MITRE

MANAGEMENT OF SAFETY RISK IN AUTOMATED DRIVING SYSTEMS

by Kent V. Hollinger, Hamid Shirazi

Abstract

Automated Driving Systems (ADS) hold great promise for improving safety by helping prevent crashes resulting from human error. However, ADS developers need to demonstrate they are effectively managing new safety risks posed by mechanical and system failures—failures that may result in severe outcomes without mitigation by a driver. Proactive management of safety risk in the design, testing, demonstration, and deployment stages of ADS development can ensure continuous reduction in safety risk and build public trust over time. This paper details the potential benefits of establishing a formal program to manage safety risks in the ADS industry where hazards are systematically identified and analyzed, and unacceptable risks are mitigated and monitored through collection of relevant safety data.

Background

A formal risk management program establishes a systematic approach to managing safety risk in an organization. It is important that the program begin with executive management's commitment to a policy promoting safety as one of the organization's top priorities. Such a policy shapes the way everyday business is conducted. The program creates a framework where existing and new safety hazards in the organization's operation or product are identified and reported for risk analysis. The program also provides analytical tools for assessing the risk and measuring it against what the organization has established is an acceptable level of risk. If the risk is found unacceptable, a risk management process puts in place control actions and mitigations to reduce the risk to acceptable levels. The process calls for periodic measurement of the effectiveness of the control actions and mitigations to ensure objectives are met and that their implementation has not introduced new hazards.

A functional risk management program includes a systems analysis that explains the functions and interactions among the hardware, software, people, and environment in which the system operates. This analysis is used to proactively identify hazards before new or revised systems or procedures are put into place.

Models of Safety Risk Management Programs

Risk management programs are not new to safety sensitive industries. Variations of risk management programs have been implemented over the past several decades in many industries. For example, nuclear energy, oil and gas, healthcare, chemical, infrastructure construction, defense, space, and aviation industries have all adopted programs geared toward managing safety risks. While the programs have slightly different names and are at various stages of development or implementation, their goal is the same: to proactively protect people and property from undue harm. Often, industries were prompted to initiate risk management programs tailored to the need of their industry in response to a large-consequence accident. Examples include the United States Navy's Submarine Safety Program (SUBSAFE), created in response to the loss of the USS Thresher (SSN-593) in 1963 (NNBE Benchmarking Team, 2002); the nuclear industry's Safety Management

System (SMS), which includes safety risk management in response to the Chernobyl disaster in 1986 (International Nuclear Safety Advisory Group, 1991); and NASA's Safety and Mission Assurance, which was in response to the loss of the Space Shuttle Columbia (NNBE Benchmarking Team, 2002).

The transportation industry also has experience with programs intended to manage safety risks. In aviation, for example, the Federal Aviation Administration (FAA) has mandated safety risk management as part of its SMS implementation for scheduled commercial airlines and is considering mandates for additional aviation stakeholders. Also, the Federal Transit Administration (FTA) has mandated SMS for public transit agencies. While the National Highway Traffic Safety Administration (NHTSA) has not required automobile manufacturers to implement risk management programs, some manufacturers have realized the necessity and have moved in that direction.

Examples of such initiatives include creating a formal safety champion position with direct access to the top management team; setting up safety field investigation teams responsible for identification and analysis of identified and reported safety concerns from employees, dealers, and customers; and devising a new division responsible for evaluating the safety impact on the whole vehicle due to a change in one part or system (LaReau, 2019).

Safety Risk Management for ADS Developers

An ADS is basically an integration of various individual automated systems—such as perception, classification, and control generation—working together to make automated driving a reality. Many technologies are being evaluated to increase the reliability of these systems, including lidar, radar, sonar, and photography. The Society of Automotive Engineers (SAE) categorizes vehicle autonomy in six levels from zero to five: no automation, driver assistance, partial automation, conditional automation, high automation, and full autonomy. To move up a level, lower levels of autonomy must first be fully tested and safely implemented (Yigitcanlar, 2019).

The implementation of a structured risk management program in a mature industry brings about notable benefits, such as the continuous safety improvements achieved in the nuclear and aviation industries. The benefits may be more profound in an evolving industry such as ADS, which is confronting multifaceted complexity and a large degree of change. As safety responsibility shifts from human drivers to automated systems, a risk management process provides a structured framework required for identifying hazards and installing controls and mitigations to address safety risks.

