experts to agree on the best location for a Nuclear Waste repository Bonano et. al (1990).

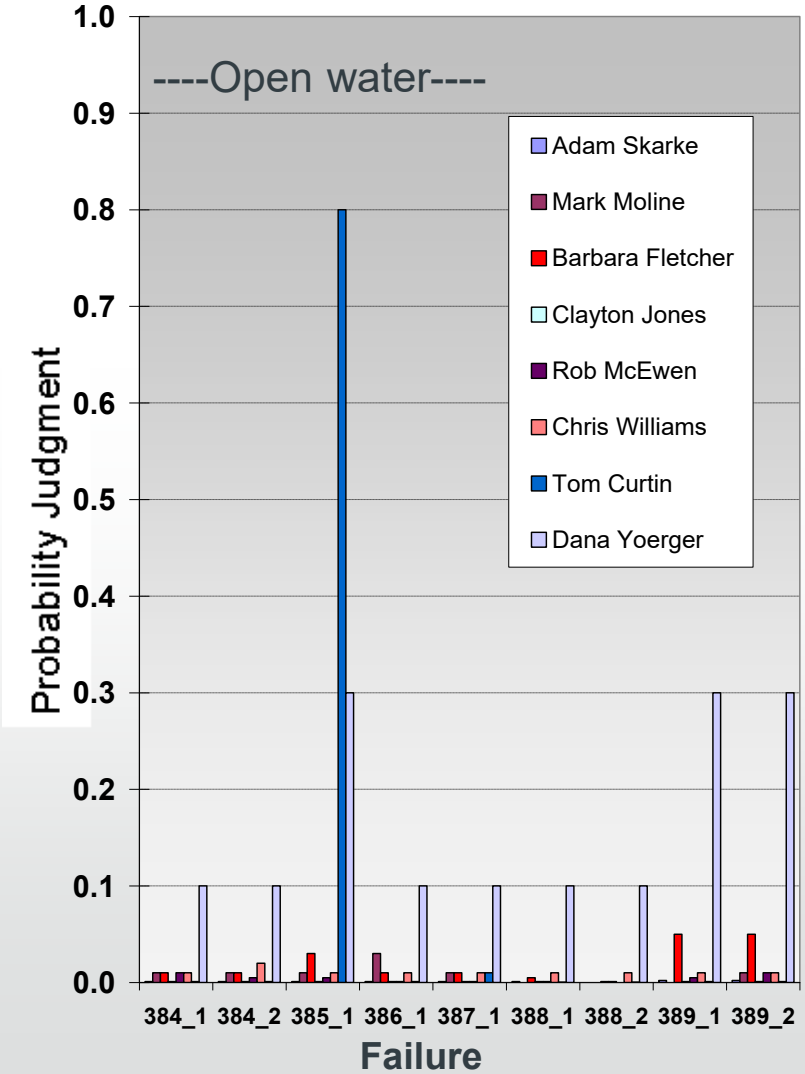
- The elicitation of formal expert judgment is a well established scientific field with crosses areas of psychology and statistics.

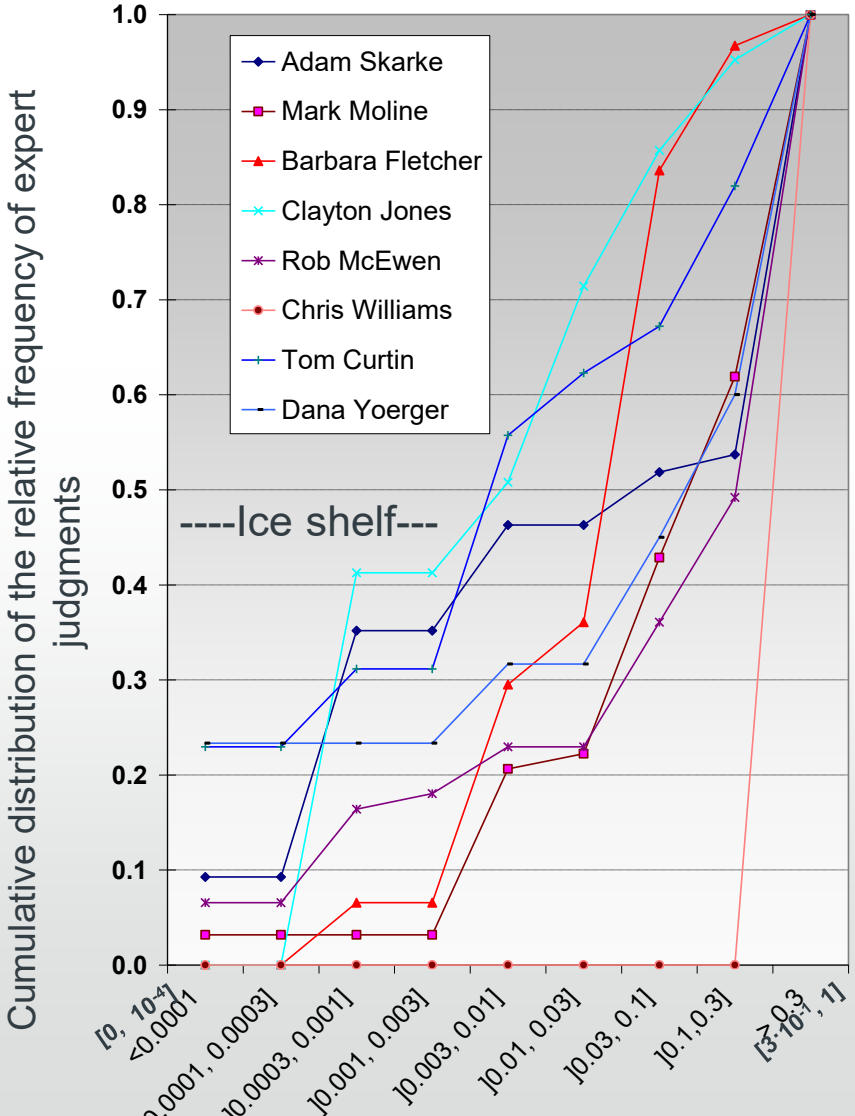


The photo captures the Yucca Mountain site, Nevada.

Bonano E.J. et. al (1990). Elicitation and use of expert judgment in Performance Assessment for High-Level Radioactive Waste Repositories. U.S. Nuclear Regulatory Commission, NUREG/CR-5411, 80 pp.

Analysis of Expert Judgment on the Probability of Autosub3 Loss: Graphical methods





Expert Judgment Aggregation

- Expert judgment aggregation methods can be either mathematical or behavioural:
  - Mathematical aggregation.
  - Behavioural aggregation methods.
- The Linear opinion pool and the logarithmic opinion pool were studied for suitability.
- The log opinion pool. The number of vetoes varied according to the environment, 35 (55% of all judgments) open water, coastal waters 27 (42%), sea ice and ice shelf 21 (33% of all judgments).

Linear pool

$$P(\text{loss}\,|\,\text{fault}) = \frac{1}{\sum_{i=1}^{n} w_i} \sum_{i=1}^{n} w_i P_i(\text{loss}\,|\,\text{fault})$$

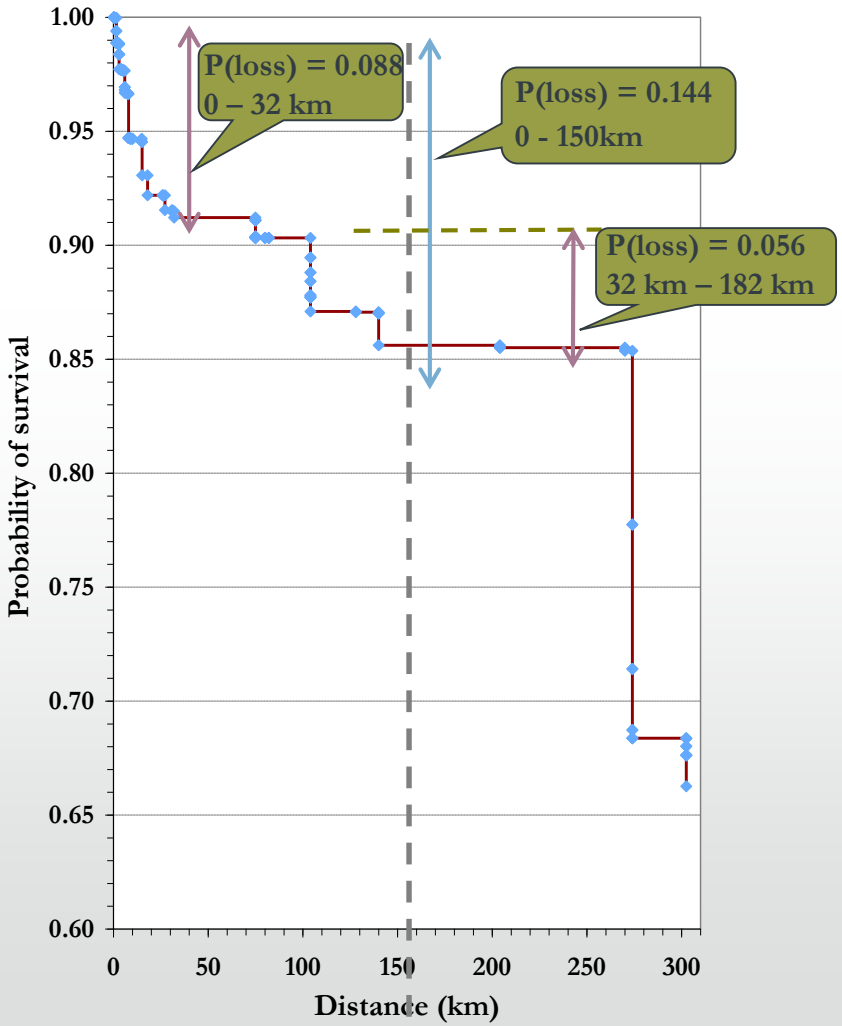
Log pool

$$P(\text{loss}\,|\,\text{fault}) = \left[\sqrt[n]{\prod_{i=1}^{n} p_i^{w_i}}\,(\text{loss}\,|\,\text{fault})\right]^{\frac{n}{\sum_{i=1}^{n} w_i}}$$

Given the number of vetoes obtained by the log. opinion pool, it was decided to use the linear opinion pool.

Autosub3 survival with distance: Non parametric methods

Autosub3 survival for ice shelf



Statistical survival methods are divided in two main groups, non-parametric and parametric methods.

$$\hat{S}(r) = \prod_{r_i < r} 1 - \left(\frac{1}{n_i}\right) P(loss_i)$$

Risk factor ni	Fault	Dist. (km)	P(loss)	Prob. Surv.	Cumulative
73	413	0.2	0	1	1
72	388_1	0.5	0.534	0.993	0.993
71	388_2	0.5	0.538	0.992	0.985
70	384_1	1.5	0.839	0.988	0.973
69	384_2	1.5	0.713	0.990	0.963

The effectiveness of using a monitoring distance can be quantified using the conditional probability function (Griffiths et. al, 2003).

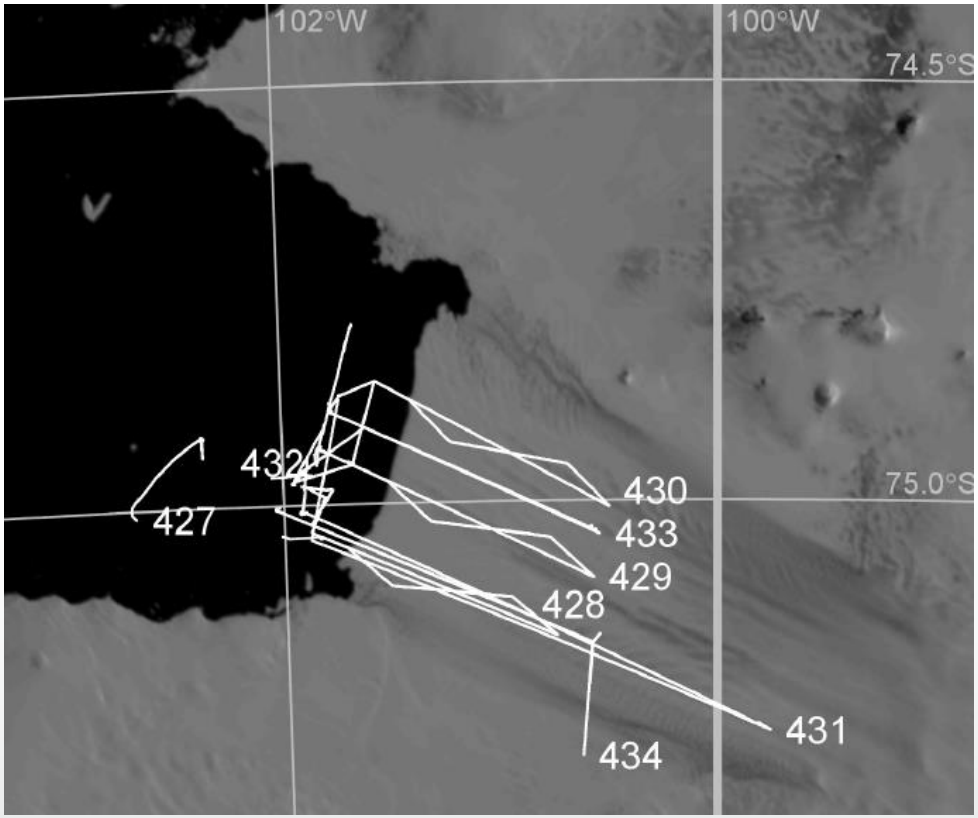
$$P(X < x \mid X > y) = \frac{F(x) - F(y)}{1 - F(y)}$$

