MITRE

12 April 2018
83 FR 12933

Public Comments Processing
Attn: Docket No. FMCSA-2018-0037
Federal Motor Carrier Safety Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
West Building, Ground Floor, Room W12-140
Washington, DC 20590-0001

Attention: Docket No. FMCSA-2018-0037

The MITRE Corporation is pleased to submit this response to the Federal Motor Carrier Safety Administration's Request for Comment on Barriers to the Safe Testing and Deployment of Automated Driving System-Equipped Commercial Motor Vehicles on Public Roads. Given the rapid transformation in Automated Driving Systems (ADS) for commercially available vehicles, it is critical that data-driven safety evaluation techniques be implemented to ensure safe and efficient adoption of these automated systems.

In 1958, MITRE provided the technical know-how and operational excellence to pioneer the nation's first air defense system and air traffic control system. Today, MITRE works across the whole of government to tackle difficult problems that challenge the safety, stability, security and wellbeing of our nation through its operation of Federally Funded Research and Development Centers as well as public-private partnerships. With a unique vantage point working across federal, state and local governments, as well as industry and academia, MITRE works in the public interest to discover new possibilities, create unexpected opportunities and lead by pioneering together for public good to bring innovative ideas into existence in areas such as AI, autonomous intelligent systems, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy automation, cyber threat sharing and cyber resilience. MITRE's mission-driven team is dedicated to solving problems for a safer world.

1 SUMMARY

Automated Driving Systems (ADS) are propagating through the private vehicle market, and provide possible safety improvements over human-driven vehicles. In the commercial vehicle space, these improvements also provide the possibility of increasing freight reliability. These technologies have the possibility of saving many lives by reducing the human failure that is implicated in more than 90% of motor vehicle crashes. To encourage this adoption, the Federal Motor Carrier Safety Regulations (FMCSRs) must be examined and updated to support these new technologies.

However, often the assumption is that ADS can only improve safety. This may not be the case—there is additional risk added from ADS technology which is not present with traditional

vehicles. Due to the immense complexity of designing ADS systems which interact with a dynamic and unpredictable world, this new risk is hard to quantify and mitigate[1]. With large, heavy vehicles operating around human-driven passenger vehicles and static infrastructure, the cost of failure is high. Still, through careful implementation, test, and evaluation of these systems, ADS technology has the potential to make our roads and highways significantly safer and more efficient.

As stated in the RFC, this information is focused on scenarios where the automated system is primarily responsible for monitoring the driving environment (SAE Levels 3-5).

MITRE encourages FMCSA to adopt a data-driven, security-aware, verification-focused approach to adoption of ADS technology into the commercial motor vehicle space—driven by testable, performance-based standards instead of prescriptive regulation. The following sections detail this approach.

2 DETAILED COMMENTS FOR BARRIERS TO THE SAFE TESTING AND DEPLOYMENT OF AUTOMATED DRIVING SYSTEM-EQUIPPED COMMERCIAL MOTOR VEHICLES

2.1 Informing Performance-Based Standards, Analytics, Evaluation, and Testing

Our suggested approach is to use data-driven safety analytics to inform performance-based standards and requirements. Specifically, data should be shared across commercial vehicle technologies and suppliers to enable industry-wide safety improvements. Also, these technologies must be implemented with careful evaluation of cyber security concerns. Finally, as current Commercial Motor Vehicles (CMVs) are inspected annually and at roadside inspection points, testing must be considered for Automated Driving System (ADS) components which supplant human operator decision-making. Each section below details methods supporting this approach.

2.2 Data Sharing for Safety Analytics

FMCSA would like to understand a driver's experience with ADS technologies in real-world settings through receiving and reviewing data and information from the private sector. Sharing data is not innate, and exposes the data provider to risk. Data sharing requires a successful data-driven, proactive safety culture enabled by a new model—a voluntary data-sharing partnership between industry and government, grounded in core principles, in a trusted environment.

An example of a successful data-driven safety culture is commercial aviation's safety information sharing and voluntary safety enhancement partnership. Together, these key efforts enable participants to monitor known risks, evaluate the effectiveness of deployed mitigations, and detect emerging risks. This has enabled air travel to be safe and trusted, and enabled government and industry to move from reacting to crashes to proactively identifying risks.

