MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

TRANSPORTATION SAFETY OF HIGHLY AUTOMATED VEHICLES: FROM DESIGN TO DEPLOYMENT

Zach LaCelle, The MITRE Corporation

Table of Contents

Introduction and Call to Action . . . 1
Challenges in ADS Deployment . . . 2
An Evolving ADS Safety Approach . . . 3
Building Out the Safety Approach . . . 4
ADS Safety Building Blocks . . . 5
- Safety Culture and Management . . . 5
- Assessing Safety through Data Sharing . . . 6
- Hazard-Aware, Traceable Data Logging . . . 8
- Requirements for Systems Engineering Practices . . . 9
- Considering Communications, Spectrum, and Connected Vehicles . . . 11
- Requiring Certification for SAE Level 3 or Higher ADS . . . 12

Conclusion . . . 13
References . . . 15

Introduction and Call to Action

In ground vehicle transportation, the decade of the 2010s has shown the enormous potential of highly automated or autonomous vehicle technology. From initial automated systems such as adaptive cruise control and blind spot monitoring, innovators have expanded to the testing of fully autonomous systems that complete routes with no human input [1]. As many researchers have highlighted, these technologies present opportunities in safety, accessibility, and efficiency [2] [3] for the entire transportation system. An entire new industry focused on these technologies has bloomed, with billions of dollars invested in non-traditional tech companies focused on autonomous vehicle technology [4]. A new paradigm is needed to ensure that the safety, accessibility, and efficiency gains promised by highly automated vehicles become a reality.

Traditional vehicle safety systems, such as antilock brakes or seat belts, use functional safety processes to create traceably and functionally safe systems. Design standards such as ISO-26262, "Road Vehicles – Functional Safety," [6] or MIL-STD-882E, "Department of Defense Standard Practice – System Safety," [7] present methods to trace hazards through a system and plan mitigations. This method does not work well for systems that are challenging to characterize—for example, the state-of-the-art neural networks and learning-based systems required to perform key tasks on highly automated vehicles [8].

Thus, given the new technical, deployment, and adoption challenges associated with autonomous and highly automated vehicles, a new approach to safety for these systems is needed. This paradigm must be both flexible and holistic, recognizing that some fundamental challenges remain unanswered. However, now is the time to engage proactively and effectively to provide a clear and unambiguous set of recommendations, best practices, requirements, and regulations around autonomous and automated driving systems (ADS). Indeed, recent actions such as the National Highway Traffic Safety Administration's (NHTSA) advanced notice of proposed rulemaking regarding safe adoption of ADS [9] underscore a sentiment throughout the industry: Now is the time for a clear safety approach, cognizant of these unique challenges, that will remove environmental and regulatory uncertainty.

A NEW PARADIGM IS NEEDED TO ENSURE THAT THE SAFETY, ACCESSIBILITY, AND EFFICIENCY GAINS PROMISED BY HIGHLY AUTOMATED VEHICLES BECOMES A REALITY.

This document outlines MITRE's position regarding how to leverage the unique opportunities ADS present and address the hard challenges they pose, with a targeted focus on safe technology adoption.

Challenges in ADS Deployment

Fully autonomous vehicles have not yet been successfully fielded at any large scale on roads today, despite many previous promises to the contrary. This is due simply to the scale of challenges facing these systems. Based on MITRE's research and prototyping experience—starting 15 years ago in the DARPA Grand Challenge and continuing throughout the last decade with research in safety best practices, human-machine interfaces, trusted artificial intelligence, data-based hazard analysis for automated vehicles, and novel new approaches to autonomous perception, controls, and behaviors—MITRE finds that the following three challenges represent key roadblocks to safe and trusted ADS deployment.

The operational domain is incredibly complex: The roadway environment is highly cluttered, with many sizes and shapes of obstacles presented to drivers. These environments are also highly dynamic, with objects moving in and out of the roadway regularly. Thus, the sensing and perception challenges are significant. Unlike human drivers, who can relatively accurately classify things they have never seen before, the current state-of-the-art systems used to detect and classify the environment do not yet adequately solve the problem for highly automated or autonomous systems. Furthermore, when the systems fail, they tend to fail unpredictably. Thus, the development and implementation challenges for safe perception systems remain fundamentally unsolved.

Human drivers cannot provide reliable failover for automated vehicles: Often, the approach taken by vendors is to assume that the human operator can serve as a backstop for the object and event detection and response (OEDR) task. This approach is used in Society of Automotive Engineers (SAE) level 3 automation, which allows for full automated driving but requires a human to monitor and take over when the ADS fails. Unfortunately, research has shown that humans make poor safety drivers [10]. The required time to obtain situational awareness [5], combined with a driver's lack of formal training regarding their automated vehicle systems, means that systems which rely on human fallback might actually be more dangerous than fully automated systems. It will be challenging for ADS to deploy without a comprehensive autonomy-focused safety framework, since a staged deployment leveraging humans-in-the-loop may not be feasible.