F(·): Cumulative probability of failure

Southampton Management School

UNIVERSITY OF Southampton

Pine Island Glacier – Mission goal

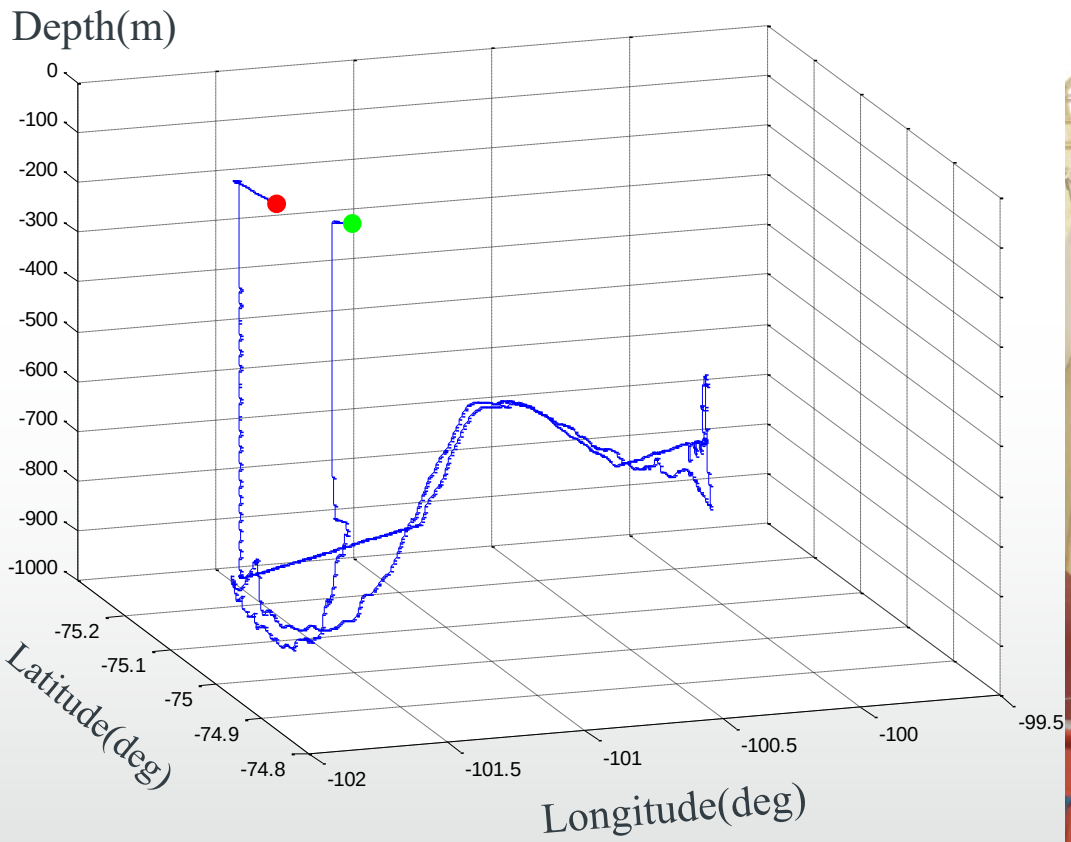


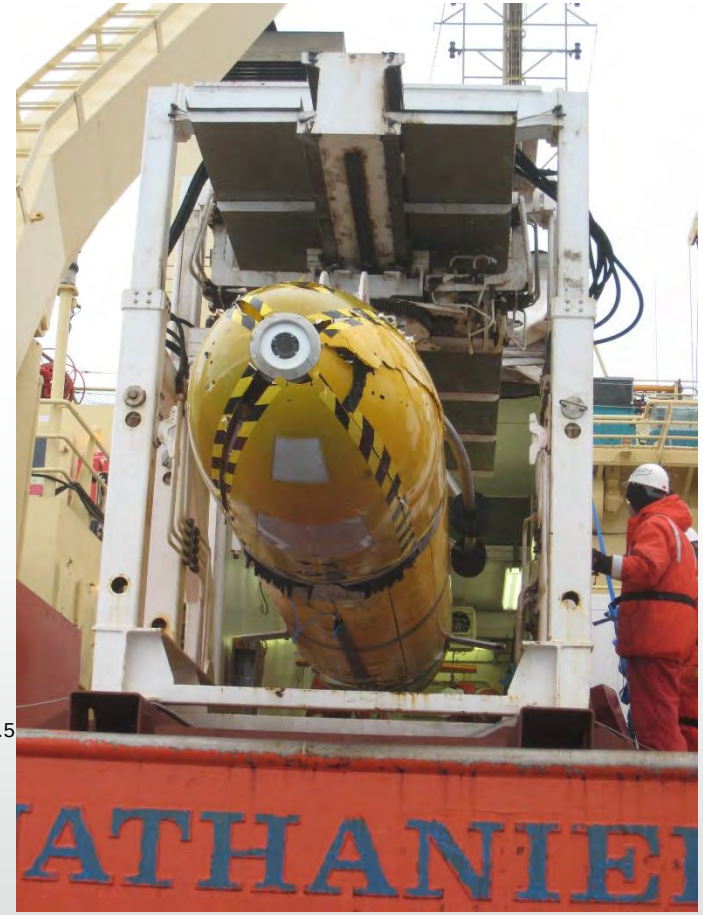
The tracks of all of the 8 Autosub3 missions carried out in the vicinity of the PIG in January 2009, superimposed on a recent MODIS satellite image. From McPhail et al. 2009.

- The main goal of the campaign was to gather data that would help determine how the warm Circumpolar Deep Water (CDW) gets beneath the glacier and how it determines the rate at which the glacier melts. Three subsidiary objectives had to be met:
  - To map the seabed beneath the glacier;
  - To map the underside of the glacier;
  - To determine where and how heat is transferred from the inflowing CDW to the outflowing ice-ocean boundary layer.

McPhail, et al. 2009. Exploring beneath the PIG Ice Shelf with the Autosub3 AUV. Online: http://eprints.soton.ac.uk/66414/01/Oceans2009_Autosub3_McPhail.pdf.

Pine Island Glacier – Campaign analysis





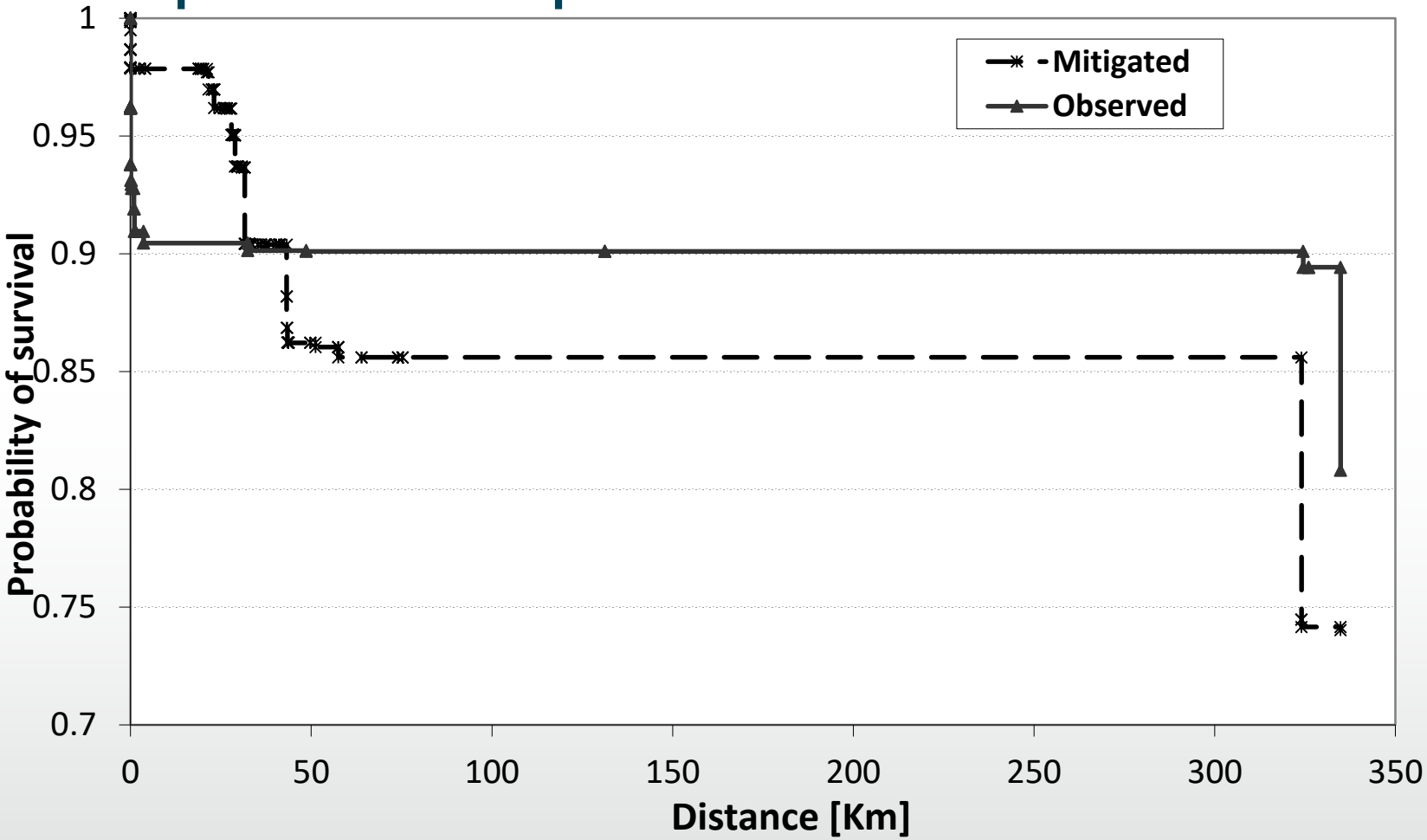
Overview of Autosub3 mission 431. The starting point is in green, and the ending point is in red.

Photo courtesy of Mr. James Ferguson. DRDC/ISE deployment team, 2010.

Southampton Management School

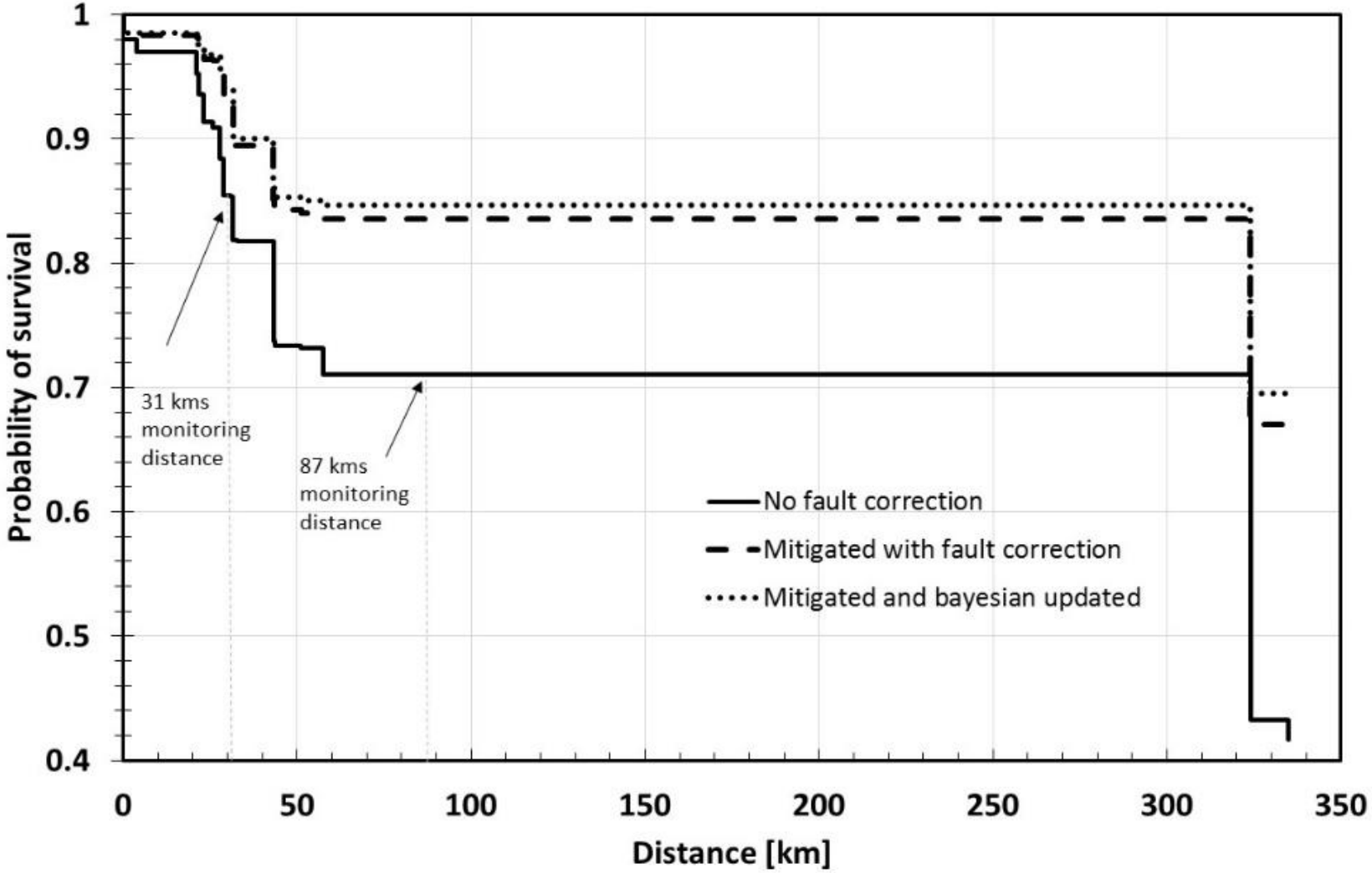
UNIVERSITY OF Southampton

ISE Explorer risk profile



Brito, MP, Griffiths, G; Ferguson, J., et al. 2012 A Behavioral probabilistic risk assessment framework for managing autonomous underwater vehicle deployments. Journal of Atmospheric and Oceanic Technology, 29 (11). 1689-1703.

Posterior Survival distribution



Brito, M.P. and G. Griffiths, 2018: Updating Autonomous Underwater Vehicle Risk Based on the Effectiveness of Failure Prevention and Correction. J. Atmos. Oceanic Technol., 35, 797–808

Case study 2: Limitations and Future directions

- The effect of possible co-variates is not clear.
  - Mission depth
  - New technology
- The reliability of expert judgments needs further exploration
  - Unlike other subject areas where expert judgment is used for AUVs the there is the possibility of obtaining post mission data to enable to test for expert's reliability
- Explore whether or not AI can replace experts

Southampton
Management School

UNIVERSITY OF
Southampton

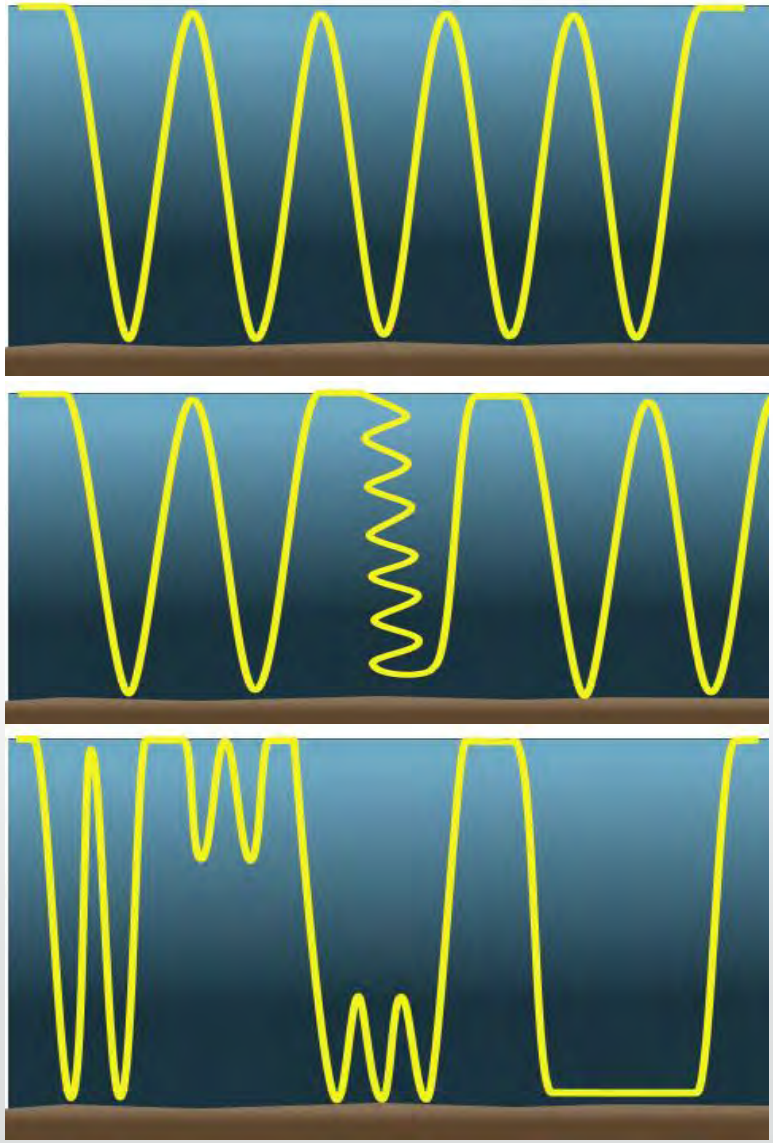
Case study 3: No operational data availability

KTP Enabling safe operations of autonomous ships and BRIDGES

Work package 7 Systems Integration and reliability consists of 4 tasks:

1. Task 7.1 Reliability modelling and analysis of the D and UD vehicles. UoS, ALSEAMAR-ALCEN and ENITECH. M13-M19 (May '16 – Nov '16)
2. Task 7.2 Design reliability tests for the D and UD Explorer. NERC, ALSEAMAR-ALCEN and ENITECH. M20-M24 (Dec. '16 – April '17)
3. Task 7.3 Implement reliability quantification tests in D and UD gliders. NERC and ALSEAMAR-ALCEN. M36-M42 (April '18 – Oct '18)
4. Task 7.4 Platform systems integration. ALSEAMAR-ALCEN. M30-M36