While there are multiple regulations governing the design of driver-controlled automobiles that can be leveraged, they define only the minimum acceptable level of risk. There is no standard or regulation that defines a minimum acceptable level of risk for ADS. Thus far, regulators have left it up to

the ADS developers to identify and manage safety risks in their products. ADS technology exhibits several characteristics, such as new technology, uncontrollable, involuntary, and luxurious (D. Litai, 1983) that could be perceived as riskier by the public than traditional human controlled vehicles. New technologies are perceived 10 times riskier than old technologies, uncontrollable risks are perceived 5 to 10 times riskier than controllable risks, involuntary risks are perceived 100 times riskier than a voluntary risk, and luxurious risks are perceived 7 times riskier than a necessary risk (D. Litai, 1983). For ADS technology to gain public trust, the technology may therefore be expected to achieve or exceed safety levels similar to those of buses, trains, and airlines (Figure 1). Also, since the technology limits how and when drivers can interfere with the operation of the vehicle, specifically in higher levels of ADS, developers bear more responsibility for identifying safety issues and addressing them before harm results.

For an effective risk management program, ADS developers may consider taking a transparent approach to risk management where employees and the public are encouraged and rewarded for reporting safety concerns through established and easily accessible mechanisms. In this approach, employees recognize that everybody plays a role in safety management and there is no fear of retribution for reporting honest mistakes.

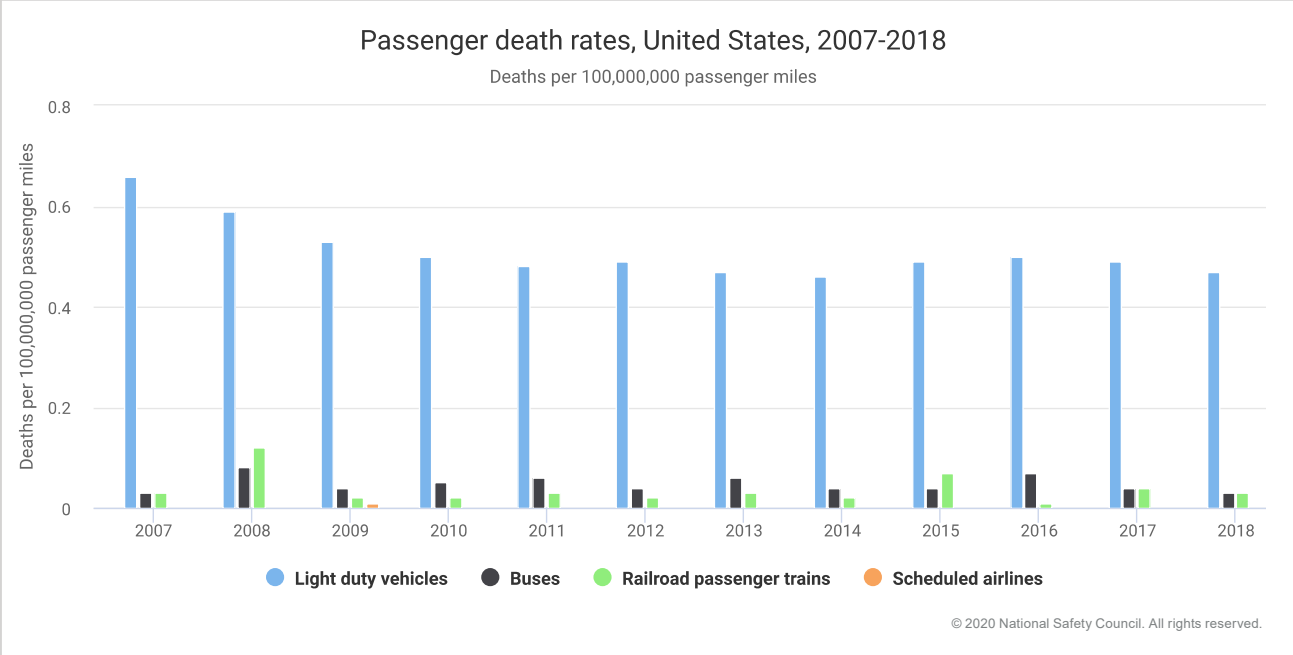

FIGURE 1. COMPARISON OF DEATH RATES BY MODE OF TRANSPORTATION

Gathering from other industries' experiences with risk management programs, the ADS industry may adapt common tools such as Failure Modes and Effects Analysis (FMEA) and bowtie modeling (Figure 2) for assessment of the product and organizational structure, processes, and interfaces to detect hazards, analyze their effects, and mitigate their resulting safety risks.