"Miles driven" is insufficient to prove safety: To show system safety, often "miles driven" is the metric of choice. The thinking is that if an autonomous vehicle has operated with low rates of failure for thousands or millions of miles, surely it is safe to deploy on our roadways. Simulated miles, while very useful for autonomous vehicle development and testing, do not necessarily prove safety. The RAND Corporation has done research on the number of miles, without software and hardware changes, necessary to show that an autonomous system is safe—and those numbers are unachievably large [11]. Furthermore, due to the black-box nature of learning-based systems present on state-of-the-art autonomous vehicles, software is often updated during testing. After a software or decision-model update, previous real or simulated miles may no longer indicate safety quality. Miles driven, while important, are not sufficient.

Therefore, due to the combination of an extremely challenging and dynamic environment, an inability to trust untrained human operators, and the insufficiency of miles driven metrics to prove safety, widescale deployment of these systems has remained elusive.

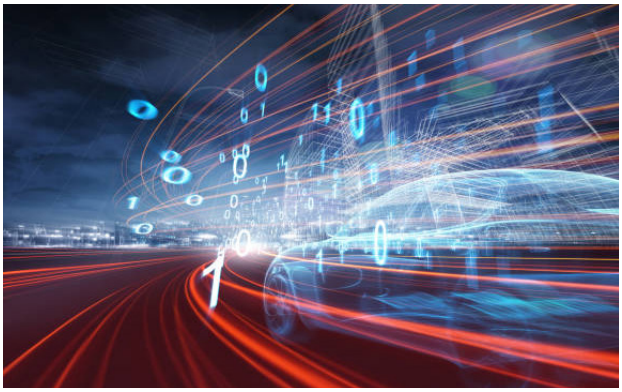
THE PROPOSED APPROACH TO ADS SAFETY LEVERAGES DATA-RICH SYSTEMS AND FAST-PACED RESEARCH AND DEVELOPMENT TO TAKE AN INNOVATIVE APPROACH TO SYSTEM SAFETY—ONE THAT EVOLVES AND IMPROVES WITH NEW BREAKTHROUGHS IN SAFETY RESEARCH.

An Evolving ADS Safety Approach

This preliminary safety approach for ADS is focused on actionable recommendations toward what will provide some level of safety intelligence, while recognizing that the solution is not complete. Autonomous vehicle systems have a very different set of strengths and weaknesses than human-operated systems, and future ADS safety approaches must be cognizant of these differences.

The proposed approach to ADS safety leverages key areas where these systems provide benefit over traditional vehicles. Specifically, it leverages data-rich systems and fast-paced research and development to take an innovative approach to system safety—one that evolves and improves with new breakthroughs in safety research.

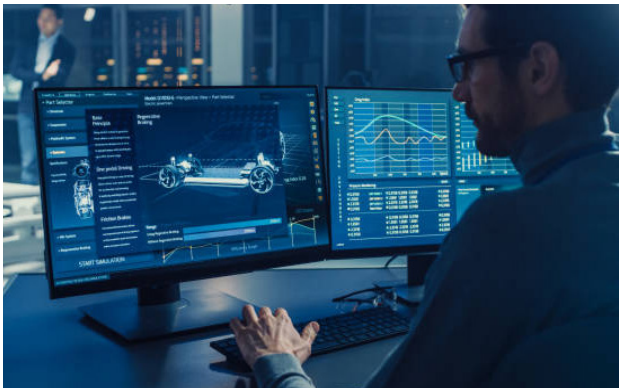
Unfortunately, old methodologies—component-level and system-level functional safety, combined with human-in-the-loop oversight—are not sufficient safety practices for ADS [8]. However, ADS present a wealth of opportunity in safety management through data-driven analysis. These



systems produce huge amounts of detailed operational data, far beyond that of a traditional vehicle. This data, in combination with safety culture practices, is also one of the only current methods to evaluate functionality and safety at scale; it is the only stand-in we have for the human operator's cognition. Thus, unlike traditional vehicle technology, a stronger and more prescriptive position must be taken regarding data logging, analysis, and sharing. Such an approach will serve as a key catalyst for systemic safety improvements and will encourage buy-in from all stakeholders such as researchers, regulators, and most importantly, the public.

ADS DEVELOPMENT CAN MOVE FROM MOSTLY DISPARATE AND SILOED EFFORTS TO A COLLABORATIVE, VIBRANT, AND SAFER ECOSYSTEM—PROVIDING BENEFIT FOR ALL PARTIES INVOLVED.

In addition to vehicle data, connectivity will play an important role in the ground vehicle fleet of the future. Stakeholders must work across government and with industry to enable connectivity wherever possible; sensing the environment is challenging and often limited to line of sight, and receiving shared communications about the environment greatly reduces risk and will thus increase deployment, adoption, and safety. This iterative and evolving approach is heavily focused on leveraging ADS data to inform safety, through methods such as domain-wide safety analytics or use-case sharing to demonstrate behaviors in common situations. By leveraging organizational structures that promote safety culture and taking into consideration future ADS system requirements for communication and collaboration, MITRE believes that ADS development can move from mostly disparate and siloed efforts to a collaborative, vibrant, and safer ecosystem—providing benefit for all parties involved.



