Human Factors in Transportation, Vol. 95, 2023, 354–366
https://doi.org/10.54941/ahfe1003820

Cybersecurity Best Practices for Managing Mixed Fleets

Xiaojian Jin[1], Elena Griffor[1], and Thomas Cannon[2]

[1]Virginia Tech Transportation Institute, Blacksburg, VA 24061, USA
[2]Pronto.AI, San Francisco, CA 94103, USA

ABSTRACT

This paper presents an overview of cybersecurity best practices for mixed fleets containing both vehicles with and without automated driving systems (ADS). It primarily focuses on the security of ADS-equipped commercial motor vehicle (CMV) fleets that integrate some degree of automated driving capabilities. The paper also provides a concise summary of prior research on the topic. The owners and operators of such fleets are naturally concerned about the potential threats and vulnerabilities that may arise from ADS technologies and their impact on the security of their operations. To address these concerns, this paper provides sections on general and specific cybersecurity best practices. The target audience for this overview includes mixed fleet owners and operators, policymakers, and other stakeholders. However, it should be viewed as a starting point for CMV fleet owners and others interested in comprehending the challenges associated with implementing cybersecurity measures related to ADS deployment. This paper aims to provide general guidelines on cybersecurity for mixed fleets.

Keywords: Operational design domain, Cybersecurity, ADS-equipped CMV, Mixed fleets, Data transfer/security, Concept of operations

INTRODUCTION

This document provides an overview of cybersecurity protocols and practices for Automated Driving System (ADS) developers and owner-operators of commercial motor vehicle (CMV) fleets. The focus is on topics that are directly relevant to end users who adopt ADS technologies for ADS-equipped CMV fleet as opposed to an ADS developer.

Automated vehicle (AV) is another term used in the field of automated driving to describe a vehicle equipped with automated driving capabilities. However, the term ADS-equipped CMVs in this paper is used to describe CMVs that may have been modified with some level of automated driving capabilities after being manufactured and during the commercial operations phase.

To date, little attention has been given to the roles, responsibilities, and vulnerabilities of CMV fleets in the current ADS cybersecurity literature. This document is a first step toward filling an important knowledge gap in that literature. For ADS technologies to be safely introduced and scaled to CMV

fleets, a deeper understanding of cybersecurity topics from this perspective is critical.

Although all ADS developers aim to provide a product that is as safe as possible, the customers have a key role to play in maintaining safe data and network practices since they participate in multiple instances of information exchanges during the operations. Therefore, no matter how secure the ADS-equipped vehicles are, fleet operators and owners will need to be well informed on the topic of cybersecurity in their operations.

While the approach in this paper is intended to address mixed fleet owners and operators, policy makers, and other stakeholders, we acknowledge the challenges presented by this material to other interested parties. For this reason, this paper is structured to begin with general concepts and proceed to more specific operations and technical points.

Among the general concepts are the definitions of security and cybersecurity themselves, several of which are outlined in this paper and selected from cybersecurity publications published by U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) and Cybersecurity & Infrastructure Security Administration (CISA). In general, cybersecurity is defined as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information (CISA, 2019). Security is a much broader term that describes the state of being free of danger or threat in general, whether kinetic or cyber. However, the term security will be used interchangeably with the term cybersecurity in this paper.

The paper aims to inform fleet owners and operators and other stakeholders of strategies for mitigating cybersecurity vulnerabilities of ADS-equipped vehicles and mixed fleets. Throughout the document, the primacy of safety is acknowledged, and the need for cybersecurity measures to protect safety-critical functions of ADS-equipped CMV fleets is emphasized. The paper begins with general cybersecurity best practices, followed by cybersecurity best practices specific to ADS-equipped CMV fleets, and finally, cybersecurity best practices that relate to specialized use cases.

GENERAL CYBERSECURITY BEST PRACTICES

Cybersecurity is a vital aspect of protecting information, both when it is stored in memory, being processed, or in transit across a network. While all trucks may exchange data with other vehicles, roadway infrastructure, and logistics networks to some extent, ADS-equipped CMVs have even greater levels of connectivity, making them more vulnerable to cyber threats. With high levels of automation, parties handling operational information have greater control, but this also means that safety-critical functions on CMVs with ADS features can be manipulated based on data or through remote actuation. Therefore, it is essential to recognize that cybersecurity is not solely the responsibility of ADS developers or operators, but rather everyone must take an active role in maintaining secure data and network practices.