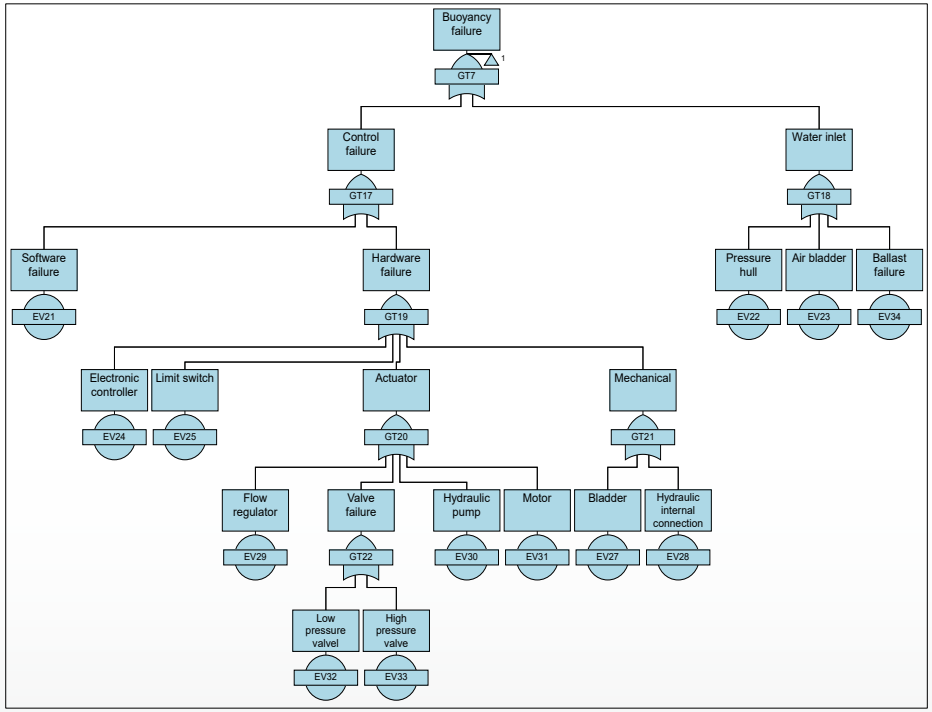
Operation profiles



Southampton Management School

Horizon 2020 - BRIDGES

UNIVERSITY OF Southampton



Fault tree for Buoyancy failure

- Training was provided on different types of heuristics
- Calibration was conducted by giving the experts seed questions
  - What is the probability of Autosub6000 GPS failure?
  - What is the probability of battery failure?
  - What is the probability of stern plane failure?
- The experts were told that the vehicle had conducted 68 missions and covered a total of 3650km

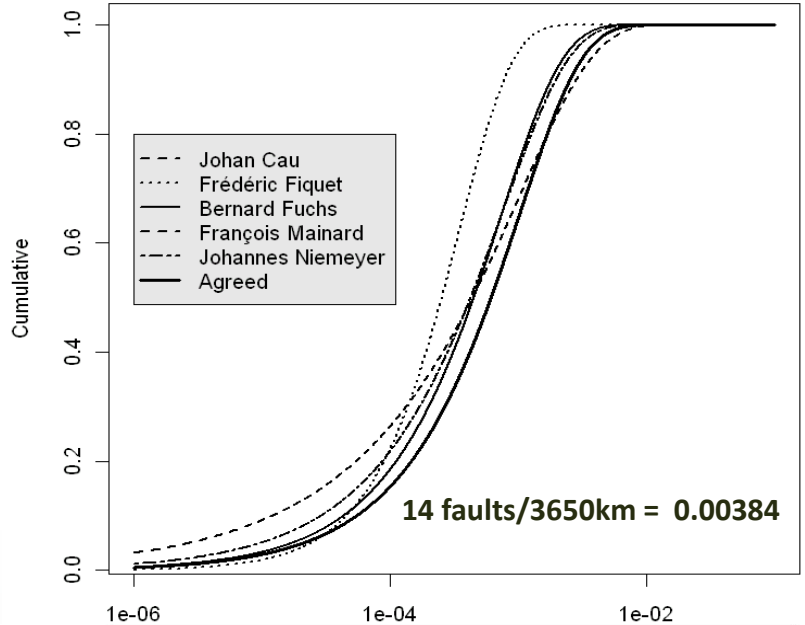
83 individual failure modes were identified.

Brito, M.P. (2015) Reliability Case Notes No. 8. Risk and reliability analysis of Autosub 6000 autonomous underwater vehicle. National Oceanography Centre Research and Consultancy Report, 50, 79pp.
Online: http://eprints.soton.ac.uk/381863/ (confidential)

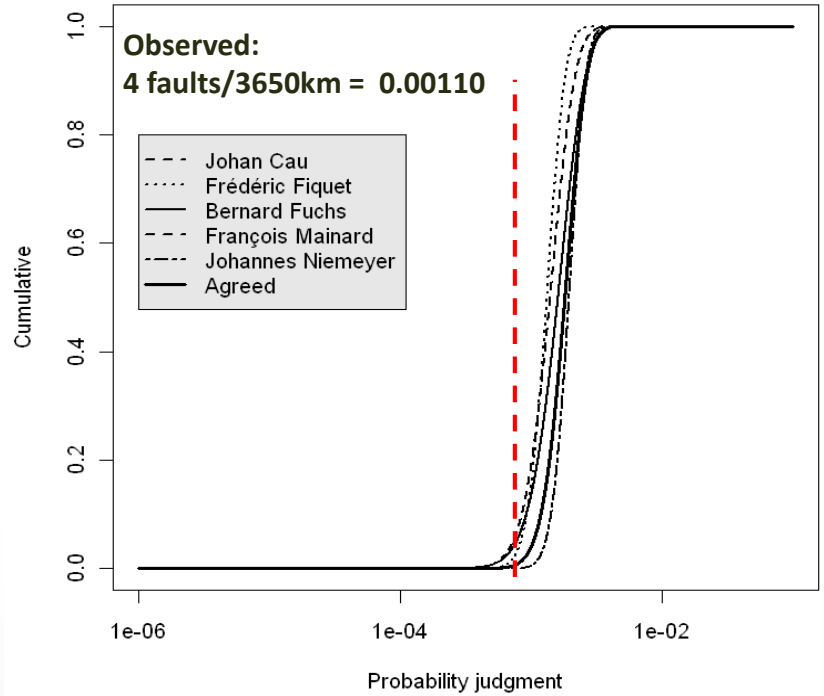
Southampton Management School

Training: Seed questions

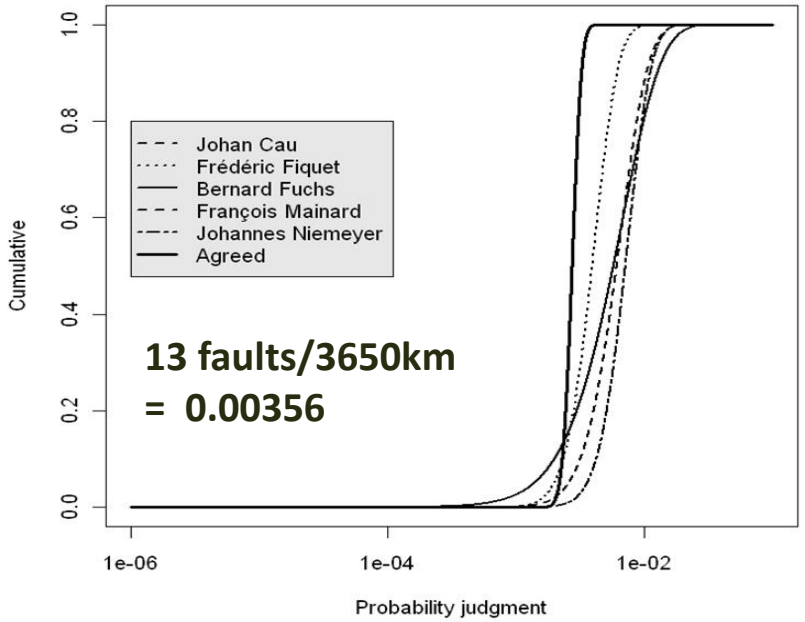
UNIVERSITY OF Southampton



Probability of *Autosub6000* GPS failure



Probability of *Autosub6000* Stern plane actuator failure



Probability of *Autosub6000* Battery failure

	LQ	M	UQ
JC	0.0011	0.0013	0.0019
FF	0.0011	0.0013	0.0016
BF	0.0011	0.00164	0.00219
F-XDM	0.0017	0.0019	0.0024
JN	0.00137	0.00192	0.00219
Agreed	0.0012	0.0015	0.002

Existing acceleration life models

Acceleration Model	Type of Relationship
Arrhenius	Exponential
Inverse Power Law	Power
Coffin-Manson Relationship	Power
Eyring's Model	Exponential
Log-Linear Relationship	Logarithmic
Generalized Eyring	Combination

Not suitable!

Buoyancy control accelerated test plan

1. Connect the pump to a sealed contained with an initial pressure of 0.8 bars absolute (≈200mbar less than the atmospheric pressure) which will simulate the pressure hull of the vehicle.
2. Connect a flowmeter on the pump output and cycle the pump in order to inflate (or extract from the sealed container) a volume of 10L of air at each cycle. During each cycle, the sealed container internal pressure will drop from 0.8bar absolute to about 0.5bars absolute. Between each cycle, this pressure should be adjusted again to 0.8bars absolute.

Air Ballast System Estimated Test Programme Costs :	
Item	Description
Test Pieces :	Mini Vacuum Pump (1 off?)
Test Rigs :	a. Vacuum Chamber b. Setting Vacuum pump, filter and controls c. Power supply, control and sensors d. Enclosures
Facilities :	Cycle Testing – 20 days

Courtesy of Dr. Michael Field, BRIDGES

Case study 3: Limitations and Future directions

- It is difficult to implement expert judgment elicitations due to lack of expertise
- Failure mechanisms are not understood, there is a need for multi-stress models
- For marine unmanned marine surface vehicles it is easier to implement data collection processes for condition monitoring systems

Assured and Composable Safety in Connected Autonomous Vehicles

John S. Baras

Institute for Systems Research

University of Maryland

Workshop on Risk Analysis for Autonomous Vehicles: Issues and Future Directions
April 26, 2019
University of Maryland
College Park, MD, USA

Outline

- Car Passing Problem
- Path Planning: Safety and Verification
- Path Planning: Spatial and Temporal Specifications
- Current and Future Work: Model-Based Systems Engineering for Large Automated Transportation Networks

Car Passing Problem

Stochastic Control for the Car Overtake Problem [1]

Our solution

Partially stochastic control formulation

Probability space constructed by Car 1 is based on joint distribution of its measurements and initial states of Cars

Numerical method to find the probability of Car 1 colliding with Car 2 and Car 3

Control algorithm minimizing the probability of collision

- At time k, the information available to Car 1 before taking its action is:

$$\mathcal{I}_1(k) = \{x_1(n), v_1(n), y_1(n), \theta_1(n), z_1(n), z_2(n)\}_{n=0}^{n=k} \cup \{z_3(n), z_4(n)\}_{n=0}^{n=k-1}.$$

- At time k, after the three cars have taken their respective actions, the information available to Car 1 is:

$$\mathcal{I}_2(k) = \{x_1(n), v_1(n), y_1(n), \theta_1(n), z_1(n), z_2(n)\}_{n=0}^{n=k} \cup \{z_3(n), z_4(n)\}_{n=0}^{n=k}.$$

1 A. Raghavan, J. Wei, J. S. Baras, K. H. Johansson, "Stochastic Control Formulation of The Car Overtake Problem", *Proceedings 15th IFAC Symposium on Control in Transportation Systems (CTS 2018)* , University of Genova, Savona Campus, Italy, June 2018

Problem Formulation

- Car 1 modeled as **unicycle**, Car 2 and Car 3 are considered as **point masses**:

$$
\begin{aligned}
x_1(k+1) &= x_1(k) + v_1(k)\cos(\theta_1(k)),\\
y_1(k+1) &= y_1(k) + v_1(k)\sin(\theta_1(k)),\\
\theta_1(k+1) &= \theta_1(k) + \omega(k).
\end{aligned}
$$

$$
\begin{aligned}
x_2(k+1) &= x_2(k) + v_2(k), \qquad & x_3(k+1) &= x_3(k) + v_3(k),\\
y_2(k) &= \frac{d}{2},\ \theta_2(k) = 0. & y_3(k) &= \frac{3d}{2},\ \theta_3(k) = 0.
\end{aligned}
$$

- **Measurements**:

$$
\begin{aligned}
z_1(k) &= x_2(k) - x_1(k) + W_1(k),\ k \geq 0,\\
z_2(k) &= x_3(k) - x_1(k) + W_2(k),\ k \geq 0.
\end{aligned}
$$

$$
\begin{aligned}
z_3(k) &= v_2(k) - v_1(k) + W_3(k),\ k \geq 0,\\
z_4(k) &= v_3(k) - v_1(k) + W_4(k),\ k \geq 0.
\end{aligned}
$$

- $\{W_i(k)\}, i = 1,2,3,4$ are white independent Gaussian processes with zero mean and variance $\sigma^2{}_i(k)$.

The Logic of Overtaking

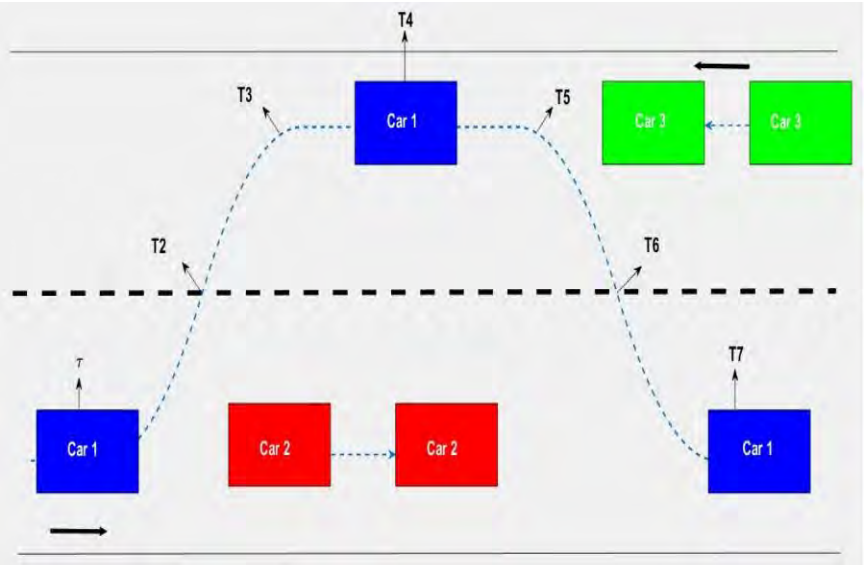
- The time taken by Car 1 to go from $y = \mathrm{d}/2$ to $y = d$, is

$$\Delta = \frac{1}{\omega_1} \arccos\left(1 - \frac{d\omega_1}{2v_1}\right)$$

- The trajectories are generated by the following sequence of control actions

$$\omega(k) = \omega_1,\ \tau \leq k < \tau + \Delta\ [T2],$$
$$\omega(k) = -\omega_1,\ \tau + \Delta\ [T2] \leq k < \tau + 2\Delta\ [T3],$$
$$\omega(k) = 0,\ \tau + 2\Delta\ [T3] \leq k < \tau + 2\Delta + t_1\ [T5],$$
$$\omega(k) = -\omega_1,\ \tau + 2\Delta + t_1\ [T5] \leq k < \tau + 3\Delta + t_1\ [T6],$$
$$\omega(k) = \omega_1,\ \tau + 3\Delta + t_1\ [T6] \leq k < \tau + 4\Delta + t_1\ [T7].$$

- Hence control Problem for Car 1:
  - Find decision time (τ),
  - Find overtake decision (D),
  - A triple (v_1, ω_1, t_1) which minimizes probability of collision with Car 2 and Car 3



Sample trajectory during overtake

Solution – Estimation and Decision Time

- Car 1 estimates the position and velocity of Cars 2 and Car 3 based on the information available $\mathcal{I}_1(k)$
- Similarly the position and velocity of Car 3 are estimated by Car 1
- **Decision Time** : distance based definition

$$\tau = \min_{k \geq 1}\{k : N \times L \leq \hat{x}_2(k) - x_1(k) \leq (N+1) \times L\},$$