Building Out the Safety Approach

This safety approach can be viewed through the lens of a logic model [12], as shown in Figure 1. Such a model provides a methodical way of identifying processes that enable specific desired outcomes.

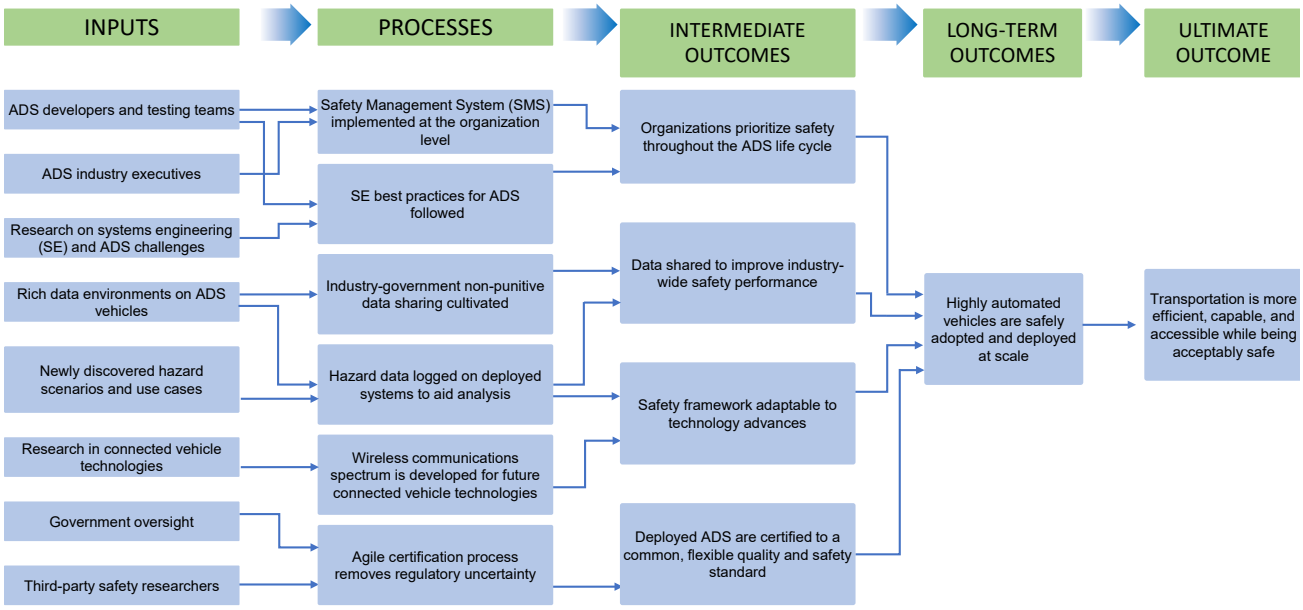


FIGURE 1: AN INITIAL PROTOTYPE LOGIC MODEL REPRESENTATION OF THE PROPOSED ADS SAFETY APPROACH. THE LOGIC MODEL IS ONE METHOD OF VISUALIZING COMPONENTS OF A BUSINESS PROCESS OR PROGRAM.

Inputs and processes can be clearly defined across multiple types of stakeholders, and clear roles and responsibilities leading to outcomes can be decomposed. This model represents an initial prototype safety approach focused on the three key challenges presented earlier in this paper. MITRE recommends that specific stakeholders, such as the U.S. Department of Transportation (DOT), leverage such an approach to develop a comprehensive, collaborative, and integrated approach to ADS safety. As new gaps in ADS safety are identified or new approaches are discovered, the model can be updated to reflect these advancements.

MITRE's recommendations throughout the rest of this white paper fall within the Processes section of the logic model, where processes take existing inputs and drive toward outcomes.

ADS Safety Building Blocks

Through MITRE's experience with safety systems in the aviation transportation domain, as well as our decades of research in autonomous and automated vehicle systems, the following initial building blocks for a safety framework have been identified. This list of building blocks is not yet complete: ADS safety remains an unsolved problem. However, these building blocks leverage known and proven safety approaches, as well as key ADS-enabling technologies, to bring down the safety risk industry-wide.