The following sections describe the role a risk management program could play in different stages of ADS technology.

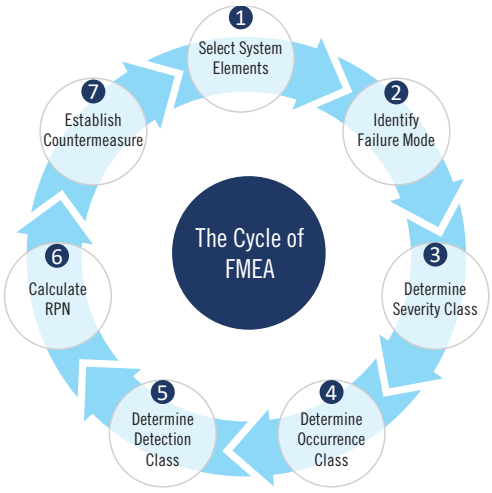

FIGURE 2. COMMON ANALYTICAL TOOLS FOR RISK MANAGEMENT: FMEA CYCLE

(Jeon, 2020)

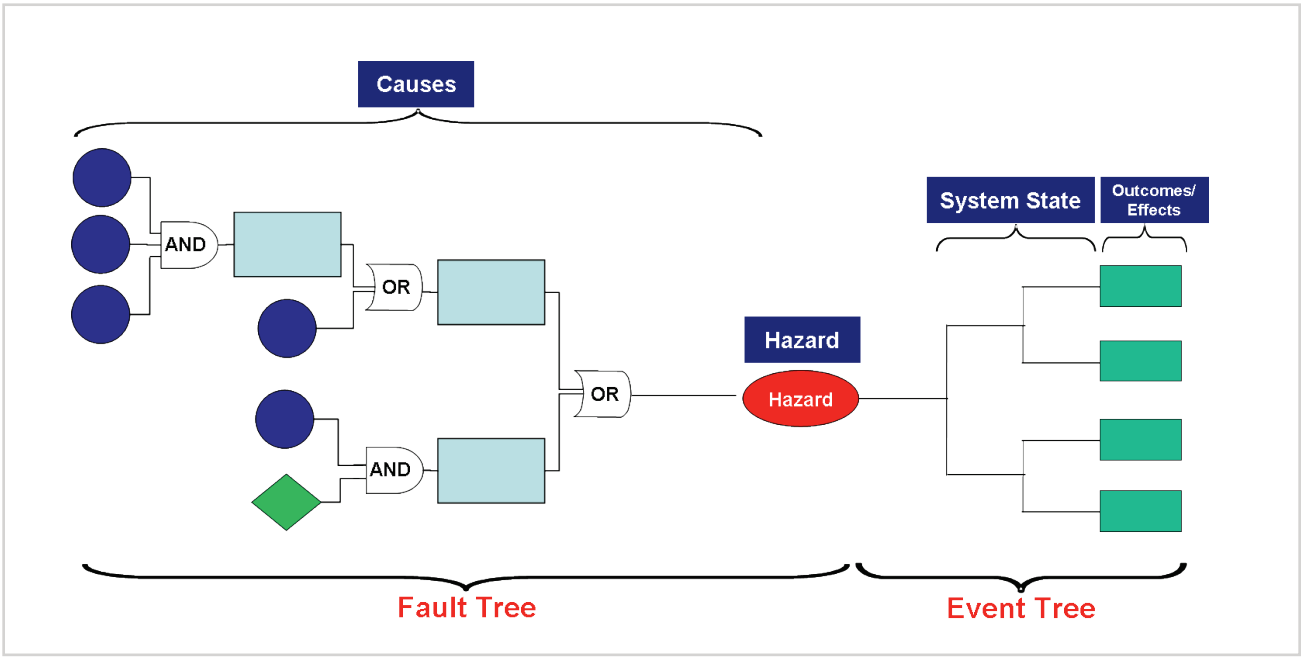

FIGURE 3. COMMON ANALYTICAL TOOLS FOR RISK MANAGEMENT - BOWTIE MODEL

(*FAA Safety Risk Management Guidance for System Acquisitions, Air Traffic Organization, March 2020*)

Risk Management Program in ADS Design

A systematic risk management program assures safety is designed into products, rather than relying upon inspections and testing to find faults or safety concerns. Features designed into the product protect against unacceptable failure events by reducing the probability and severity of potential outcomes. Ideally, ADS developer members who are evaluating the adequacy of the designed protections should be organizationally independent from members setting production objectives. These members should also validate that existing standards for design and testing are properly addressed.