Vulnerabilities and Challenges in ADS Environment

In the ADS environment, i.e., in an operating environment that includes ADS-equipped vehicles, the information shared between ADSs and between ADSs and infrastructure can impact safety-critical functions on the vehicles. Protecting this information must be included in any cybersecurity strategy for ADS-equipped vehicles, along with vehicle development itself. To discover issues early, such as requirements failing or failing to meet objectives, cybersecurity should be a fundamental objective in this process and be subjected to continuous testing and confirmation (SAE International/International Organization of Standardization, 2021).

An ADS-equipped CMV is a commercial vehicle equipped with an ADS feature (see J3016 and J3164; SAE International, 2021). The ODD of an ADS feature describes "operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics[1]." An ADS feature operating a vehicle within its operational design domain (ODD) faces challenges in mitigating vulnerabilities noted above and in obtaining the information required for ADS feature functions. These functions include path planning and monitoring, trajectory and vehicle control (longitudinal and lateral control algorithm), safety-comfort trade-off analysis, driving alert human machine interface, and intent communication with the environment (Serban et al., 2022).

Cybersecurity Considerations

When designing driving automation features, it is crucial to consider access by both authorized and unauthorized users, as well as intentional and unintentional attacks on ADS operations. Safe and easily maintained cybersecurity measures, such as logging, auditing, and recovery, must be implemented to ensure that ADS can be safely integrated into CMV fleets, particularly when end-users lack technical expertise. Stakeholders must remain vigilant and aware that ADS can be misused or abused, and this awareness must be a priority when deploying and managing ADS-equipped CMV fleets. To minimize potential risks, operational safeguards and frequent system audits should be implemented.

It is critical to provide training and education about ADS safety measures, as incidents can occur when system checks are missed or best practices are not followed, particularly in future ADS-equipped CMVs deployed in mixed fleets. Implementing a robust ADS that can monitor itself, self-audit, and prompt an external audit when necessary can help mitigate the adverse consequences of human error. The goal of any ADS cybersecurity program should be to have as many built-in automatic safety checks and audits as possible, ensuring that an end-user who is not fully trained or unsure of the ADS's capabilities does not endanger others.

[1]J3216_202107, Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles.

Cybersecurity should not just be considered a "virtual" matter that involves potentially valuable information and data. There is also a critical physical component. Keeping the hardware as secure and robust as possible helps to maintain the safest possible physical operations. Although each ADS deployment is unique, the goal of any cybersecurity program should be that any significant failure avoids physical harm or damage. The ADS-equipped CMV should possess the capability of stopping the operation in a manner that minimizes potential harm to surrounding traffic and people. ADS developers and other stakeholders are already familiar with the concept of a minimal risk condition (MRC). The MRC is a vehicle state that reduces risk, a reasonably safe operating mode that an ADS-equipped CMV attempts to achieve when the CMV's ADS fails in a way that renders the vehicle unable to perform the entire dynamic driving task (DDT). Fleets should adopt the same mindset when it comes to serious cybersecurity breaches—bringing the ADS-equipped CMV to a reasonably safe state to prevent the cybersecurity issue from becoming a physical danger to others.

In addition, there are malicious software programs available on the Internet designed to damage or repurpose computers. Trucking fleets should be vigilant and aware of potential threats targeting connected devices. In this respect, ADS should be treated like other highly sensitive computer systems. General best practices for computer security and monitoring from organizations like the Automotive Information Sharing and Analysis Center(Auto-ISAC, n.d.) and the National Institute of Standards and Technology (NIST, n.d.) should be followed. Although ADS developers are known to follow procedures similar to those of other highly data-sensitive industries like aerospace, defense, electric utilities, and other critical infrastructure, trucking fleets should approach the cybersecurity of their ADS-equipped fleet with the same level of rigor and protection that they would apply to their most sensitive digital assets (e.g., financial systems, customer and pricing information, logistics and dispatch platforms, etc.).