Safety Culture and Management

An organizational culture that proactively engages in safety risk management is critical to managing safety throughout design, development, and deployment of an ADS system. MITRE recommends that government collaborate with

AN ORGANIZATIONAL CULTURE THAT PROACTIVELY ENGAGES IN SAFETY RISK MANAGEMENT IS CRITICAL TO MANAGING SAFETY THROUGHOUT DESIGN, DEVELOPMENT, AND DEPLOYMENT OF AN ADS SYSTEM.

developers of ADS technologies to encourage organizational safety practices, such as the Safety Management System (SMS) approach, with possible consideration toward regulation. In December 2020, MITRE published "Management of Safety Risk in Automated Driving Systems" [13], which outlines how the SMS organizational approach can be applied to ADS development. This approach focuses on safety as a core cultural attribute of an organization, from the technical contributor up to company executives, and has been used in industries ranging from airlines to nuclear energy, and recently in the automotive industry [14]. ADS technology implementation is technically challenging, and often organizations focus solely on these technical hurdles—but

SAFETY CANNOT BE ADDED ON AS AN AFTERTHOUGHT: IT MUST BE CONSIDERED FROM DESIGN ALL THE WAY TO DEPLOYMENT.

safety must not be an afterthought. It must be considered from design all the way to deployment.

An SMS program defines a framework where safety hazards throughout an organization are identified and reported for risk analysis. Risks are analyzed and measured to compare against what is acceptable to the organization. If risks are unacceptable, a risk management process is used to put into place control actions and mitigations to reduce risk to acceptable levels. Systems-level analysis across hardware, software, people, and the operating environment is key to identifying hazards before new or revised systems or procedures are put into place.

Another key component of SMS is a positive safety culture. Employees, management, and operators must feel empowered to share safety concerns and report safety issues with the ADS. This transparent approach is important, as all stakeholders play a role in safety management and are protected from retribution for reporting honest mistakes. For more specific details on SMS implementations, refer to MITRE's previous report [13].

Collaborating to improve organizational safety practices will help expose safety challenges and unique situations more quickly. Automotive manufacturers who had safety issues due to an insufficient safety culture have identified the importance of adopting organizational safety practices [14]. These practices are even more important when dealing with the high complexity of autonomous vehicles, as this complexity results in hard-to-identify hazards and risks.

EMPLOYEES, MANAGEMENT, AND OPERATORS MUST FEEL EMPOWERED TO SHARE SAFETY CONCERNS AND REPORT SAFETY ISSUES WITH THE ADS.

Assessing Safety through Data Sharing

Autonomous vehicles produce massive amounts of data, from sensors to complex models of the world, to control actions, to vehicle location information. All of this data provides insights into causes of hazards, both local to a specific ADS implementation and systemic across all vehicles. Because functional safety approaches for ADS cannot yet guarantee (or even accurately measure) system safety, researchers, regulators, and developers must be able to assess performance and hazards effectively at scale. Data sharing partnerships help to address these challenges. Today, automobile manufacturers are already voluntarily collaborating on safety with each other and the NHTSA in a data-sharing partnership, called the Partnership for Analytics Research

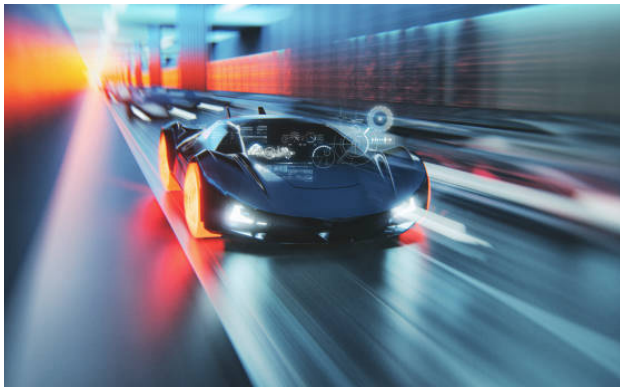
VEHICLE CONTENT AND OTHER SAFETY DATA IS ANONYMIZED, POOLED ACROSS ORGANIZATIONS, AND JOINED WITH POLICE-REPORTED CRASH INFORMATION TO PROVIDE DATA-DRIVEN SAFETY INSIGHTS.

in Traffic Safety (PARTS) [15]. While currently focused on conducting analyses to gain insight into how advanced driver assistance systems (ADAS) perform in real-world scenarios, the PARTS vision is to expand to ADS. Vehicle content and other safety data is anonymized, pooled across organizations, and joined with police-reported crash information to provide data-driven safety insights—especially those related to system interdependencies. Data protection through a trusted third party builds trust from all participants, protecting driver privacy and preventing punitive responses to hazards, which stifle safety reporting.

A data sharing approach must be designed, through the use of a third-party aggregator and the anonymization of results, to not reveal participants' proprietary or sensitive data. It would anonymize and share information that highlights the "problem space" facing ADS vehicles; for example, hazard scenarios associated with a particular operational domain. Such a data sharing program supports evaluation of behavioral competencies and use cases for autonomous vehicles. Indeed, such a method of evaluating these systems has been proposed by Underwriter Laboratories (UL) in UL-4600: Standard for Evaluation of Autonomous Products [16]. This data should be protected by a trusted third party, with the resulting data and analytics anonymized and not attributed to a specific partner. Additionally, the operational model of the data sharing partnership should be designed to keep the data within the partnership (and not directly shared with outside organizations) to help build trust and prevent punitive responses to hazards and risks.

Based on MITRE's experience with PARTS and other data sharing public-private partnerships, we recommend an ADS data sharing effort be founded on a set of guiding principles.