- *N* a natural number; can be used to characterize behavior of Car 1 driver

  5 or 8 for passive driver, 1 or 2 for aggressive driver

Solution – Determination of Feasibility Conditions

Solution – Determination of Collision Conditions

Solution – Determination of Decision

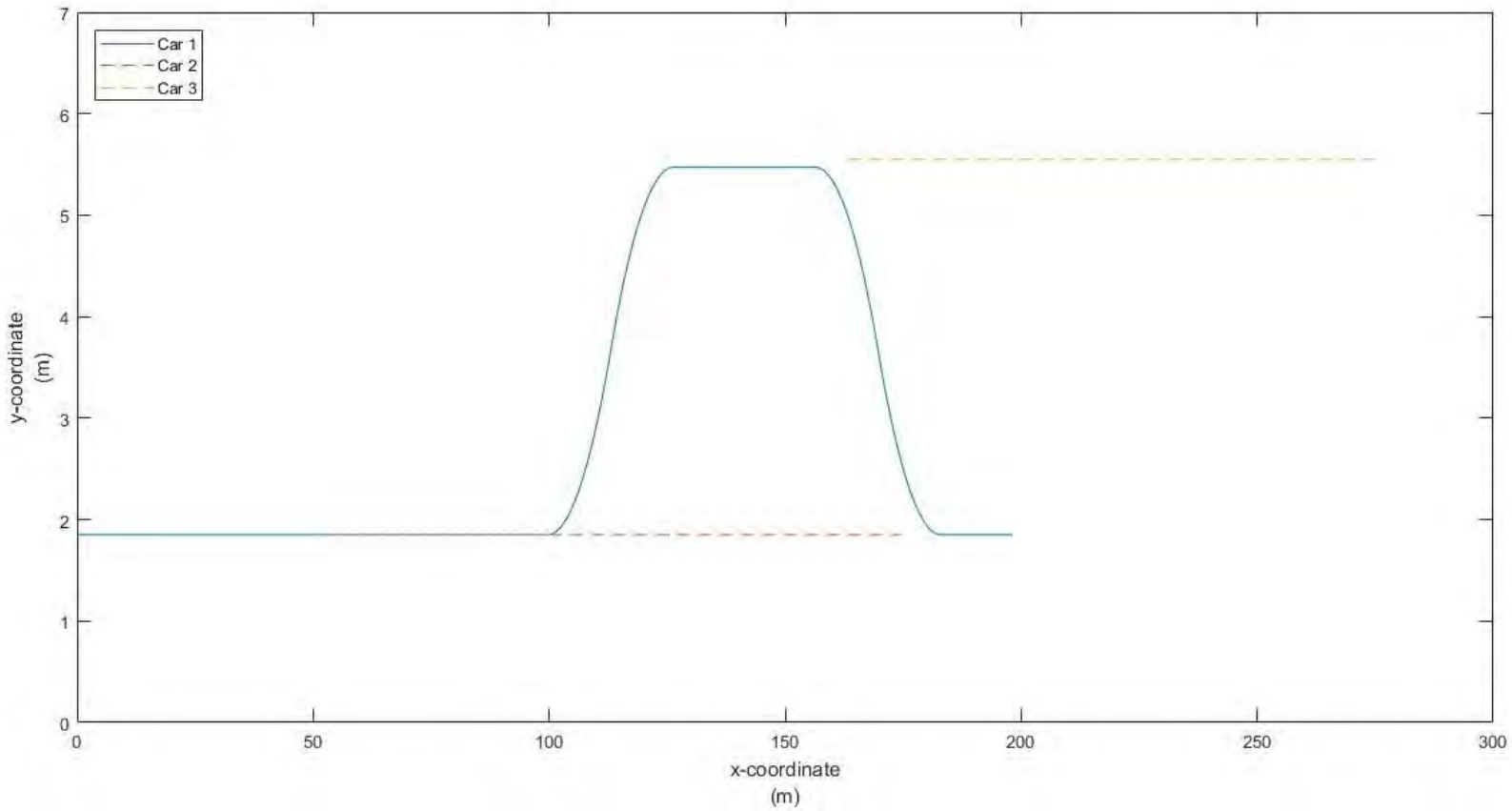
Simulation Setup

- $d = 3.7m, L = 1.5m, M = \bar{M} = 2$.
- Simulation Time step = 0.01 sec.
- If k is even, then $\sigma_1(k) = \sigma_2(k) = c_1$ and $\sigma_3(k) = \sigma_4(k) = 10 \times c_1$.
- If k is odd , then $\sigma_1(k) = \sigma_2(k) = 10 \times c_1$ and $\sigma_3(k) = \sigma_4(k) = c_1$.
- $T = 0.01$. Three values of N considered, $N = 8,5,2$.
- Three values of c_1 considered, $c_1 = 1, 0.5, 0.1$.
- $P^* = 0$ for all scenario's except for $(N = 5, c1 = 0.5)$. For that pair, $P^* = 0.0945$.
- $(N = 5, c1 = 0.5)$, the optimal triple was $(15m/s, 0.3rad/s, 2s)$.

Parameter	Value	Variance
$x_1(0)$	0m	0.001
$x_2(0)$	50m	0.001
$x_3(0)$	275m	0.001
$v_1(0)$	17m/s	-
$v_2(0)$	10m/s	-
$v_3(0)$	-9m/s	-

Parameter	Maximum	Minimum	Step size
v_1	30 m/s	8m/s	0.5
ω_1	0.7m/s	0.1rad/s	0.2
t_1	10s	2s	0.5

Simulation Results – Trajectory

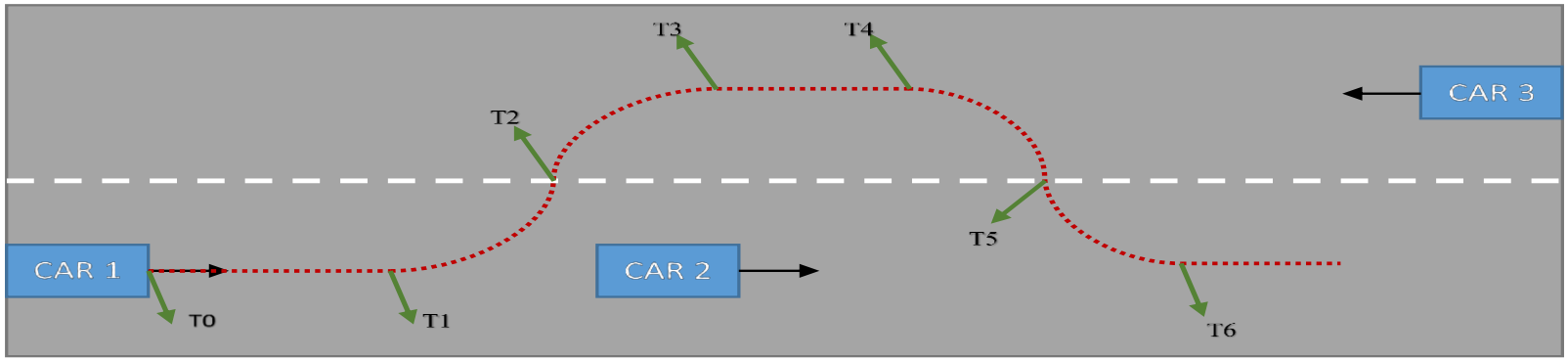


Conclusion and Future Work

- **Conclusion**:
  - Stochastic Control problem formulated for Car 1.
  - Probability of collision calculated based on the information available to Car 1.
  - Control action by Car 1 minimizing the maximum of the probability of collision with other two cars.
  - If Car 1 decided to overtake Car 2 at a farther distance, then probability of collision was lower.
  - Multi- Agent problem, solution relies only on probability space constructed by Car 1.
- **Future Work**:
  - Incorporate delay in information sharing between the vehicles.
  - Study of the problem with different levels of infrastructure (Car – Car communication, Car – Satellite – Car communication)
  - Current formulation Car 1 cannot return to original lane while overtaking. If Car 1 is given the freedom to return to the original lane without overtaking Car 2, what is the optimal time to do so ?

Model-Based Systems Engineering Approach [2]

Car passing trajectory

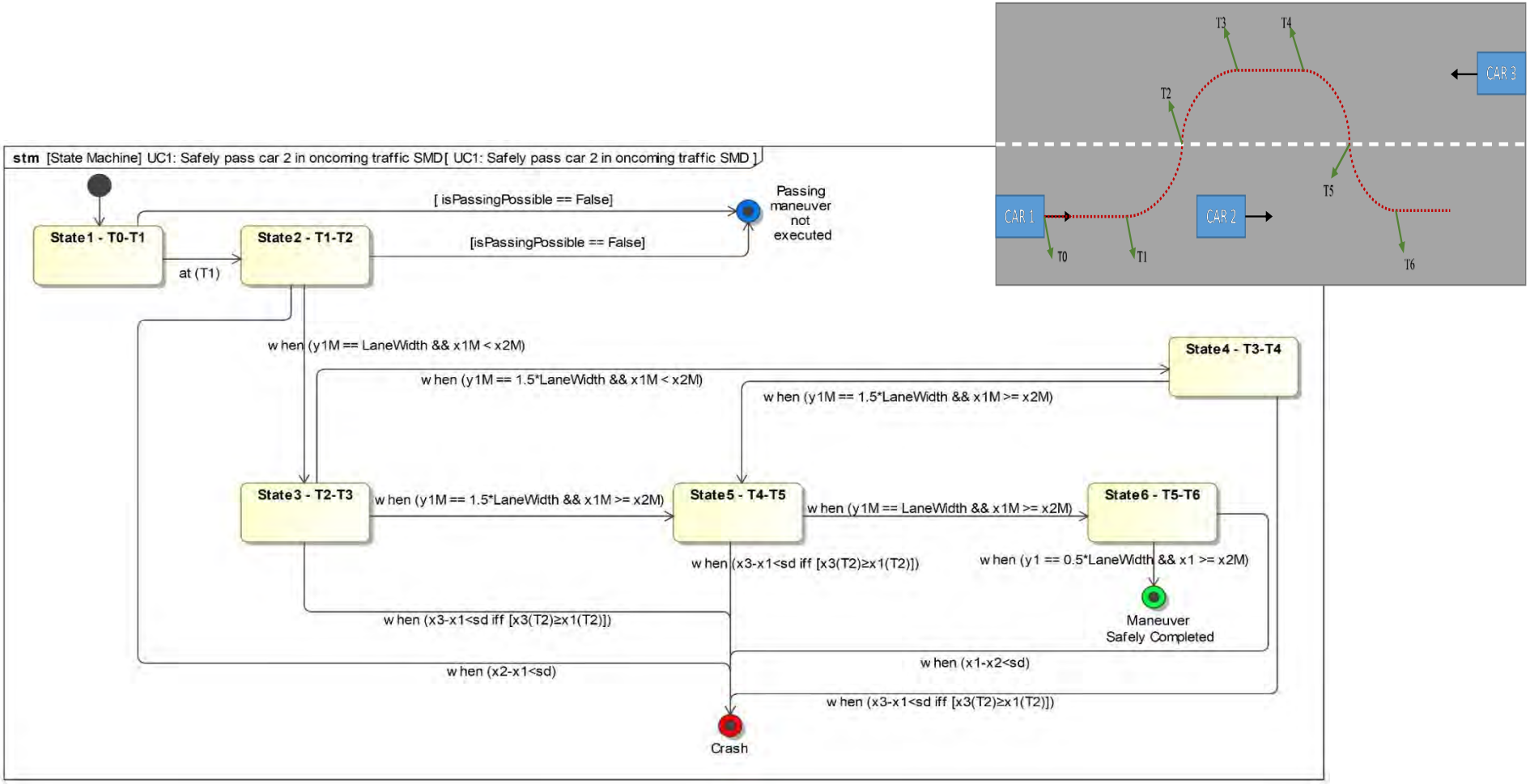


Car passing problem evaluation metrics

- Passing Decision Evaluation:
  - P(A): Probability of deciding to pass given that it is feasible to safely pass
  - P(B): Probability of deciding not to pass given that it is infeasible to safely pass
- Safety Evaluation:
  - P(C): Probability of safely executing the passing maneuver given that car 1 decides to pass

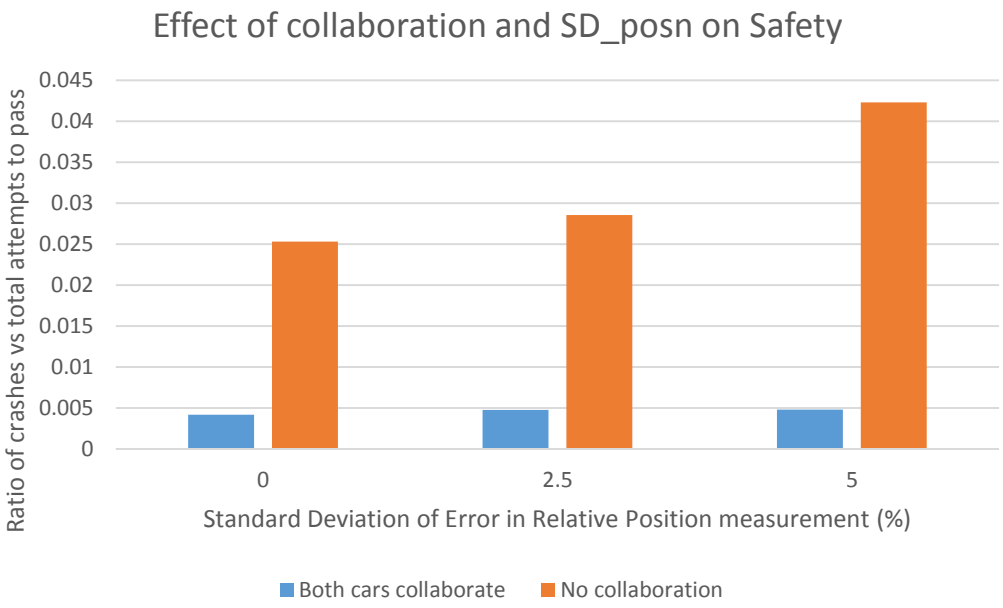
2 S. Bansal, F. Alimardani, J. S. Baras, "Model-based Systems Engineering Applied To The Trajectory Planning For Autonomous Vehicles", to appear in *Proceedings 2018 IEEE International Symposium on Systems Engineering (ISSE),* Rome, Italy, October 2018.

Car Passing Problem Model (SysML, Logic, etc.)