[1] *Koopman, P; Wagner, M. (Jan 2016). "Challenges in Autonomous Vehicle Testing and Validation." https://doi.org/10.4271/2016-01-0128*

To ensure that data and safety measures can be assessed across the industry in a consistent way, MITRE recommends that FMCSA continue engaging with industry and exercise its broad authority to encourage and enforce data standardization for ADS technology to support safety analytics. Event Data Recording (EDR) technology specifically adapted to ADS and required in all ADS vehicles will enable this effort. This includes coordinating with SAE to extend J1698 defining event data recording for traditional ground vehicles to include ADS-specific information. Such information could include vehicle obstacle data obtained from sensors, control trajectories generated by behavior modules, and localization information determining vehicle location in the environment. Extending an existing standard and adapting it to ADS enables a backwards comparison to non-ADS CMVs. This would enable FMCSA and industry to assess whether a CMV equipped with ADS technology is being operated as safely as a traditional CMV operating on a public roadway. Additionally, new or extended standards for non-traditional (i.e. non-CAN-bus) standards may be necessary, as ADS system component data requirements often fall outside of the bounds of current automotive data bus capabilities.

To evaluate how a driver is using an ADS-equipped commercial vehicle, MITRE recommends focusing on the causal factors to emerging safety issues to get ahead of systemic safety risk through voluntary reporting of safety issues and events that come to the attention of drivers. The commercial aviation industry has been successful in using the data that comes out of their program (Aviation Safety Action Program (ASAP)) to enhance safety through the prevention of crashes.

All voluntary data sharing efforts will be moot without the appropriate legal protections. All voluntarily shared data from industry must be protected from disclosure and punitive action. For example, the FAA provides confidentiality under FAR CFR 14 Part 193, which outlines the protection of voluntarily submitted information. FMCSA does not currently have a provision and will have to develop confidentiality protections to create an environment conducive to data-sharing.

2.3 Cyber Security Concerns for ADS in CMV

As recent industry papers and National Highway Traffic Safety Administration (NHTSA) documents[2] have discussed, concerns about minimizing risks to safety must include cybersecurity threats and vulnerabilities. As mentioned above in this RFC response, ADS must be examined for additional safety issues even while providing safety improvements. Since ADS technology is significantly more complicated than traditional automotive control software or mechanical design, system complexity is greatly increased in ways not previously seen in the ground transportation sector. This software complexity leads to the prospect of harm, possibly through purposeful intent of a malicious actor—something demonstrated in multiple industrial sectors. This increased complexity in ADS is a benefit to would-be attackers, given the potential of sending misleading data to (i.e. spoofing) sensors, anticipating and exploiting predictable automated responses of ADS software algorithms, and from discovering and maliciously

[2] *National Highway Traffic Safety Administration. (2017). "Automated Driving Systems 2.0 – A Vision for Safety".* https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf

exploiting new system flaws in the implementation, configuration, and algorithms of the software. CMVs offer an enticing target for bad actors, given their size or purpose (e.g. first responders, hazmat vehicles). Also, cybersecurity exposures are often direct safety exposures, since system and environment conditions could trigger the activation of an ADS cybersecurity flaw with harmful results. Current concerns for cybersecurity for CMVs manifest in actions such as the National Motor Freight Traffic Association (NMFTA) series of meetings on current CMVs even without ADS augmentation[3] and DHS research efforts.

ADS on CMVs require renewed attention to regulations for standardization of requirements for data to be collected and monitored, as mentioned earlier. Existing data gathering and analysis approaches will need a fresh view, refocused on a cybersecurity and ADS perspective. In consideration of both increasing system complexity and the possibility of active, intentional compromise, and given inability to forecast new cybersecurity attack methods, the type and detail of data required will likely need to be more comprehensive, and include more introspective and complete status of ADS components and overall sensor and vehicle status. Development of supporting specifications should be done as an open initiative to arrive at a shared industry approach to what can be provided and how, an approach that will be far from simple to define, and will need a diversity of viewpoints to achieve good standards. The requirements need also consider active monitoring, not just data recording, given the new connected vehicles setting.

Actions undertaken should be considered from a connected vehicle context for CMVs with ADS. CMVs require remote connection to cloud or infrastructure based systems, given ADS requirements for access to outside information sources. Fleet management mechanisms, already widely used for economic benefits, will become more prevalent with arrival of ADS enabled vehicles. These external vehicle connections form an additional path for cybersecurity concerns and extend the safety concerns to the CMV's fleet and the supporting infrastructure. Maintenance systems are also part of that cybersecurity assessment since compromises can enter through the common infrastructure points that service the CMVs. To help mitigate concerns, fleet management data that is transmitted, either by CMV operators or by systems themselves, should be required to include full system status information—allowing for not only augmented forensic data availability to facilitate analysis, but future possible active response mechanisms given CMV with ADS connectivity to the related infrastructure.