Access

To ensure network security, access should be restricted to authorized users and controlled further through an online management portal. Allowing unfettered access to the ADS through a VPN can pose a significant threat as it may become infected from other devices on the VPN. To reduce access and segregate devices, access control lists should be implemented. By assigning user accounts to specific groups and defining access on a per-group basis, these lists provide granular control to users or devices that can communicate across the VPN to another device.

When evaluating cybersecurity risks, physical access to the ADS should also be taken into account. While the installed components should be easy to service, they should be challenging to break into to prevent unauthorized physical access. Unauthorized physical access can bypass many network software restrictions and provide access to the local network the ADS is connected to or direct access to the onboard components. Additionally, physical access to the main ADS computer or other hardware leaves the system vulnerable to tampering.

To address this, most of the ADS product should be housed in a closed, ruggedized enclosures secured with non-standard security screws to prevent unapproved access. Any physical connections not necessary after development and installation should be removed, and exposed physical ports (such as serial, USB, SATA, Ethernet) should be minimized as they pose potential risks for unauthorized access to the ADS. While it may be challenging to monitor physical access continuously, tamper-resistant physical designs, along with tamper tape or seals across physical service or access points, can help identify unauthorized access.

Training and Management

To ensure effective cybersecurity, employees must have a clear understanding of proper procedures and safe data handling practices. This necessitates comprehensive and user-friendly training, accompanied by a concise and comprehensive cybersecurity policy from fleet management. Employee cybersecurity training is essential for developing knowledge of cybersecurity and ADSs, as well as providing explicit instructions on proper procedure implementation.

Policies on Physical Facility and Individual Login Devices

To ensure physical security of a facility, it is crucial to develop comprehensive rules that cover all potential security loopholes. This includes preventing unauthorized access to the facility, as well as establishing protocols for handling individual login devices. By implementing these measures, organizations can effectively safeguard their physical infrastructure and protect sensitive data from potential cyber threats.

Monitoring of Facility, Property, Driver States, and Vehicle Information

To ensure the safety and security of ADS-equipped fleets, it is crucial to have a reliable mechanism in place to detect cyberattacks, whether they originate from physical or wireless sources. Abnormal behavior within the system can be a key indicator of such an attack, and a visually observable monitoring function should be developed to constantly monitor the system and report any suspicious activity to both the system and its human users. This monitoring function should have full access to all aspects of the fleet's operations, ensuring that any potential threats are identified and addressed in a timely manner.

Internal Cybersecurity Team Risk Assessment

The U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) released its *Cybersecurity Best Practices for the Safety of Modern Vehicles* in 2022, an update to its 2016 edition (NHTSA, 2022). This NHTSA document states that the cybersecurity risk assessment process "should include a cybersecurity risk assessment that is appropriate and reflects mitigation of risk for the full life cycle of the vehicle," and "Safety of vehicle occupants and other road users should be of primary

consideration when assessing [cybersecurity] risks" (NHTSA, 2022, p. 4).[2] Meanwhile, monitoring and limiting outbound traffic from devices, such as monitoring for outgoing connections to known "Command and Control" botnets (or unexpected traffic to anywhere), is an excellent way to recognize a compromised device.

Sensor Function Vulnerability/Reliability

The sensing and perception functions of ADS-equipped vehicles play a critical role in providing the vehicle with an understanding of its operating environment. Conducting a risk assessment for these functions is therefore essential for a comprehensive cybersecurity evaluation of the vehicle. Depending on the type of connection, sensors may be wirelessly connected to other vehicle components, such as tire pressure monitoring systems, or wired, such as parking assistance systems. Appropriate measures must be taken to ensure the security of sensor data, considering the type of connection in use.

Penetration Testing and Review

Penetration testing involves attempts to breach or penetrate the cybersecurity defenses and information assurance measures implemented on a system. After conducting a penetration test, the results are analyzed to identify any weaknesses in the system's defenses. If the test reveals vulnerabilities that were successfully exploited and resulted in harm, the testing review summary should recommend additional measures to be taken to improve the system's security.