- **Strictly for safety advancement:** Data and results will be used for safety only and not for competitive advantage.
- **Equal voice:** All participants, whether public or private, are peers. Decisions are made by consensus, with each participant receiving one vote.
- **Protection of data:** No participant will be able to access another PARTS participant's data or individual benchmark results.
- **Voluntary participation:** Participation is entirely voluntary. Participants may choose to end participation at any time.
- **Transparency:** Governance and security processes will be documented, reviewed, and approved by the Governance Board,



and decisions will be made in an open and transparent way among the participants.

- **Collaborative:** All participants will work together in good faith to achieve the goals of the partnership and strive for consensus.
- **Meaningful contribution:** All participants will contribute in a meaningful way, which may vary by study or project.

Hazard-Aware, Traceable Data Logging

Currently, there are no prescriptive requirements on data logging for autonomous vehicles. However, when an incident occurs, the only information available to identify root causes and mitigations is that data. In ADS systems, there is no guarantee of a human driver to question, whereas in non-fatal accidents involving traditional vehicles, interviews with drivers are a key component of the incident report. Manufacturers and ADS developers may be logging this information for various proprietary uses, but to fulfill the needs of safety analysts this data must be tied to specific hazards, be traceable, and must be updated iteratively as new hazards are discovered. Thus, a compulsory data logging standard that enables hazard root cause analysis is needed.

Recently, MITRE explored methods to leverage new research in top-down hazard analysis to

CURRENTLY, THERE ARE NO PRESCRIPTIVE REQUIREMENTS ON DATA LOGGING FOR AUTONOMOUS VEHICLES. HOWEVER, WHEN AN INCIDENT OCCURS, THE ONLY INFORMATION AVAILABLE TO IDENTIFY ROOT CAUSES AND MITIGATIONS IS THAT DATA.

inform data elements to log in an ADS. This method, called Systems Theoretic Process Analysis (STPA), provides a high-level approach for identifying hazards and decomposing them into causal factors. Dr. Nancy Leveson from MIT has researched how to apply this process to highly complex, software-intensive systems [17] and, continuing this research, other safety researchers [18] and industry [19] have applied this process to autonomous vehicle systems. MITRE added to this research by defining how the design constraints identified by STPA/System-Theoretic Accident Model and Processes (STAMP) models can be tied to data elements necessary to determine if a constraint is satisfied, thus tying the novel hazard analysis of STPA to data logging parameters.

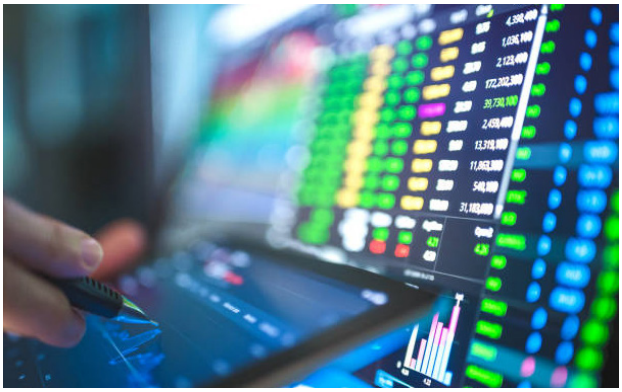
The National Transportation Safety Board (NTSB) has a similar recommendation. In its 2016 report regarding an ADS crash investigation, NTSB specifically states that the DOT should "define the data parameters needed to understand the automated vehicle control systems involved in a crash" and that NHTSA should "define a standard format for reporting automated vehicle control

systems data, and require manufacturers of vehicles equipped with automated vehicle control systems to report incidents, crashes, and vehicle miles operated with such systems enabled." [20] MITRE believes that this recommendation should be extended to state that such a set of data parameters should be tied not only to understanding vehicle control systems but also to the external hazards these systems face, with a clear method of iteratively improving this set of parameters as new hazards are discovered.

Additionally, such data logging can be leveraged for use-case and behavioral competency identification. If systems continuously fail in a specific scenario, safety researchers can identify the core components of the scenario that must be addressed to demonstrate safety. UL-4600, previously mentioned, recommends development and sharing of these use cases across industry to collectively address these hard problems. Thus, MITRE recommends that ADS developers be required to demonstrate a hazard-aware process for identifying and updating data elements within their data logger—to improve safety across the ADS operational domain.

Requirements for Systems Engineering Practices

As previously discussed, classical approaches to functional safety and systems engineering seem to be insufficient for ADS. The software complexity, the divergent nature of learning-based and non-deterministic algorithms, and the enormity of the operational design domain mean that new methods must be considered. There are a few new approaches to safety, listed below, that should be directly considered. However, regardless of the specific approach, MITRE believes a more prescriptive set of requirements or standards on safety-focused systems engineering



practices is necessary. When approaching extremely challenging technical problems such as autonomous driving, innovators often leverage a culture of speed and risk-taking to attack the problem. This focus provides significant benefit for innovation but may not provide benefit with respect to safe adoption of the solution. Providing a clear set of systems engineering best practices to these innovators will give a clear roadmap to follow—and allow industry to focus on the hard, unsolved challenges of autonomy.