To supplement existing design standards in the ADS industry, standards from other safety-critical industries may be evaluated for implementation. For example, the safety standards airplane manufacturers use could be leveraged by ADS developers in developing their software applications. As in the ADS industry, airplane manufacturers have incorporated complex software applications in the design of modern airplanes and their failure may result in catastrophic outcomes. For example, RTCA DO-178C is a software standard the aviation industry uses to account for the possibility of such failures and to mitigate the potential outcomes through increased rigor.

Risk Management Program in ADS Testing and Demonstration

The testing and demonstration phases ensure that the design and manufacturing processes meet their design intent and the integrated test vehicles perform as intended.

A Quality Management System can supplement a risk management program by monitoring findings from the testing and demonstration phases. This includes monitoring products and services integrated from outside sources in ADS-dedicated vehicles. In the testing and demonstration phases, ADS developers collect data to confirm whether pre-defined practices are being followed. These phases typically involve the operational management responsible for the system(s) being evaluated.

Having an independent group within the organization conduct evaluations at planned intervals helps ADS developers determine if risk management methods and practices are meeting safety objectives and expectations. Evaluation planning should consider the safety criticality of the processes that are being evaluated. The scope, content, and frequency of evaluations should be based on the need for the assessment of operational risks.

Inputs from field employees testing the vehicle are important data, as these employees may observe aspects of the operation or the environment that were not expected or not included in evaluation protocols. A confidential employee reporting system can formalize this data collection process.

ADS developers establish traceability to the environmental test categories such as temperature variation, humidity, vibration, waterproofness, sand

and dust, magnetic effect, and voltage spikes. This capability can provide permanent records related to those categories, which may be used as an additional data source for testing evaluations.

Risk Management Program in Vehicle Deployment

As the public begins using ADS-dedicated vehicles, ADS developers should continue to monitor the safety of the operations through vehicle performance evaluations to detect quality escapes and areas for design improvements. Data acquired through in-service monitoring is analyzed to detect trends and identify hazards, which then become inputs to a risk management process. Due to the scope and mutability of the operational environment, such continued data analysis is critical for ADS technology since unforeseen conditions are likely to arise.

In-service monitoring provides the confidence that ADS-dedicated vehicles are meeting the developers' safety objectives and that the mitigations developed as part of a safety risk management process are effective. When objectives are not met, the in-service data allows the ADS developer to continuously improve the safety and effectiveness of driving algorithms. Each developer can learn from its own failures and those of similar developers if safety data is properly shared.

Key Opportunities for Shared Safety Advancements in ADS Technology

For successful implementation of a formal program to manage safety risk in the ADS industry, research is needed to develop safety benchmarks, safety metrics and performance indicators, and to devise data collection and sharing mechanisms and protocols.

Industry-wide safety benchmarks can be established from aggregated and anonymized data shared by ADS developers. The availability of such benchmarks may help bridge gaps in industry-wide standards and regulations. Data-driven safety benchmarks may help to inform government authorities tasked with oversight of ADS. That data could help them enhance guidance or regulations and might also be used to shape public expectations. When industry safety benchmarks are established, individual ADS developers may monitor their own safety performance against the rest of the industry and establish goals for improvements.

Another important research question is whether automated vehicle system performance should be benchmarked against human performance or against another metric—and if the system must perform like a human to gain public trust.

The development of safety metrics to measure the state of safety risk in ADS technology is another important item on the research agenda. Safety metrics are tied to the stage of the technology's development. While some metrics must account for the technology in the design stage, others are relevant only when the technology is being

tested with human-in-the loop simulations, or during constrained field testing. As the technology meets target levels of safety in such controlled environments, safety metrics are needed to assess its performance for deployment in environments where the ADS-dedicated vehicle is mixed with real traffic.

While crash rate is certainly a relevant metric, other metrics that constitute undesirable behaviors, such as near misses, must be devised as well. A ranking scheme may be required to account for the severity of such events. Also, while instances of driver intervention as a response to a perceived safety event could be viewed as a metric, drivers' perceptions of what constitutes a safe drive are not consistent; that should be accounted for in the development of the metric. Perceived safe driving may be influenced by a variety factors, including demographics, driving style, personality, and regional and social influences.