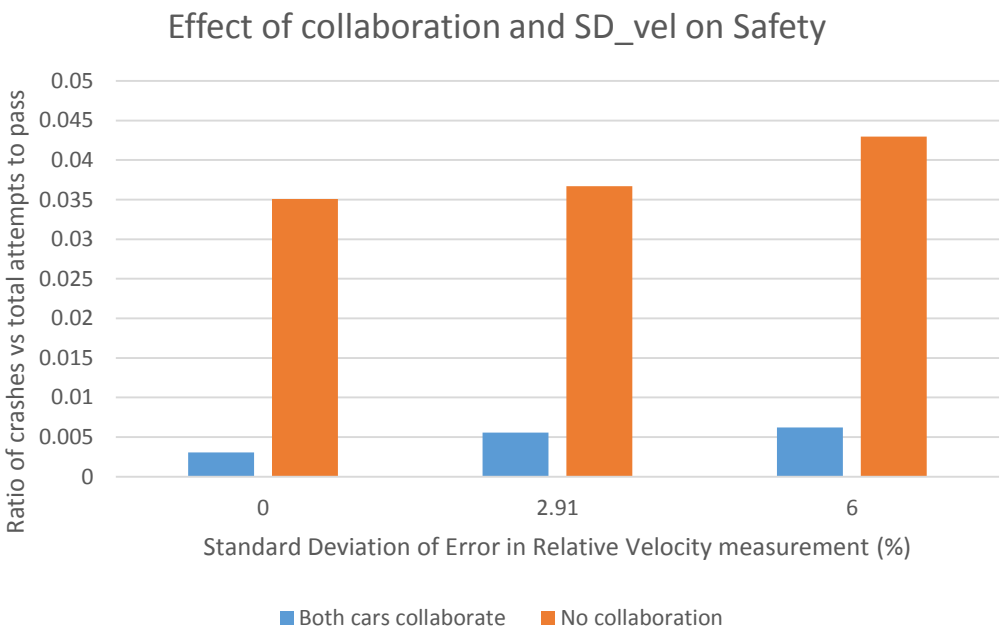
Results: Effect of Collaboration on Measurement Uncertainty

- 1000 iterations of the model
- Graph shows ratio of crashes vs total attempts to pass for different uncertainties in position measurement
- **Ratio of crashes is significantly lower when cars collaborate**
- **Increase in uncertainty in position increases crashes**



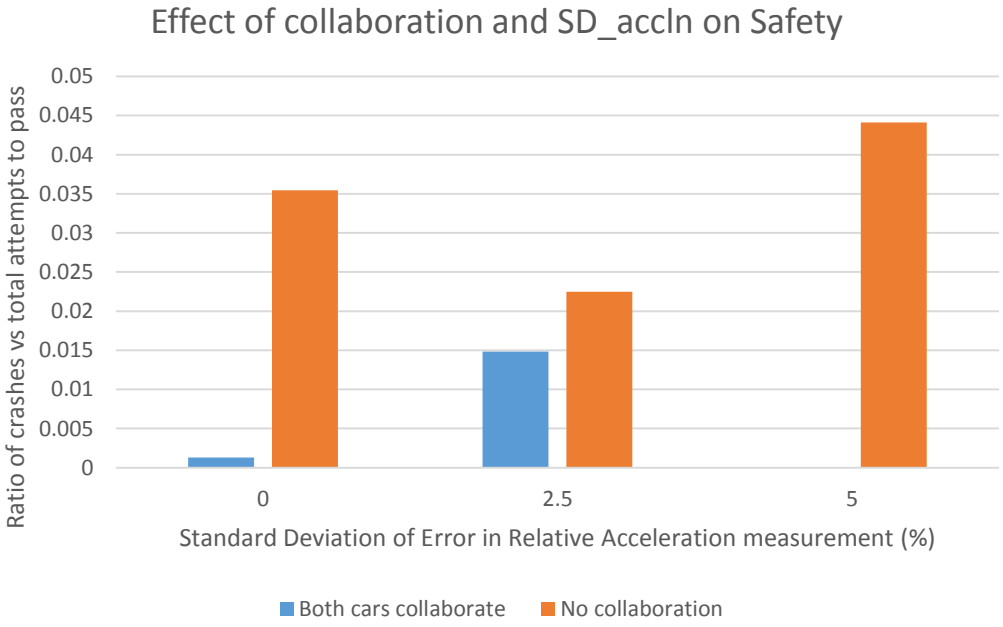
Results: Effect of Collaboration on Measurement Uncertainty

- 1000 iterations of the model
- Graph shows ratio of crashes vs total attempts to pass for different uncertainties in velocity measurement
- **Ratio of crashes is significantly lower when cars collaborate**
- **Increase in uncertainty in velocity increases crashes**



Results: Effect of Collaboration on Measurement Uncertainty

- 1000 iterations of the model
- Graph shows ratio of crashes vs total attempts to pass for different uncertainties in acceleration measurement
- **Ratio of crashes is significantly lower when cars collaborate**
- **Further investigation needed**



Conclusion and Future Work

- **Conclusion**:
  - MBSE facilitates managing complexity, making system modular while allowing design space exploration and evaluation.
  - A functional architecture of the car passing problem was modelled using SysML.
  - Well-defined architecture and interfaces facilitated development and integration of modules in MATLAB .
  - Use of the model to evaluate different design options was demonstrated.
  - Use of the model to identify emergent behavior was demonstrated.

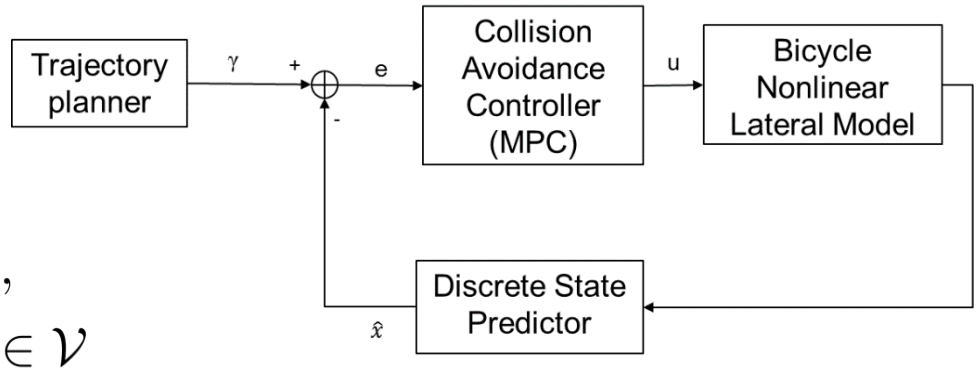
- **Future Work**:
  - Incorporate formal metric temporal logic models
  - Incorporate reachability analysis
  - Incorporate MPC
  - Integrate the above
  - Develop Real-Time V&V (via model-checking) using the above and the model described
  - Add non-commutative probability models and compare

Path Planning: Safety and Verification

Verification for Collision Avoidance Controller

- Lateral dynamics of autonomous vehicle

$$\dot{x}(t) = A(t)x(t) + B(t)u(t) + v(t),$$
$$x(0) \in \mathcal{X}_0,\ u(t) \in \mathcal{U}(t),\ v(t) \in \mathcal{V}$$



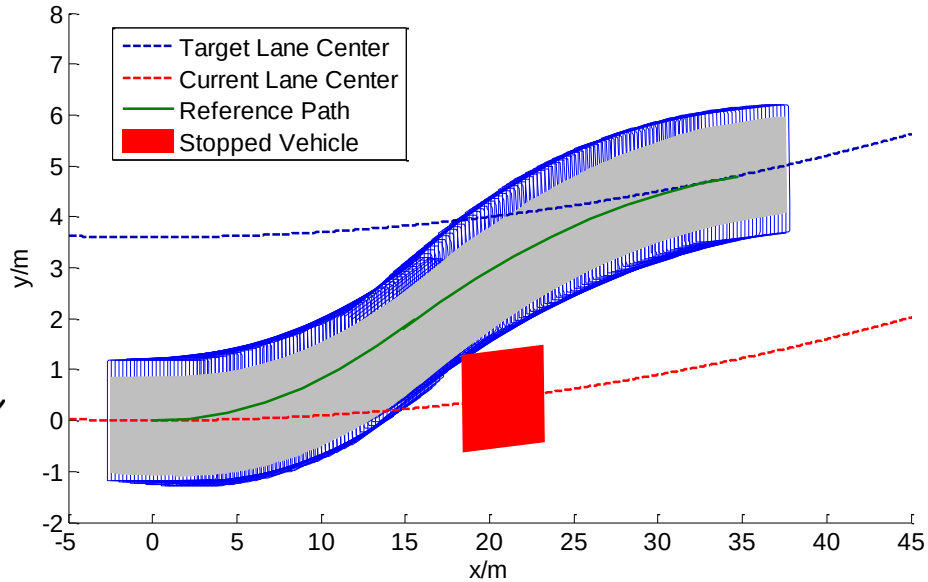
- Trajectory tracking controller based on MPC

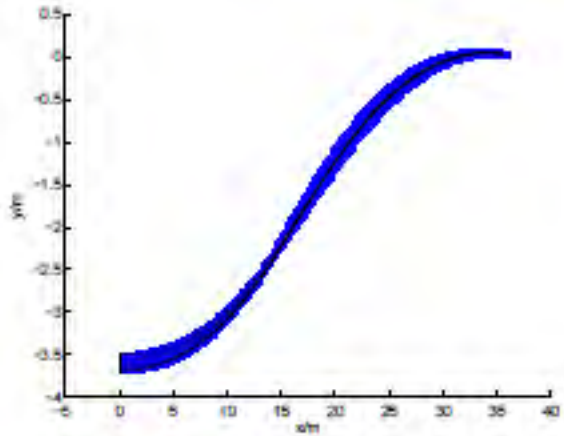
$$u(t) = -K(t)x(t) + h(\gamma(t), t)$$

- Overall linear system

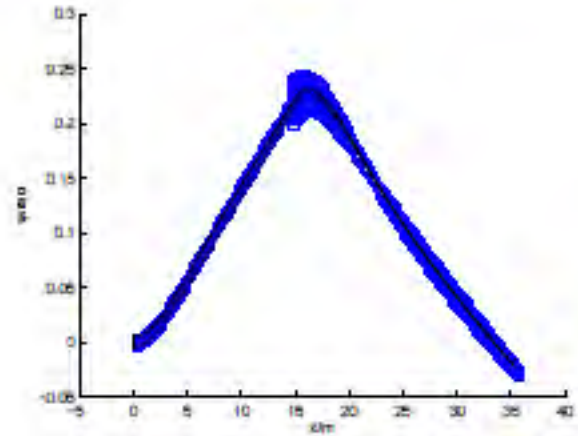
$$\dot{x}(t) = A_c(t)x(t) + \underbrace{v(t) + B(t)h(\gamma(t), t)}_{w(t) \in \mathcal{W}(t)}$$

- Verification result

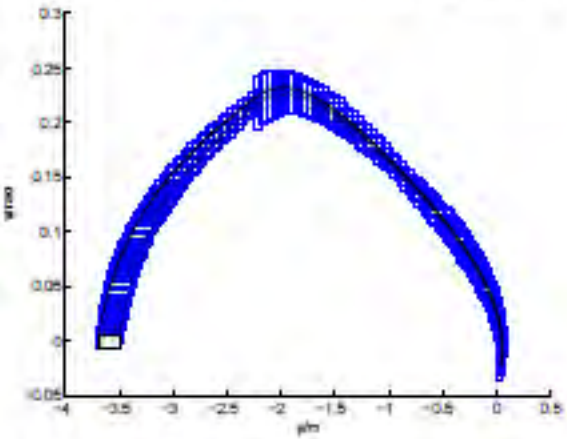




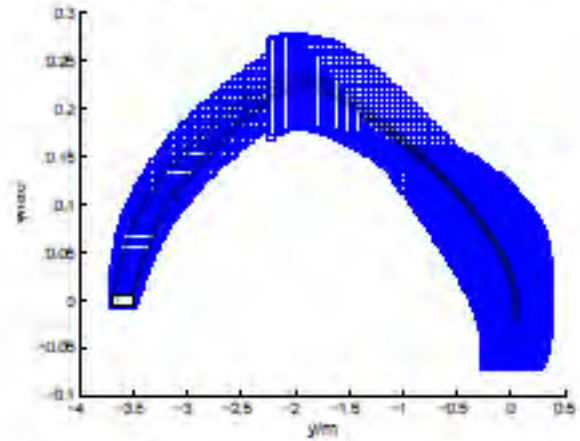
(a) Reachable set projected to longitude distance x and relative lateral distance y.



(b) Reachable set projected to longitude distance x and relative heading ψ.



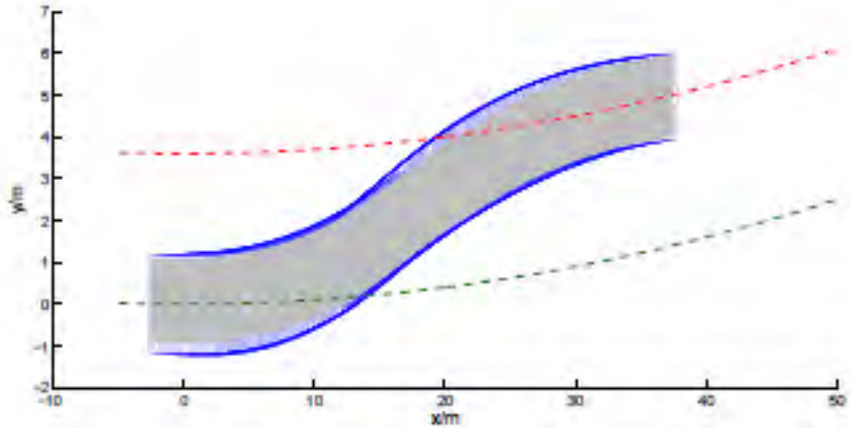
(c) Reachable set projected to relative lateral distance and relative heading.



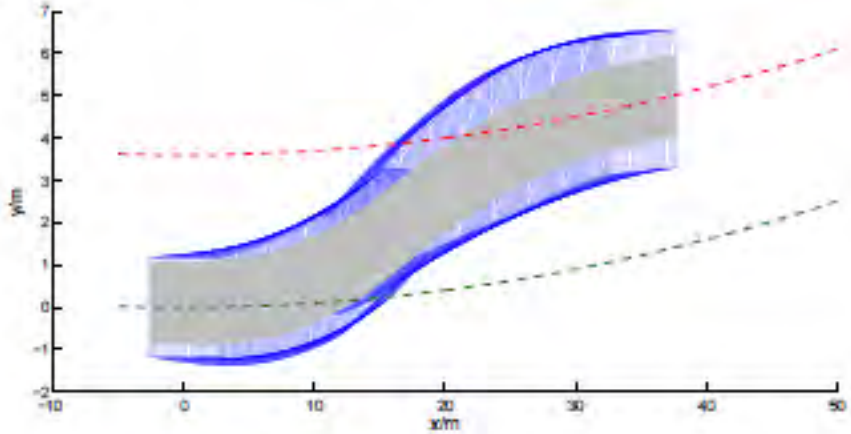
(d) Reachable set after adding deviation on lateral speed and yaw rate.

Figure 2.4: Reachable set of linear hybrid system model. In all the plots, the reachable sets are shown as blue polytopes and simulation traces are black lines. The noise produced a large deviation on the reachable set (Fig. (c) and Fig. (d)). Although the system is still stable, the system is not robust in rejecting noise.

Results with Noise



(a) Occupancy set of the vehicle for hybrid linear system model without sensor noise.



(b) Occupancy set of vehicle for hybrid linear system model with sensor noise

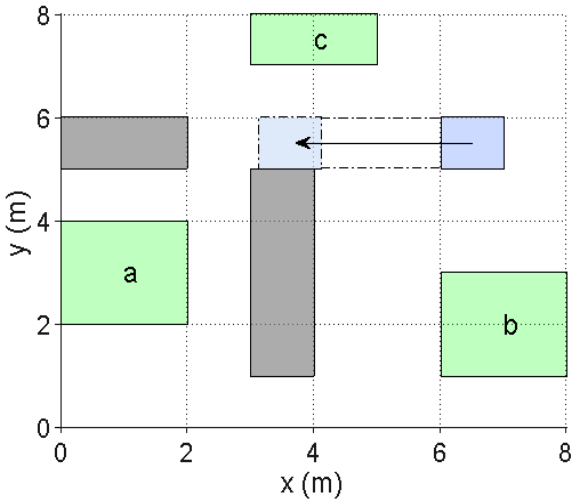
Figure 2.5: Clearly the hybrid linear model is not robust in terms of rejecting sensor noise, the occupancy set is enlarged to about 1m around the vehicle. In this particular case, the distance required to avoid collision is reduced for about 2m due to the sensor noise.

Results with Noise

Path Planning: Spatial and Temporal Specifications

Path Planning with Space and Temporal Logic Constraints

- **Problem**: How to generate trajectory/path based on temporal specifications such as ordering, repetition, safety?
- **State of the art**: motion planning with temporal constraints without duration, such as Linear Temporal Logic (LTL).
- Two methods for timed temporal logics, such as Metric Temporal Logic(MTL):
  - An optimization based method[8]
  - A timed-automata based method[9]



Task: Always visiting area a,b,c and stay there for at least 2s. Always avoiding obstacles

8. Y. Zhou, D. Maity and J. S. Baras, “Optimal Mission Planner with Timed Temporal Logic Constraints", Proceedings of 2015 European Control Conference, Linz, Austria, pp. 759-764, July 15-17,2015.
9. Y. Zhou, D. Maity, and J. S Baras. “Timed automata approach for motion planning using metric interval temporal logic.“, accepted to 2016 European Control Conference, Aalborg Denmark, June 29 - July 1, 2016.