MITRE's two specific recommendations regarding systems engineering practices center on:

- Effective, interdependency-aware hazard analysis for ADS vehicles
- Using use cases and behavioral competencies in the system design process

ADS DESIGNERS SHOULD LEVERAGE A MODERN SYSTEMS APPROACH FOR HAZARD ANALYSIS THAT RECOGNIZES THE COMPLEXITIES OF ADS COMPONENT INTERACTIONS.

These two recommendations can help address some of the safety considerations from traditional vehicle systems that are often hard to apply to autonomous vehicles. The recommendations also reflect the state of the art in ADS system safety practices.

First, ADS designers should leverage a modern systems approach for hazard analysis that recognizes the complexities of ADS component interactions. While functional safety is still important to consider for ADS components, it is insufficient on its own. Practices like Fault Tree Analysis and Failure Modes and Effects Analysis improve component-level safety, but to address system-level safety of non-deterministic, learning-based, and highly complex systems, additional approaches are needed. The STPA approach leverages STAMP models to approach safety engineering from a top-down, component- and interaction-aware model analysis. The basic concept of a control loop with a set of inadequate actions is extended all the way from component- and vehicle-level operations up through company management and to regulatory and legislative considerations. This design-focused hazard analysis is one way to consider systemic and interdependent system failures that result in unsafe behavior. A full systems engineering approach to safety may or may not consider STPA/STAMP specifically, but MITRE recommends that the safety framework pointedly address and implement an equivalent hazard analysis process.

Second, known hazard scenarios and behavioral competencies should be collected, evaluated, updated, and shared throughout the design, testing, and deployment of ADS. A group of researchers and industry representatives have partnered to produce the UL-4600 "Standard for Evaluation of Autonomous Products." This standard, coupled with effective hazard analysis, provides a method to answer the hard question throughout the design, test, and deployment of an ADS: "Did you think of this edge case?" Fundamentally, the design and testing of ADS systems is limited to design and scenario considerations that a specific implementer thinks of. A team designing in sunny and urban southern California may not properly consider the operational design domain of inclement weather in northern Michigan, or rural roadways in Wyoming. Furthermore, edge cases for ADS vehicles are defined by their specific weaknesses, such as novel object classification, which do not necessarily match our human understanding of edge cases. UL-4600 provides a way to document and share these safety cases and help all vendors prepare for hard problems and collectively address that growing list of "Did you think of this?" questions [21]. Including consideration of these ADS-specific use cases throughout the systems engineering process is key to designing a safe ADS system.

KNOWN HAZARD SCENARIOS AND BEHAVIORAL COMPETENCIES SHOULD BE COLLECTED, EVALUATED, UPDATED, AND SHARED THROUGHOUT THE DESIGN, TESTING, AND DEPLOYMENT OF ADS.

As stated above, these two example systems engineering approaches provide a tangible starting point for developing a full systems engineering approach to ADS development, but a full framework will likely uncover additional methodologies.

THE CERTIFICATION PROCESS MUST BE ADAPTIVE AND AGILE, AS AUTONOMY REMAINS AN UNSOLVED PROBLEM AND NEW APPROACHES TO SAFETY ARE LIKELY TO EMERGE.

Considering Communications, Spectrum, and Connected Vehicles

Due to challenges with initial deployment of connected vehicle communications, some ADS developers are designing without consideration for broad, cross-vendor connectivity. However, MITRE believes that connected vehicle technologies provide important safety and capability benefits, discussed below. Therefore, to improve ADS safety, MITRE recommends continuing to push toward broadly deployed connected vehicle capabilities.

For cross-fleet vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications (collectively known as V2X, or vehicle-to-everything), the following are needed:

- Message set standardization
- Funding to deploy technology
- Stakeholder buy-in to a particular set of capabilities
- Support from the federal government, state government, and industry participants.

The initial effort toward this capability was the Dedicated Short-Range Communications (DSRC) standard, codified in IEEE 802.11p. This specific technology had a dedicated wireless spectrum allocated by the Federal Communications Commission (FCC) in 1999, and prototype hardware has been available for some time. However, in late 2020, the FCC reallocated the majority of this spectrum to unlicensed wireless communications, with only 30MHz remaining dedicated to transportation safety [22], effectively ending the possible adoption of 802.11p.

An alternative technology, Cellular V2X (C-V2X), is a different approach to enable ADS to communicate with each other and with infrastructure. This technology received some of the spectrum from the FCC's DSRC spectrum allocation, and currently a variety of C-V2X prototype technologies are available. However, widespread C-V2X adoption has not occurred. Furthermore, as network latency is very important for ADS communications, C-V2X may rely on the deployment of broad 5G networks where localized infrastructure is not feasible. The rate of deployment of these networks is uncertain, and thus the rate of adoption of C-V2X may be slow.