Weakest Point Assessment, Reporting, and Monitoring

Adversaries always try to find the weakest link in any system or process to minimize their effort and maximize the impact of their attacks. While it may not be immediately apparent to system designers which of their system components are more vulnerable to attacks, there are active measures available for monitoring and reporting intrusions throughout the vehicle system. Gathering information about the occurrences and consequences of attacks against the components of the system can help identify any weaknesses in the system.

Continuous Improvement and Assessment

The vulnerability of ADS-equipped vehicles to different types of cyberattacks is constantly evolving. Therefore, it is essential to continuously improve the information assurance measures by enhancing the existing defenses and developing new ones to counter novel attacks. However, sustaining this improvement requires having well-defined metrics that can measure the effectiveness of the monitoring in terms of incremental improvement, such as reducing the number of successful attacks on the system. By using these metrics, regular

[2]This guide also refers to the ISO/SAE 21434 [RQ-05-01] that requires that "the organization shall define a cybersecurity policy that includes: b) the executive management's commitment to manage the corresponding risks." Also, "a risk assessment process is described in clause 15 of ISO/SAE 21434. The work product [WP-0-02] 'Threat analysis and risk assessment' results from requirements [RQ-09-03] and [RQ-09-04] which pull from clause 15 sections" (NHTSA, 2022, p. 4).

assessments and reviews can be conducted to ensure continuous improvement in the information assurance measures.

Failure and Recovery

In the event of an ADS failure, it is essential to have robust monitoring systems in place that can assess the severity of the failure and determine whether any action is necessary to improve resilience to failure. The monitoring system should be able to detect any interruption of regular operations, and the ADS should be able to restart itself safely. If the ADS cannot continue safely, it needs to enter an MRC failure state, which includes cybersecurity-related failures.

Recovery should be as quick as possible, as a stopped vehicle in an MRC can pose a hazard to other vehicles and people. However, it is important to ensure that restarting services while the vehicle is in operation does not cause additional issues. Each service that runs on ADS computing devices should be as independent and modular as possible. Although the ADS will require the coordination of many subsystems and services, a smooth transition between failure and recovery can make all the difference in maintaining long-term operations without the need for frequent, in-person maintenance.

Data Protection

Data stored in databases or other storage systems needs to be protected against various threats such as unauthorized access, modification, and processing errors. Modifications can lead to data becoming useless or causing errors in analytics and queries. It is important to log, tag with validation information, and audit pre and post-processing to identify any modification or processing errors.

Data being processed by components of an ADS is also vulnerable to threats, including unexpected software components, processing errors, and unauthorized access or modification. To address these threats, it is important to implement logging, tagging, and auditing practices that help identify any anomalies or errors during processing.

During transit, data is formatted using the transport protocol of the network in use, and vulnerabilities include unauthorized access, modification of the protocol formatting, and data modification. To address these threats, network monitoring for anomalies, data sharing rules, and various audit practices can be implemented. It is important to protect data both in transit and in storage to ensure the reliability and accuracy of data analytics and queries.

Auditing

To ensure that the ADS is functioning as intended and to understand the cause of unexpected events, it is essential to review and verify the events recorded in the system's logs. A thorough review of the logs can provide insight into the devices connected to the system, communication methods utilized, access and authentication protocols employed, configuration changes, and the overall life cycle of the ADS. By analyzing this information, developers can identify weaknesses in the system's cybersecurity policies and take corrective action.

Regular audits of the ADS can also provide valuable information about the system's health and identify potential issues that standard monitoring might overlook. Creating audit tools that quickly analyze and clearly display the logs generated by the ADS can streamline the auditing process and make it easier to assess incidents.

SPECIFIC CYBERSECURITY BEST PRACTICES AND SPECIALIZED ADS USE CASES

Cyberattack Through Wireless Connections

Numerous wireless connections through cellular networks are required to manage mixed fleets, which involve exchanging information from various sources. These connections include communications with the fleet control center, cloud uplink, other ADS vehicles, and the connection used for traffic coordination. All of these exchanges involve the transfer of transit-related information, and ensuring its security may necessitate permission and access measures to prevent unauthorized individuals or systems from accessing the network. The information exchanged encompasses job descriptions, dispatching information, instructions for tasks, general communication, navigation, and GPS data.