Metric Temporal Logic (MTL) and Time Constrained Task

Definition: The syntax of MTL[12] (MITL[13]) formulas are defined according to the following grammar rules:

$$\phi ::= \top \mid \pi \mid \neg\phi \mid \phi \vee \phi \mid \phi U_I \phi$$

where $I \subseteq [0, \infty]$ is an interval with end points in $\mathbb{N} \cup \{\infty\}$and the end points have to be distinct. $\pi \in \Pi$ is the atomic proposition.

More sophisticated MTL (MITL) operators can be derived using the grammar defined above; such as: always in $I_1 \equiv \bot\, U_{I_1}$, eventually always $\Diamond_{I_1} \Box_{I_2}$ etc.

12. R. Koymans, "Specifying real-time properties with metric temporal logic," *Real-time systems*, vol. 2, no. 4, pp. 255–299, 1990.
13. R. Alur, T. Feder, and T. A. Henzinger, "The benefits of relaxing punctuality," J. of the ACM (JACM), vol. 43, no. 1, pp. 116–146, 1996.

Optimization Based Method

$$\min_{u} \quad J(x(t,u),u(t))$$

$$\text{Subject to} \quad x(t+1) = f(t,x(t),u(t))$$

$$\mathbf{x}_{t_0} \vDash \varphi$$

Remarks:

The task φ may be a finite duration task within an infinite time horizon task such as surveillance, periodic tasks etc.

From MTL Constraints to Linear Constraints

A polygon can be represented as intersections of several half-planes.

The constraint $z_i^t = 1$ iff $h_i^T x(t) \leq k_i$ is enforced by the linear constraints:

$$\begin{aligned} h_i^T x(t) &\leq k_i + M(1 - z_i^t) \\ h_i^T x(t) &\geq k_i - M z_i^t + \epsilon \end{aligned} \tag{1}$$

where M is a very large positive number and ϵ is a very small positive number, and $z_i^t \in \{0,1\}$.

Let $\mathcal{P} = \cap_{i=1}^n H_i$ be a polygon with $H_i = \{x | \, h_i^T x \leq k_i\}$.
Define $P_t^{\mathcal{P}} = \wedge_{i=1}^n z_i^t$, then $P_t^{\mathcal{P}} = 1$ iff $x(t) \in \mathcal{P}$.

MTL Rules as Linear Constraints

$x_t \vDash \mathcal{P}$ iff $x(t) \in \mathcal{P}$ is equivalent to $P_t^{\mathcal{P}} = 1$.

The linear-integer constraints equivalent to $P_t^{\mathcal{P}} = 1$ are given in (1)

Negation Operator:

$\varphi = \neg p$: $\quad P_t^{\varphi} = 1 - P_t^{p}$

MTL Rules as Linear Constraints (Cont.)

Conjunction Operator:

$$\varphi = \wedge_{i=1}^{m} p_i : \quad P_t^{\varphi} \leq P_t^{p_i}, \quad i = 1, \cdots, m$$

$$P_t^{\varphi} \geq 1 - m + \sum_{i=1}^{m} P_t^{p_i}.$$

Disjunction Operator:

$$\varphi = \vee_{i=1}^{m} p_i : \quad P_t^{\varphi} \geq P_t^{p_i}, \quad i = 1, \cdots, m$$

$$P_t^{\varphi} \leq \sum_{i=1}^{m} P_t^{p_i}.$$

MTL Rules as Linear Constraints (Cont.)

Let $t \in \{0,1,\cdots,N-t_2\}$, N is the total time horizon for planning.

Eventually within $[t_1, t_2]$: $\varphi = \Diamond_{[t_1,t_2]}\, p$:

$$P_t^{\varphi} \geq P_{\tau}^{p}, \quad \tau \in \{t+t_1,\cdots,t+t_2\}$$
$$P_t^{\varphi} \leq \sum_{\{\tau=t+t_1\}}^{\{t+t_2\}} P_{\tau}^{p}.$$

Always within $[t_1, t_2]$: $\varphi = \Box_{[t_1,t_2]} p$

$$P_t^{\varphi} \leq P_{\tau}^{p}, \quad \tau \in \{t+t_1,\cdots,t+t_2\}$$
$$P_t^{\varphi} \geq \sum_{\{\tau=t+t_1\}}^{\{t+t_2\}} P_{\tau}^{p} + \mathrm{t}_1 - \mathrm{t}_2.$$

MTL Rules as Linear Constraints (Cont.)

Until within $[t_1, t_2]$: $\varphi = pU_{[t_1,t_2]}q$

$$j \in \{t + t_1, \cdots, t + t_2\}$$

$$a_{tj} \leq P_j^q,$$

$$a_{tj} \leq P_k^p, \quad k \in \{t, \cdots, j-1\},$$

$$a_{tj} \geq P_j^q + \sum_{k=t}^{j-1} P_k^p + t - j\ ,$$

$$P_t^\varphi \leq \sum_{j=t+t_1}^{t+t_2} a_{tj},$$

$$P_t^\varphi \geq a_{tj},$$

Modification of Original Problem into MILP

$$\min_{u, z_0, \ldots, zN \in \{0,1\}^p} \quad J(x(t,u), u(t))$$

$$\text{Subject to} \quad x(t+1) = f(t, x(t), u(t))$$

$$L(x(t), z_t, t) \leq 0 \quad \forall t \in [0, N]$$

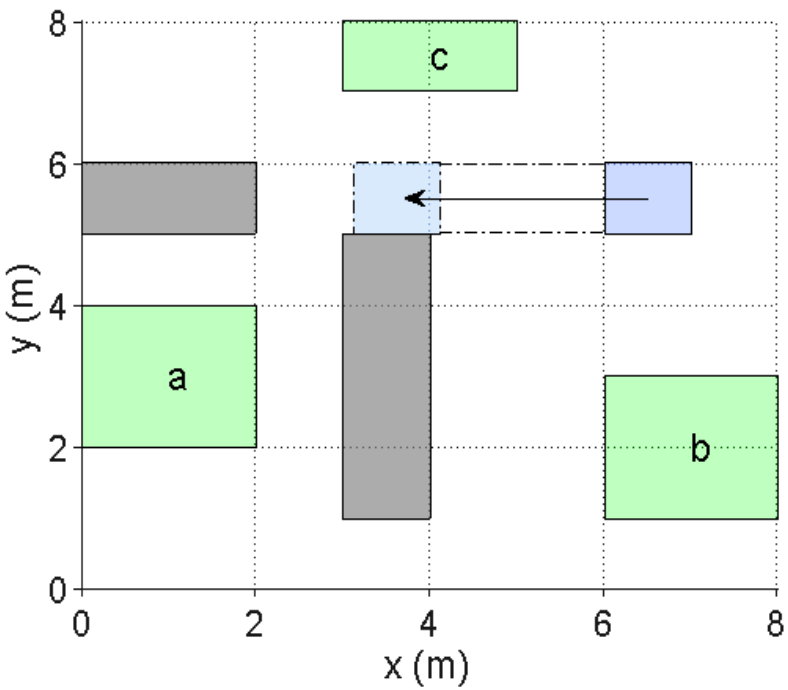
The timed temporal constraint $\mathbf{x_{t_0}} \vDash \boldsymbol{\varphi}$ can been converted into the linear and integer constraints.

Remark:

If $J(\cdot,\cdot)$ $f(.,.,.)$ are linear functions of $x(t)$ and $u(t)$, then entire problem will be a Mixed-Integer Linear Optimization Problem.

Results and Discussion

- **Task**:
  - The specification requires the autonomous vehicle to eventually visit area ‘a’, ‘b’, and ‘c’, and stay there for at least 2 time units, while avoiding obstacles.



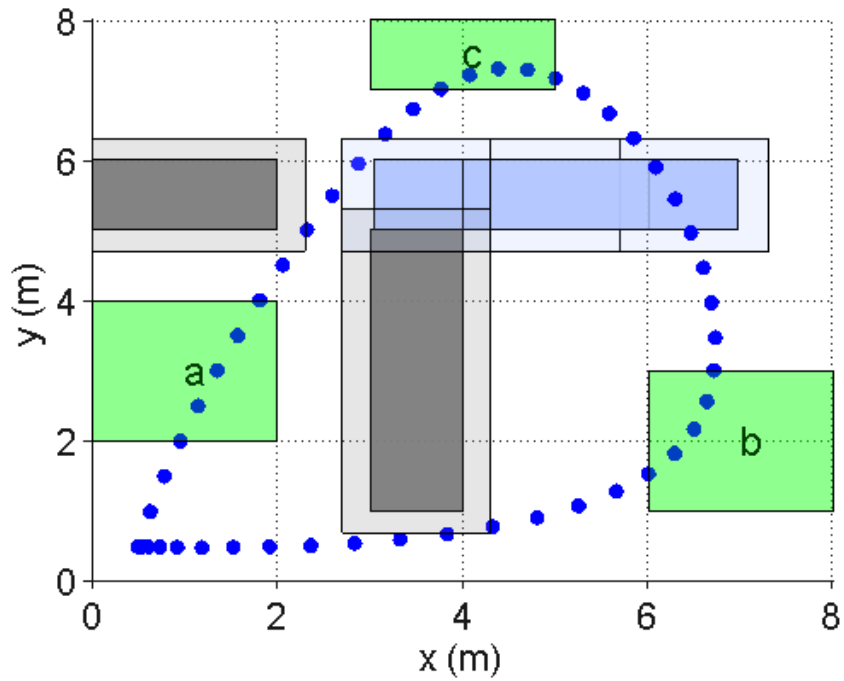
The grey boxes represent fixed obstacles, while the blue one is a moving obstacle with fixed speed.

Results and Discussion

- Specification in MTL

$$\phi_1 = \Diamond\Box_{[0,2]}A \wedge \Diamond\Box_{[0,2]}B \wedge \Diamond\Box_{[0,2]}C \wedge \Box\neg O$$

- The resulting trajectory for the linearized quadrotor dynamics, projected in 2D.



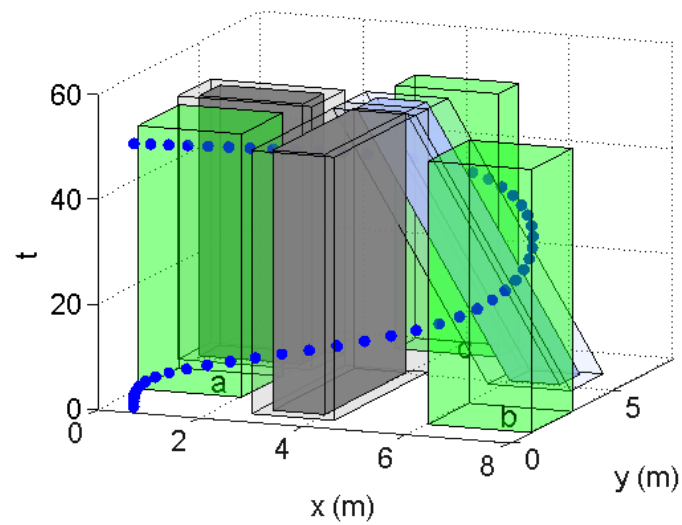
2D projection of the trajectory of the quadrotor satisfying the task.

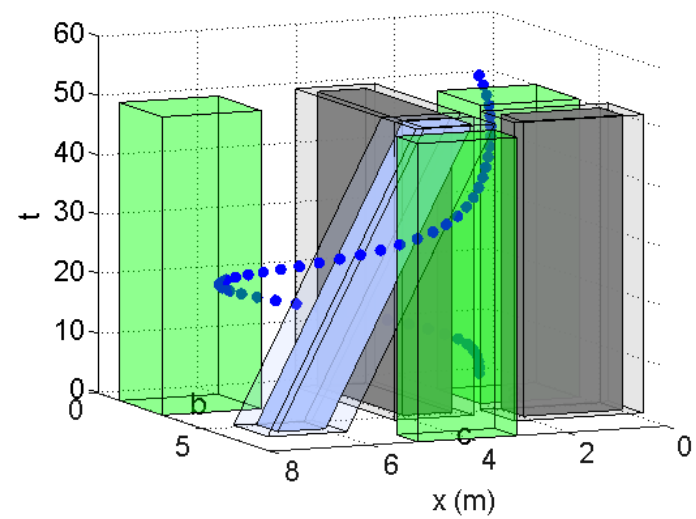
Results and Discussion

- Specification in MTL

$$\phi_1 = \Diamond\Box_{[0,2]}A \wedge \Diamond\Box_{[0,2]}B \wedge \Diamond\Box_{[0,2]}C \wedge \Box\neg O$$

- 3D Trajectory
  - The trajectory avoids the obstacle region in time and space



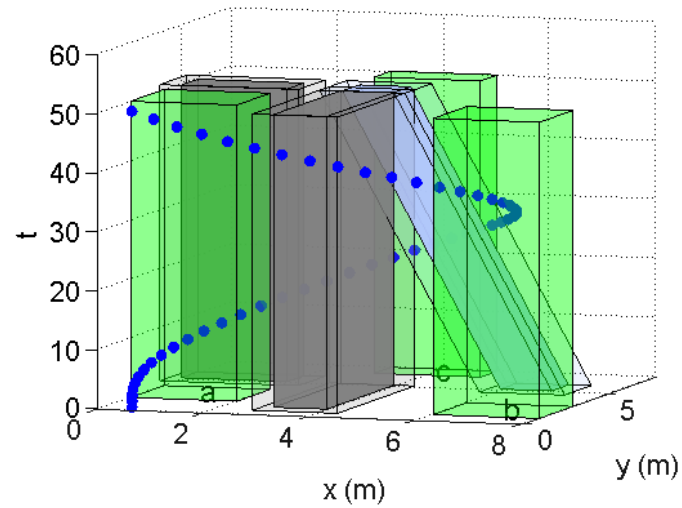


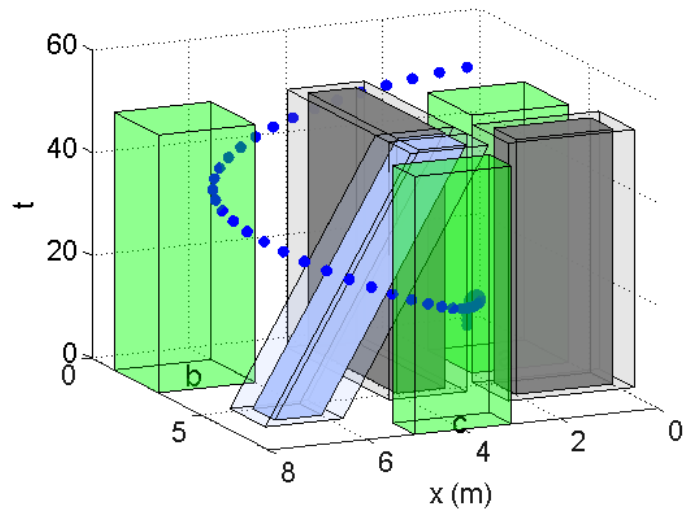
Results and Discussion

- If ordering between area A and area B is restricted, for example, area A has to be visited first, the modified specification in MITL will be the following

$$\phi_2 = \Diamond\Box_{[0,2]}A \wedge \Diamond\Box_{[0,2]}B \wedge \Diamond\Box_{[0,2]}C \wedge \Box\neg O \wedge \neg B\,\mathcal{U}_{[0,N]}A$$

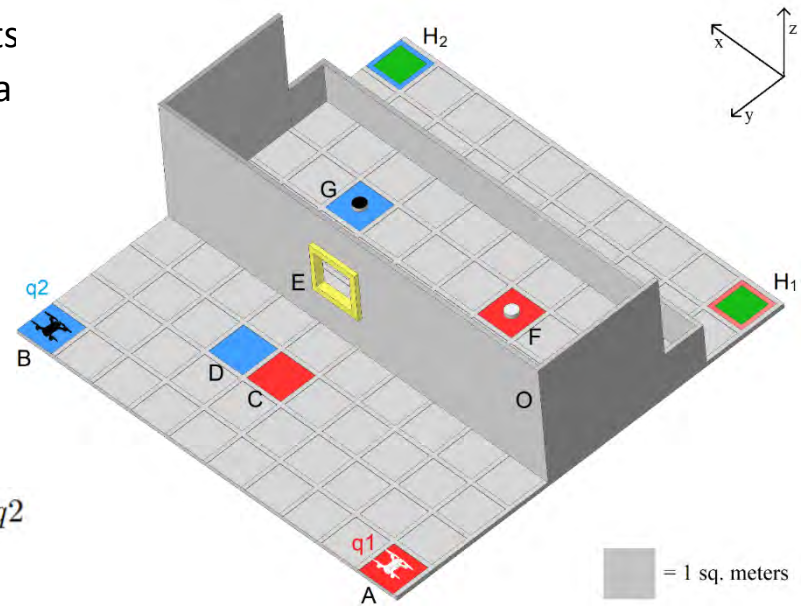
- 3D Trajectory from two different points of view is shown in right.