It is important that regulators maintain dedicated spectrum resources for V2X technologies—be they DSRC, C-V2X, or some future communications framework. The operating domain for vehicles is very challenging, and any capability that simplifies part of this domain is critical in safe deployment. As one example, identification and tracking of other motor vehicles requires a variety of cutting-edge sensing and perception technologies, as

does detection of signage and other infrastructure. V2X removes errors caused by failures in these technologies. Vehicles that can communicate telemetry and perception information with each other reduce a significant risk in vehicle deployment; namely, operating safely among other vehicles and acting safely in a dynamic environment. MITRE believes that, over the long term, V2X is essential to safe ADS deployment. However, adoption and roll-out may be slow, as was seen by the now-defunct DSRC technology. Thus, aggressive protection of communications resources throughout the beginning of adoption is important. Additionally, unlike with the DSRC standard, if a new V2X implementation that is co-developed with industry and government partners shows promise in prototype tests, MITRE recommends that regulators require the technology in vehicles that are SAE level 3 or higher, as these systems execute complete vehicle control without effective low-latency human oversight. Such a requirement will increase the rate of deployment and mitigate significant safety challenges introduced by higher levels of automation.

Requiring Certification for SAE Level 3 or Higher ADS

Currently, regulatory oversight at the federal, state, and municipality levels has focused on guidance, recommendations, and best practices. As ADS technology increases in maturity and prevalence throughout the ground transportation space, however, MITRE expects that more prescriptive approaches may be required. NHTSA has recognized this in human-controlled vehicles with the Federal Motor Vehicle Safety Standards approach to codifying safety requirements for traditional automotive technologies. For ADS, the increased system complexity requires a delicate balance of requirements and regulations that do not stifle innovation and prevent technologists from making headway against the unsolved problem of autonomous driving. Thus, an evolving and flexible certification process should be used to provide a common set of requirements to design toward, with a set of scenarios and simulation requirements that enable a level of trust in the system, while also providing for data logging and analysis of fielded vehicles. This is especially important for highly automated vehicles, systems that rely primarily on ADS for safety and functionality.

FOR ADS, THE INCREASED SYSTEM COMPLEXITY REQUIRES A DELICATE BALANCE OF REQUIREMENTS AND REGULATIONS THAT DO NOT STIFLE INNOVATION AND PREVENT TECHNOLOGISTS FROM MAKING HEADWAY AGAINST THE UNSOLVED PROBLEM OF AUTONOMOUS DRIVING.

This component of the safety approach requires additional research and analysis to determine exactly what the certification process would entail,

and it would involve collaboration between industry leaders and regulators at the federal, state, and municipality levels. MITRE recommends that this certification process include:

- Business and organizational practices that promote safety as a key aspect of an ADS development process
- Systems engineering practices that help identify and mitigate both isolated and interdependent component- and system-level hazards
- Effective data logging requirements that address the hazard mitigation and systems engineering practices identified above
- Data and use-case sharing and analytics that reduce domain-wide ADS risk and promote safety across industry.

The certification process must be adaptive and agile, as autonomy remains an unsolved problem and new approaches to safety are likely to emerge. It must be performance-based and technology-agnostic. But as these systems are fielded, certification and independent review of ADS vehicles being deployed on our roads are necessary.

Conclusion

Automated driving systems and autonomous vehicle technology promise many transportation system improvements, from convenience such as shared mobility, to improved accessibility, to safer vehicles on the roads. However, the engineering and scientific challenges facing designers of these systems are substantial. Key challenges—notably, how to operate in a world with previously unseen obstacles, changing environmental conditions, and unreliable human drivers—mean that widely deployed self-driving vehicles remain elusive. As the technology continues to mature, a systematic and broad ADS safety approach should be embraced by industry, regulators, legislatures, and safety researchers as a method of bringing better safety practices to the development, testing, and deployment of these systems. Additionally, as the safety approach matures, it should be codified into a systemic ADS Safety Framework. Regulators have recognized this need in traditional vehicles and have codified it in the Federal Motor Vehicle Safety Standards, and states require their own levels of driver certifications through licenses and behavioral testing. By carefully and thoughtfully bringing evidence-driven and prescriptive sets of standards to the challenges in ADS, with a focus on flexibility and adaptability in how these challenges are met, these autonomous vehicle systems can be safely and effectively deployed—realizing their safety and capability promises.

This preliminary approach is focused on the unique opportunities that the rich data ecosystem on ADS platforms provides. It also highlights effective system and organizational safety practices that are tailored to highly complex cyber-physical systems. Key recommendations include effective data logging and sharing; collection, dissemination, and action on key safety cases surrounding autonomy; a robust organizational safety culture; protecting the future of connected vehicle technology through spectrum and capability identification; and throughout, action toward certification of autonomous systems seeking deployment on public roads. These recommendations are made based on MITRE's decades of experience in transportation safety and in automated vehicle and artificial intelligence research. While not solving all technical challenges, or "proving" system safety, these steps are necessary to start down the path of widely deployed, safe, and effective ADS technology.