Most important of all, and probably most challenging, is gathering data to support analysis of safety metrics and performance measurements. Research is required to identify what data must and can be made available for these analyses. Automated Vehicle Safety Consortium (AVSC) has developed a best practice for ADS data collection and event reconstruction (AVSC, 2020).

Data on safety events is relatively scarce. The ADS industry would benefit if developers were able to learn from each other's mishaps. Given the sensitivities involved in safety data sharing between companies, it might be possible for the industry to adopt an approach similar to the one aviation has used, where the motto is "We don't compete on safety."[1] If ADS developers decide to take some form of that approach, a trusted entity may be established to intake safety-relevant data from participating ADS developers and share aggregated de-identified findings with them.

Conclusions and Recommendations

Limited industry-wide safety standards and regulations have led ADS developers to make their own safety risk acceptance decisions. Adoption of a formal risk management process, as other industries have done successfully, will provide ADS developers with a systematic approach to managing safety risk in their organization and in their product. Extensive testing and in-service monitoring are critical processes for an emerging technology such as ADS since serious unforeseen conditions may be revealed upon initial public deployment. Data acquired through testing and public deployment monitoring should be analyzed to detect trends and other hazards. These trends and hazards then become inputs to risk management programs to determine if the risk is acceptable or if mitigations are required. The ADS industry would benefit from developers learning from each other's mishaps and abnormal operations by sharing safety data for common analysis. This may be achieved through the establishment of a trusted third party that intakes safety-relevant data from ADS developers and shares aggregated de-identified analysis findings to participating entities. The Partnership for Analytics Research in Traffic Safety (PARTS)[2], Aviation Safety

1. Steve Dickson, Administrator, Federal Aviation Administration

Information Analysis and Sharing (ASIAS)[3], and Data4Safety (D4S)[4] programs are strong examples of such experiences in data sharing and analysis.

The experience gained in other industries through research and development in risk management programs can be leveraged within the ADS industry. Elements such as safety gap analysis, creation of a positive safety culture to engage the entire organization in the identification of hazards, and collecting data for analysis of potential hazards are example activities that are relatively mature in other industries and could be tailored for the ADS industry.

ADS developers would enhance safety by:

- adapting proven risk management processes
- developing consensus-based safety and performance metrics
- collecting and analyzing operational data during testing and deployment
- sharing safety data across the ADS industry

2. https://www.transportation.gov/briefing-room/us-transportation-secretary-elaine-l-chao-announces-new-initiatives-improve-safety
3. https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18195
4. https://www.easa.europa.eu/newsroom-and-events/news/data4safety-partnership-data-driven-aviation-safety-analysis-europe

Bibliography

AVSC. (2020). AVSC Best Practice for Data Collection for Automated Driving System-Dedicated Vehicles to Support Event Analysis. *https://avsc.sae-itc.org/*.

FAA Safety Risk Management Guidance for System Acquisitions, Air Traffic Organization, March 2020.

International Nuclear Safety Advisory Group. (1991). Safety Culture. *Safety Series.*

Jeon, H. (2020). Comparison and Verification of Reliability Assessment Techniques for Fuel Cell-Based Hybrid Power System for Ships. *J. Mar. Sci. Eng.*, 8(2), 74.

LaReau, J.L. (2019). GM: We Encourage Employees, Dealers to Tattle After Ignition Switch Crisis, Detroit Free Press. *https://www.freep.com/story/money/cars/general-motors/2019/09/06/gm-ignition-switch-nhtsa-recalls-safety-defects/2099289001/*

Litai D., Lanning D.D., Rasmussen N.C. (1983). The Public Perception of Risk. In: Covello V.T., Flamm W.G., Rodricks J.V., Tardiff R.G. (eds) The Analysis of Actual Versus Perceived Risks. Advances in Risk Analysis, Volume 1. Springer, Boston, MA.

NNBE Benchmarking Team. (2002). NASA/Navy Benchmarking Exchange, Volume 1.

Yigitcanlar, T. (2019). Disruptive Impacts of Automated Driving Systems on the Built Environment and Land Use: An Urban Planner's Perspective. *J. Open Innov. Technol. Mark. Complex*, 5(2), 24.

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™