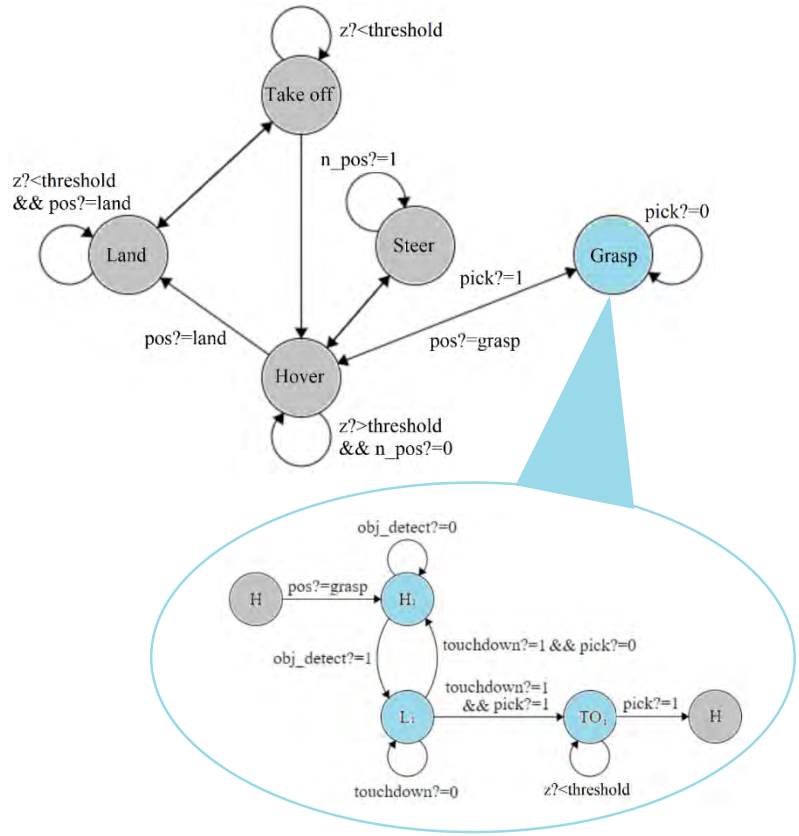
Another Example

- Time critical search and rescue mission
  - Two quadrotors need to evacuate two objects
  - Workspace is a 10 sq. meter constrained area
  - The only access is through a window "*E*"
- Certain areas of interest are marked
  - Task represented by MTL specification
  - Robots must satisfy finite time constraints
  - Robots must avoid obstacle "O"
- For example: Task for quadrotor "*q1*"
  - $\phi = \Diamond_{[0,T_1]} F \wedge \Box_{[0,T_2]} F' \wedge \Diamond_{[0,T_3]} \Box H_1 \wedge \Box \neg O \wedge \Box \neg q2$
  - "*q1*" has priority over "q2"
  - i.e., "*q2*" has to wait for "q1" to pass through the window



Quadrotor dynamics

- Hybrid model for the quadrotor
  - Five different linear modes
    - *Take off*
    - *Land*
    - *Hover*
    - *Steer*
    - *Grasp*
  - Linearization about different operating points
- *Grasp* mode dynamics
  - Under two realistic assumptions:
    - Reliable touchdown on the object
    - Instantaneous object grasp upon touchdown
  - *Grasp* mode is represented as combination of:
    - *Hover* (H_1) and
    - *Land* (L_1) and
    - *Take off* (TO_1) modes



Problem formulation and solution approach

Problem 1:

$$\begin{aligned} \min_{x,u} \quad & J(x(t,u(t)),u(t)) \\ \text{subject to} \quad & x(t+1) = f(t,x(t),u(t)) \\ & \mathbf{x}_{t_0} \models \phi \end{aligned}$$

Problem 2:

$$\begin{aligned} \min_{x,u} \quad & J(x(t,u(t)),u(t)) \\ \text{subject to} \quad & x(t+1) = At)x(t) + B(t)u(t) \\ & \mathbf{x}_{t_0} \models \phi \end{aligned}$$

Problem 3:

$$\begin{aligned} \min_{x_i,u_i} \quad & \textstyle\sum_{t=0}^{N} |u_i(t)| \\ \text{subject to} \quad & x_i(t+1) = A_i(t)x_i(t) + B_i(t)u_i(t) \\ & \mathbf{x}_{t_0^i} \models \phi_{sub_i} \end{aligned}$$

- **Problem 1** is the general optimal control formulation with nonlinear dynamics.
- However, since the quadrotor modes are linear we can simplify and rewrite **Problem 1** with linear dynamics as **Problem 2**.
- We then divide the mission into several sub-tasks by exploiting the invariant nature of various task specifications i.e., the mutual independence of safety and timing constraints along the way, and the different modes (i.e., dynamics) of the robot coreesponding to each sub-task.
- Thus, instead of solving an optimization problem for the complete mission specification ϕ, we break down the problem into smaller optimization problems for each sub-task ϕ_{sub_i}, as in **Problem 3**.

Problem formulation and solution approach

$$\phi = \neg p \iff K_t^{\phi} = 1 - K_t^{p}$$

$$\phi = \wedge_{i=1}^{m} p_i \iff K_t^{\phi} \leq K_t^{p_i}, \quad i = 1, ..., m$$
$$K_t^{\phi} \geq 1 - m + \sum_{i=1}^{m} K_t^{p_i}$$

$$\phi = \vee_{i=1}^{m} p_i \iff K_t^{\phi} \geq K_t^{p_i}, \quad i = 1, ..., m$$
$$K_t^{\phi} \leq \sum_{i=1}^{m} K_t^{p_i}$$

$$\phi = \Box_{[t_1,t_2]} p \iff K_t^{\phi} \leq K_{\tau}^{p}, \quad \tau \in \{t + t_1, ..., t + t_2\}$$
$$K_t^{\phi} \geq \sum_{\tau=t+t_1}^{t+t_2} K_{\tau}^{p} - (t_2 - t_1)$$

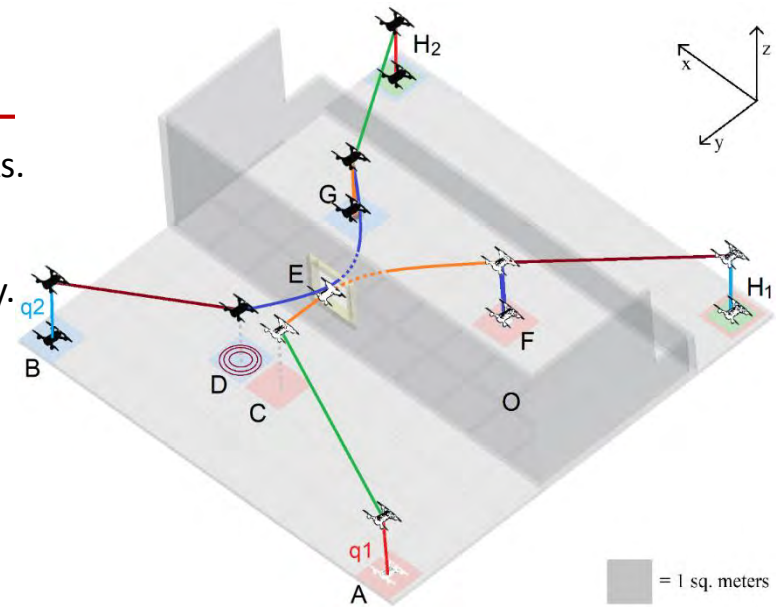
and so on..

- Based on methods presented in [1] and [2], we translate the MTL sub-task specifications to a set of mixed integer linear constraints.
- Thus, **Problem 3** converts to an optimal control problem in discrete time with linear cost and linear constraints i.e., a Mixed Integer Linear Program (MILP).
- This set of smaller optimization problems can be solved efficiently with a solver such as YALMIP-CPLEX and MALTLAB.
- Worst case complexity of this MILP is exponential in terms of the Boolean variables (i.e., the number of halfspaces needed to represent the MTL formula) and the discrete time horizon or the number of iterations.
- Thus, the decomposition o ϕ is intuitive.

[1] Karaman et. al, Optimal control of mixed logical dynamical systems with linear temporal logic specifications, CDC'08
[2] Zhou et. al, Optimal mission planner with timed temporal logic constraints, ECC'15

Simulation and results

- The resulting composed trajectories for the sub-tasks.
- N = 30, and rate of discretization is 5 Hz.
- Both "*q1*" and "*q2*" in the workspace simultaneously.
- The *Hover* and *Steer* altitude is set to 1.5 m.
- The number of circular rings at "*D*" represent the number of time units spent by "*q2*" while waiting in *Hover* mode.
- The two quadrotors satisfy the finite timing constraints for the task and avoid the obstacle "*O*".



Sub-tasks for "q1"

$$\phi_{q1(AA')} = \Box A \wedge \Diamond_{[0,5]} A' \quad [mode: Take\ off]$$
$$\phi_{q1(AC)} = \Diamond_{[0,5]} C \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q1(CF)} = \Diamond_{[0,10]} F \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q1(FF')} = \Box F \wedge \Diamond_{[0,10]} F' \quad [mode: Grasp]$$
$$\phi_{q1(FH_1)} = \Diamond_{[0,10]} H_1 \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q1(H_1H_1')} = \Box H_1 \quad [mode: Land]$$

Sub-tasks for "q2"

$$\phi_{q2(BB')} = \Box B \wedge \Diamond_{[0,5]} B' \quad [mode: Take\ off]$$
$$\phi_{q2(BD)} = \Diamond_{[0,5]} D \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q2(D)} = \Box D\ \mathcal{U}(\neg(pos(q1)? = C) \quad [mode: Hover]$$
$$\phi_{q2(DG)} = \Diamond_{[0,10]} G \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q2(GG')} = \Box G \wedge \Diamond_{[0,10]} G' \quad [mode: Grasp]$$
$$\phi_{q2(GH_2)} = \Diamond_{[0,10]} H_2 \wedge \Box\neg O \quad [mode: Steer]$$
$$\phi_{q2(H_2H_2')} = \Box H_2 \quad [mode: Land]$$

TABLE I

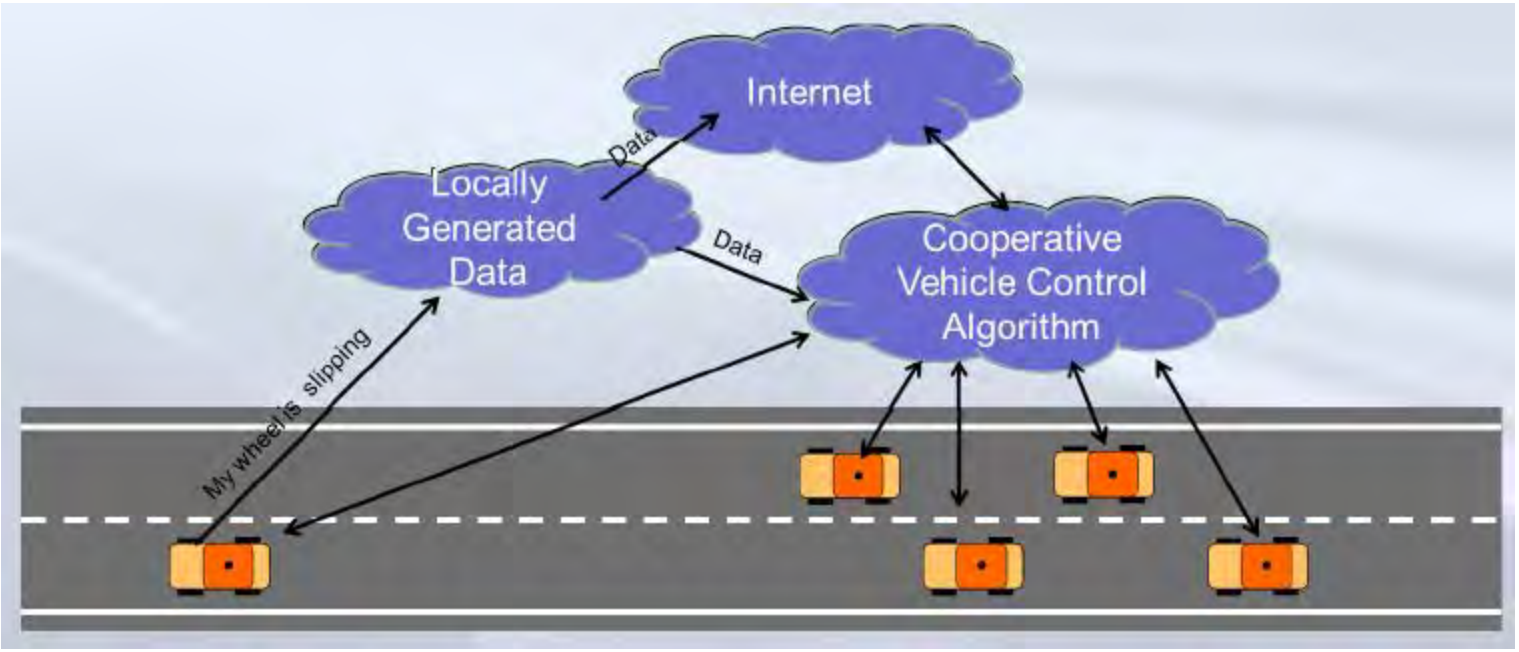
COMPUTATION TIMES FOR SUB-TASKS (ϕ_{sub_i})

Task(q1)	Time (sec)	Task(q2)	Time (sec)
$\phi_{q1(AA')}$	2.7	$\phi_{q2(BB')}$	2.7
$\phi_{q1(AC)}$	6.3	$\phi_{q2(BD)}$	5.8
$\phi_{q1(CF)}$	10.3	$\phi_{q2(D)}$	2.0
$\phi_{q1(FF')}$	3.0	$\phi_{q2(DG)}$	11.1
$\phi_{q1(FH_1)}$	5.7	$\phi_{q2(GG')}$	3.0
$\phi_{q1(H_1H_1')}$	2.5	$\phi_{q2(GH_2)}$	5.7
—	—	$\phi_{q2(H_2H_2')}$	2.5

Current and Future Work

Connected Cars

Connected Cars: Effects of Communications -- Cognitive and Collaborative



Key Challenge: Humans

We are developing novel frameworks to include humans in this collaborative networked CPS environment

Vehicle Distribution and Routing in Large Automated Transportation Networks

- Autonomous vehicles (driverless) small-to-moderate size
- Dedicated pathway networks (dynamically planned), with on-line or off-line stations
- Varying complexity: vehicle size, system capacity, network density,
- Routes are fixed or variable, selected at the time of trip request, or dynamically selected as vehicles progress through the network
- Large ATN network: a dense network of hundreds of miles of connected guideways, joining as many as a hundred stations, with thousands of vehicles
- Strategic problem: distributing and routing the vehicles

Motivation: Joint work with Alan Pue

ABSTRACT

Title of Dissertation: Vehicle Distribution and Routing in a Large Automated Transportation Network