2.4 Inspection of ADS Components

Per the FMCSRs §396, CMV must be inspected annually as well as daily by the ADS drivers. Since ADS systems at SAE level 3 and higher supplant driver decision-making, it stands to reason that they must also be inspected to maintain safe operations of the vehicle. The RFC's question, "How should motor carriers ensure the proper functioning of ADS prior to operating in an automated mode?", highlights this concern.

[3] *For example, see Heavy Vehicle Cybersecurity meetings held by NMFTA (www.nmfta.org)*

In the report on FMCSRs and ADS issued by Volpe[4], they point out two sections of interest which are worth stating here. §393.3 states "The use of additional equipment or accessories in a manner that decreases the safety of operation of a commercial motor vehicle in interstate commerce is prohibited," and §396.3 states, in part, that "Parts and accessories shall be in safe and proper operating condition at all times." Especially for highly autonomous systems, MITRE encourages FMCSA to extend the equipment covered under these sections to include components of autonomy systems which directly affect safety—notably, sensing systems and control systems. Volpe underscores the necessity for this extension: "It remains unclear whether adding automated driving technologies could inadvertently cause or contribute to a breakdown of a vehicle," adding that "FMCSA may wish to initiate research on the performance of AV systems at increasing levels of degradation (e.g., wear on or damage to sensor surfaces) in order to inform the development of inspection procedures and criteria." MITRE concurs with this conclusion.

Further, as the operation of the vehicle is a combination of the vehicle automation capabilities along with the control paradigm of the fleet (e.g. onboard-safety driver, onboard technician, or remote supervisor), the inspection must be relevant to this combination—referred to as "Concept Group" in the Volpe report. Towards this purpose, we propose extending the §396.3(2)(b)(1) identification of the vehicle to include the SAE automation level as well as the "Concept Group". Further, §393 (parts and accessories required for safe operation) should be extended to include sensors and controllers, as well as requiring ADS software to be patched and updated as required for safe and secure operation.

With regards to extending §396.11 (2) to include defects in sensors and controllers as well as ADAS software, MITRE recognizes the difficulties and complexity in testing ADS software. This effort may have to be performed in non-traditional ways, such as requiring the carriers to maintain a repository of events in which the ADAS system malfunctioned or had to be disengaged within its ODD (similar to disengagement reports required by California DMV), which are then analyzed during the annual inspection. Other aspects may include exercising a critical set of testing scenarios and "Core Competencies" such as requiring ADAS coming to a safe state (including transfer to a driver/technician on the vehicle or a remote operator as applicable within the "Concept Group") when sensors are degraded or fail, or when a vehicle transitions to a scenario outside of its Operational Design Domain (ODD).

3 CONCLUSION

As Automated Driving Systems (ADS) become a reality, possibilities exist for safety improvements, mobility opportunities, and efficiency enhancements. Human error and limitation causes most accidents and crashes; these technologies thus pose an opportunity to save lives and improve commercial transportation. However, the technology is young and unproven—and carries with it additional risk. MITRE believes that taking a data-driven, analytic approach to

[4] *John A. Volpe National Transportation Systems Center. (Mar 2018). "Review of the Federal Motor Carrier Safety Regulations for Automated Commercial Vehicles." https://www.regulations.gov/document?D=FMCSA-2018-0037-0003*

system safety, testing, inspection, and certification will help ensure consumer confidence and acceptance of these systems into the Commercial Motor Vehicle (CMV) fleet.

The replacement of the human driver with an automated system necessitates more stringent cyber security analysis, data collection, and system inspection and evaluation. Otherwise, the system cannot provide insight into its actions, and tracing failures or near misses becomes difficult. FMCSA should first enable data-driven security and safety analytics for ADS technologies in CMV fleets, then use this data to inform updates to the FMCSR to enable safety, reliability, and efficiency through novel ADS capabilities.

The MITRE Corporation appreciates FMCSA's consideration of these comments for moving Automated Driving System technology forward. Should you have questions, please contact transportation@mitre.org.