References

[1] I. Boudway, "Waymo Begins Fully Driverless Rides for All Arizona Customers," 08 10 2020. [Online]. Available: https://www.bloomberg.com/news/articles/2020-10-08/waymo-one-app-offers-driverless-alternative-to-uber-in-arizona. [Accessed 31 12 2020].

[2] S. Kitajima, K. Shimono, J. Tajima, J. Antona-Makoshi and N. Uchida, "Multi-agent traffic simulations to estimate the impact of automated technologies on safety," Traffic Injury Prevention, vol. 20, pp. S58-S64, 2019.

[3] Energetics, Inc & Z, Inc, "Study of the Potential Energy Consumption Impacts of Connected and Automated Vehicles," U.S. Energy Information Agency, 2017.

[4] D. Holland-Letz, M. Kasser, B. Kloss and T. Muller, "Start me up: where mobility investments are going," McKinsey & Company, 2019.

[5] C. Gold, D. Dambock, L. Lorenz and K. Bengler, "Take over! How long does it take to get the driver back into the loop?," Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 57, no. 1, pp. 1938-1942, 2013.

[6] ISO/IEC, "26262:2011," Road Vehicles -- Functional Safety, 2011.

[7] Department of Defense, "Department of Defense Standard Practice, System Safety," MIL-STD-882E, 2012.

[8] P. Koopman and M. Wagner, "Challenges in Autonomous Vehicle Testing and Validation," SAE International Journal of Transportation Safety, pp. 15-24, 2016.

[9] National Highway Traffic Safety Administration, "Framework for Automated Driving Systems," 19 11 2020. [Online]. Available: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/ads_safety_principles_anprm_website_version.pdf. [Accessed 19 02 2021].

[10] P. Koopman and B. Osyk, "Safety Argument Considerations for Public Road Testing of Autonomous Vehicles," SAE International Journal of Advances and Current Practices in Mobility, vol. 1, no. 2, pp. 512-523, 2019.

[11] N. Kalra and S. M. Paddock, "Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?," RAND Corporation, 2016.

[12] W.K. Kellog Foundation, "Developing and Using a Logic Model," Jan 2004. [Online]. Available: https://www.wkkf.org/resource-directory/resources/2004/01/logic-model-development-guide. [Accessed 01 Mar 2021].

[13] K. Hollinger and H. Shirazi, "Management of Safety Risk in Automated Driving Systems," 2020. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-20-3326-management-of-safety-risk-in-automated-driving-systems.pdf. [Accessed 29 1 2021].

[14] J. L. LaReau, "GM: We encourage employees, dealers to tattle after ignition switch crisis," Detroit Free Press, 6 9 2019. [Online]. Available: https://www.freep.com/story/money/cars/general-motors/2019/09/06/gm-ignition-switch-nhtsa-recalls-safety-defects/2099289001/. [Accessed 29 1 2021].

[15] National Highway Traffic Safety Administration, "PARTS Partnership for Analytics Research in Traffic Safety," [Online]. Available: https://www.nhtsa.gov/parts-partnership-for-analytics-research-in-traffic-safety. [Accessed 19 02 2021].

[16] Underwriters Laboratories Inc., "ANSI/UL 4600".Standard for Evaluation of Autonomous Products.

[17] N. Leveson, C. Fleming, M. Spencer and J. Thomas, "Safety Assessment of Complex, Software-Intensive Systems," SAE International Journal of Aerospace, vol. 5, no. 1, pp. 233-244, 22 10 2012.

[18] M. Stoltz-Sundes, "STPA-Inspired Safety Analysis of Driver-Vehicle Interaction in Cooperative Driving Automation," KTH Royal Institute of Technology, 2019.

[19] Waymo, "Wayo Safety Report," 2020. [Online]. Available: https://storage.googleapis.com/sdc-prod/v1/safety-report/2020-09-waymo-safety-report.pdf. [Accessed 29 1 2021].

[20] National Transportation Safety Board, "Accident Report NTSB/HAR-17/02 PB2017-102600," 2016. [Online]. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/HAR1702.pdf. [Accessed 29 1 2021].

[21] P. Koopman, U. Ferrell, F. Fratrik and M. Wagner, "A Safety Standard Approach for Fully Autonomous Vehicles," WAISE, 2019.

[22] Federal Communications Commission, "In the Matter of Use of the 5.850-5.925 GHz Band: FIRST REPORT AND ORDER, FURTHER NOTICE OF PROPOSED RULEMAKING, AND ORDER OF PROPOSED MODIFICATION," Washlington, D.C., 2020.

ABOUT THE AUTHOR

Zachary LaCelle is an Autonomous Systems Principal at The MITRE Corporation. He leads MITRE's Mobile Autonomous Systems Experimentation Lab, which serves as a resource for government and research partners enabling prototyping, experimentation, testing, and analysis of autonomous and automated systems—across the defense, security, and transportation domains.

MITRE's Mission

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®