Alan J. Pue, Doctor of Philosophy, 1981

Dissertation directed by: John Baras
Associate Professor
Electrical Engineering

Motivation: Test Example from my work with Pue

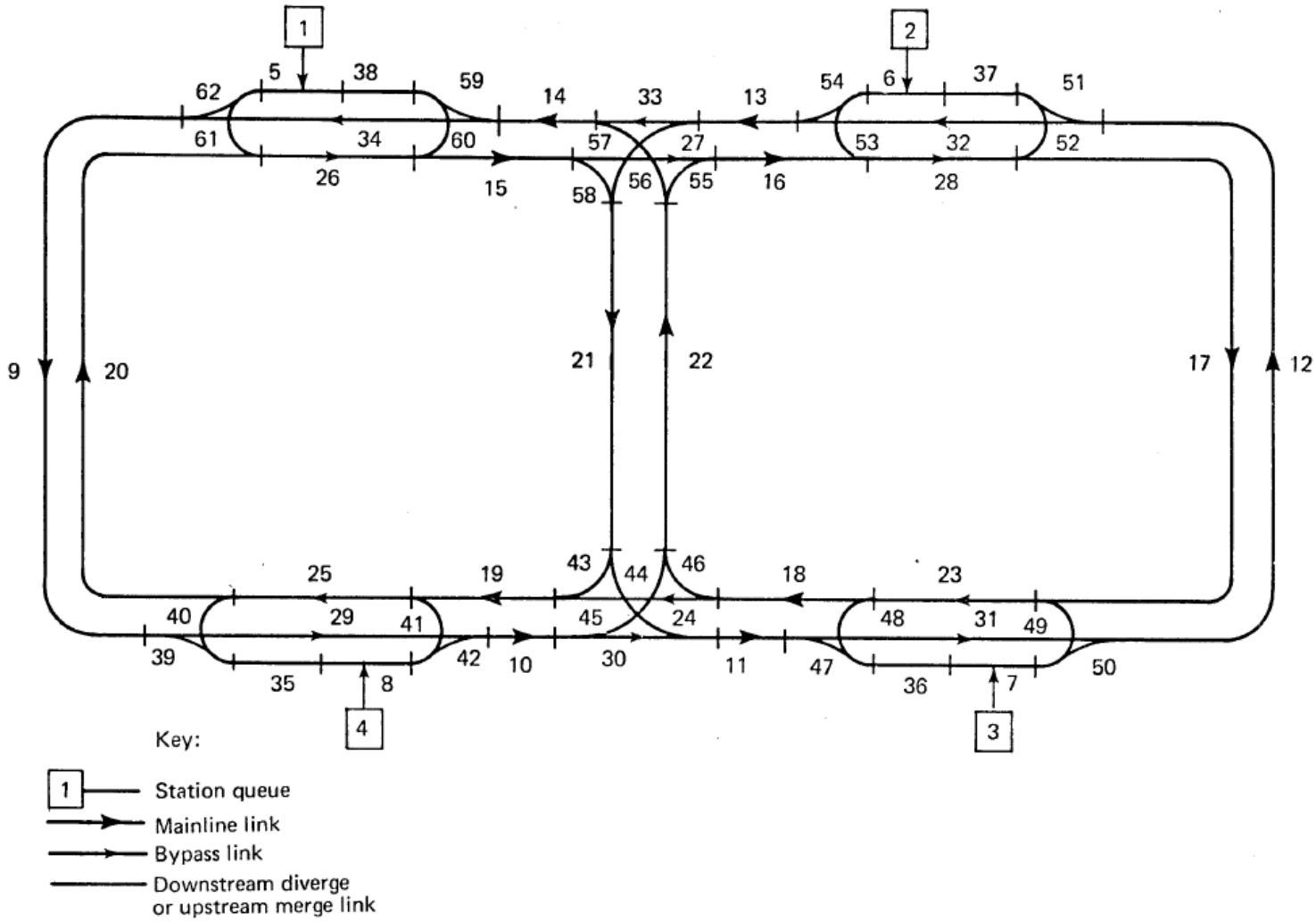


Fig. 8.1 Simulated network.

Approach – Longitudinal control

Two approaches

- First – point following: assigns each vehicle to a moving cell, cells propagated at predetermined velocities and spacings
- Second – vehicle following: vehicles communicate motion coordinated with neighbors
- Special case we use: vehicle follows immediate predecessor

GOALS:

- Formulate problem as a control problem, including routing and traffic assignment
- Emphasize distributed and local algorithms
- Models vehicle flows and formulate performance index based on total, time averaged, travel time
- We get a problem with convex cost , nonconvex constraints

Duality decomposition

- Apply duality – decouples overall network dynamics into vehicle type (origin destination pair) subnetworks
- Triangular structure of subnetwork dynamics allows distributed control computation to solve the dual problem
- Upper level coordination control (localized to each link) is used to satisfy the interconnection constraint (sum of vehicle type densities equals total vehicle density on the link)
- Investigate convergence
- Develop efficient and faster suboptimal algorithms

Specific Problem Details

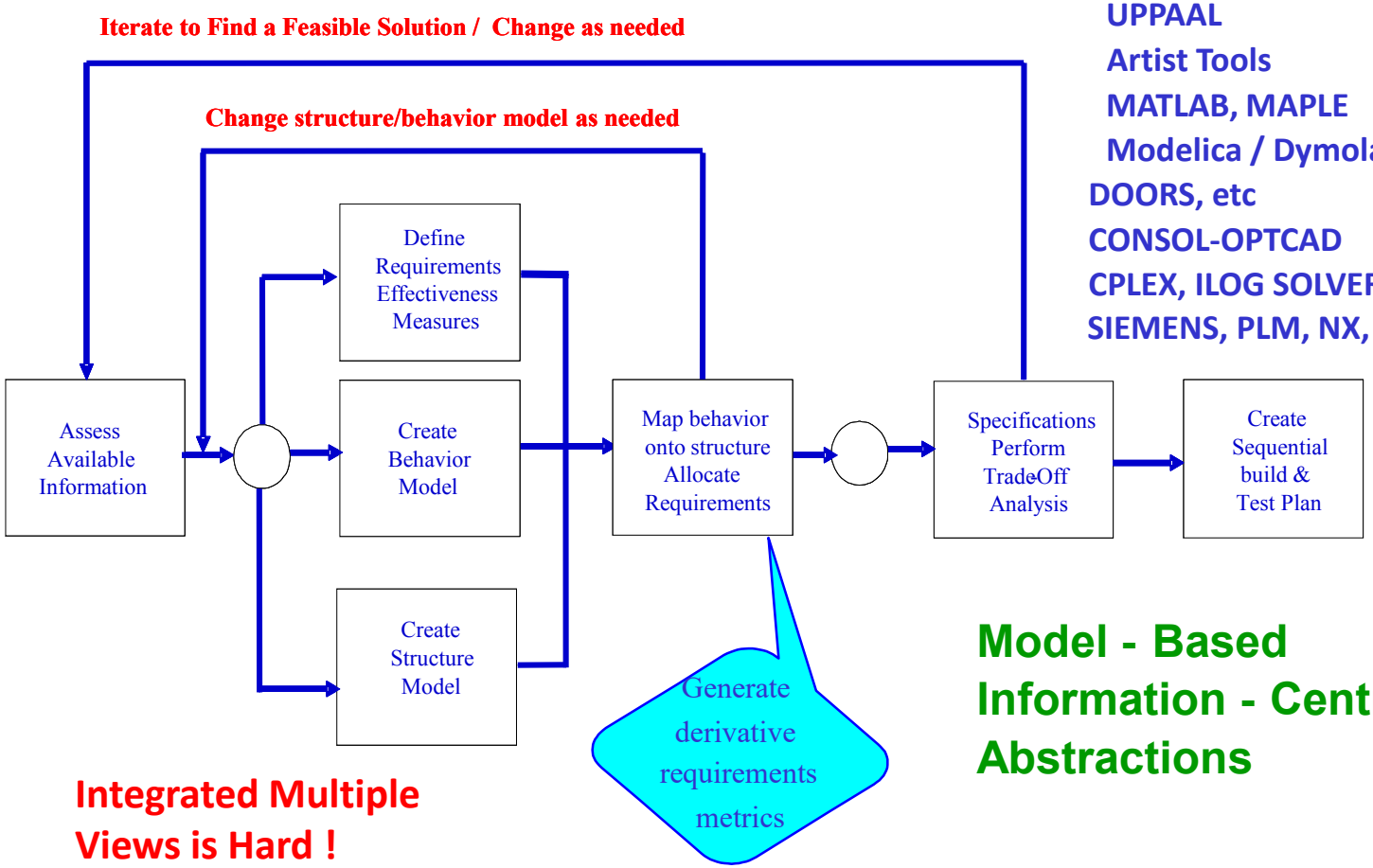
- Application to cell transmission model (CTM) for freways and urban situations
- Signalized intersections – green wave constraints – comparison to max pressure
- Integration of intersection signaling (or access control signaling) and routing via back pressure principles
- Improvements on backpressure via hyperbolic embedding
- Effects of cooperative control – learning to cooperate
- Multimode traffic
- Dynamic Scheduling
- On-line estimation (or learning) of fundamental flow functions
- Resilience – fault and accident recovery algorithms

Model-Based Systems Engineering Workflow

Integrated System Synthesis Tools - & Environments missing

Model- - based
- UML - SysML - GME - eMFLON
- Rapsody
- UPPAAL
- Artist Tools
- MATLAB, MAPLE
- Modelica / Dymola

DOORS, etc
CONSOL-OPTCAD
CPLEX, ILOG SOLVER,
SIEMENS, PLM, NX, TEAM CENTER



Model - Based Information - Centric Abstractions

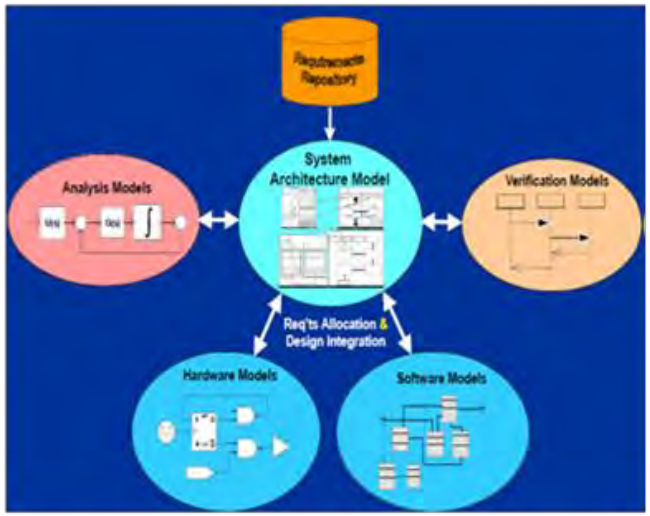
Integrated Multiple Views is Hard !

Integration of Design Space Exploration Tools with SysML– Integrated Models

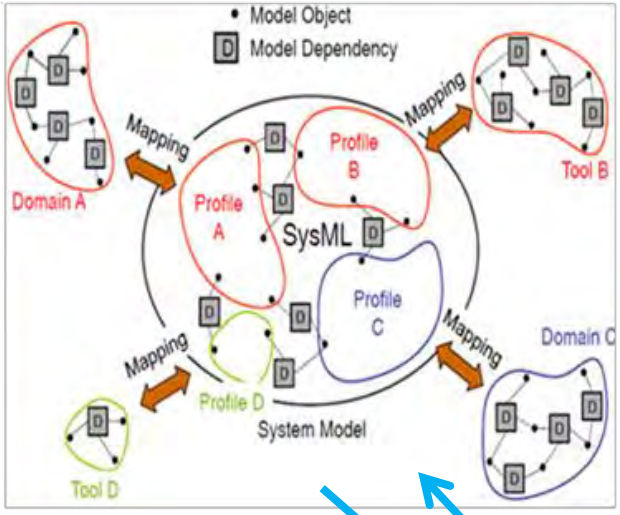
The Challenge & Need:

Develop scalable holistic methods, models and tools for enterprise level system engineering

Multi-domain Model Integration via System Architecture Model (SysML)



System Modeling Transformations



BENEFITS

- **Broader Exploration of the design space**
- **Modularity, re-use**
- **Increased flexibility, adaptability, agility**
- **Engineering tools allowing conceptual design, leading to full product models and easy modifications**
- **Automated validation/verification**

APPLICATIONS

- **Avionics**
- **Automotive**
- **Robotics**
- **Smart Buildings**
- **Power Grid**
- **Health care**
- **Telecomm and WSN**
- **Smart PDAs**
- **Smart Manufacturing**

" Master System Model"

Update System Model

ILOG SOLVER, CPLEX, CONSOL-OPTCAD

Tradeoff parameters

ADD & INTEGRATE

Multiple domain modeling tools

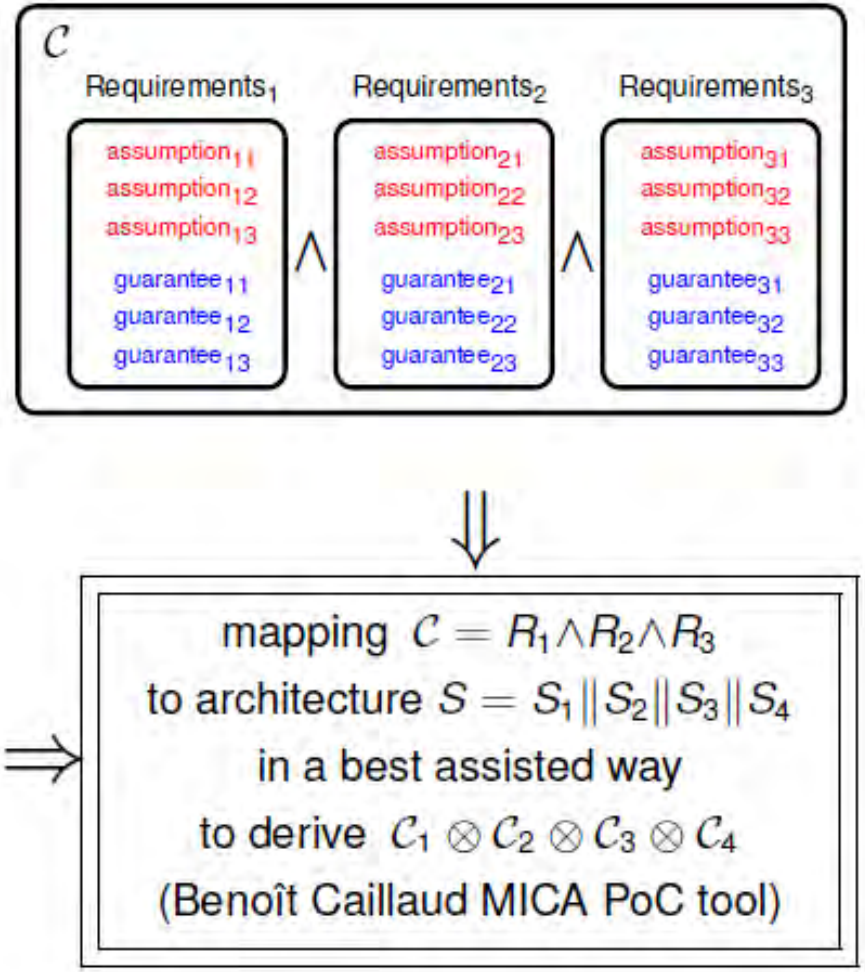
- **Tradeoff Tools (MCO & CP)**
- **Validation / Verification Tools**
- **Databases and Libraries of annotated component models from all disciplines**

DB of system components and models

Requirements Engineering

- How to represent requirements?
  - Automata, Timed-Automata, Timed Petri-Nets
  - Dependence-Influence graphs for traceability
  - Set-valued systems, reachability, … for the continuous parts
  - Constraint – rule consistency across resolution levels
- How to automatically allocate requirements to components?
- How to automatically check requirements?
  - **Approach**: Integrate contract-based design, model-checking, automatic theorem proving
- How to integrate automatic and experimental verification?
- How to do V&V at various granularities and progressively as the design proceeds – not at the end?
- The front-end challenge: Make it easy to the broad engineering user?

Contract-Based Requirements Engineering



Thank you!

baras@isr.umd.edu

301-405-6606

http://www.isr.umd.edu/~baras

Questions?