Cyberattack Through Physical Connections

An analysis of the cybersecurity of ADS vehicles must take into account the vulnerabilities and cyberattacks that may result from unauthorized physical connections. These can occur during maintenance and repair, rest and fuel stops, cargo transfers, accidents, and other scenarios. If such connections are established by the personnel of the ADS vehicle operator, adequate provisions must be implemented to safeguard them. On the other hand, if third parties establish these connections, additional security measures should be put in place, as outlined below.

Maintenance-and-Repair

When a third party performs maintenance and repairs on an ADS vehicle, they may establish physical connections to the vehicle and its network to facilitate the repair process. However, such connections can pose a risk of cyberattacks. To address this, several measures can be taken, such as disconnecting the component(s) being repaired from the vehicle network during service and reconnecting it afterwards.

Routine-Maintenance

Routine maintenance by a third party is maintenance that is planned, and the agreement between the fleet operator and the party performing routine maintenance should include provisions for security.

Collision-Repair

In a collision, there may be damage to the vehicle that includes components responsible for protection against cyberattack. In this situation, provision

should be made for the fleet operator's cybersecurity professional to be involved to ensure that the previously established protections are in good working order when repairs to the rest of the vehicle are undertaken.

Customized-Vehicle-Parts-From-Third-Party-Providers

Customized vehicle parts have had their design modified to meet the needs of the fleet owner or operator. Security measures that applied to the original parts may no longer be effective protections for the custom design; in extreme cases, the provider may have knowingly introduced other threats. While the latter may be rare, this scenario is the topic of a recent Presidential Executive Order on U.S. supply chains (The White House, 2021).

Rest-Stops-and-Fuel-Stops

During rest and fuel stops, physical connections with an ADS may be active. In this case, the cybersecurity analysis and resulting measures should address vulnerabilities. ADS information on the vehicle, either in storage or being processed, should be protected, as well as information that may be accessed through the ADS's connections to its control center or other ADSs in the fleet.

Cargo-Transfer-at-Different-Locations

During the transfer of cargo from or to an ADS, physical connections between the ADS and other entities may be active. In this case as well, the cybersecurity analysis and resulting measures should address vulnerabilities. As with rest and fuel stops, ADS information on the vehicle, either in storage or being processed, should be protected, as well as information that may be accessed through the ADS's connections to its control center or other ADSs in the fleet.

Ports

During an ADS stay in a port, physical connections between the ADS and other entities may be active. As in the previous two examples, the cybersecurity analysis and resulting measures should address vulnerabilities. ADS-related information on the vehicle, either in storage or being processed, should be protected, as well as information that may be accessed through the ADS's connections to its control center or other ADSs in the fleet.

Warehouse

At the terminal or in the warehouse, physical connections may be in use to monitor and control cargo status using "Internet of Things" devices on vehicle and off. As these connections will often be owned and provided by third parties, it is important that fleet cybersecurity efforts include provisions for protecting the ADS-equipped CMVs and fleet infrastructure.

Crashes-and-Data-Retrieval

Resilience of cybersecurity measures to crashes is an important component of CMV fleet security (NHTSA, 2018), including retrieving/recovering vehicle data after crashes and ensuring that cybersecurity measures recover and are returned to their nominal state.

Roadside-Inspections

Physical connections to the ADS during roadside inspections pose additional security challenges. Cybersecurity measures to meet these challenges include using connections between automated vehicles and connections from automated vehicles in the fleet to the control center to help monitor and check security status.

Cooperative Technology

Cooperative technology refers to technologies that enable sharing of information such as, sensing and perception and other operational information among ADSs, to improve accuracy and precision, thereby reducing uncertainty (Kim, S., Shrestha, R., 2020). In other words, cooperative technology allows vehicles to exchange data with each other and the surrounding infrastructure in real-time, enabling them to operate more intelligently and adaptively in complex and dynamic environments. This technology can improve the accuracy of sensor data, reduce the risk of collisions, and optimize traffic flow by enabling vehicles to anticipate and respond to traffic conditions before they occur.

Cooperative technology is also enabled by communications between ADSs and infrastructure such as control centers and roadway infrastructure. As noted above, cybersecurity measures will need to consider and address the cyber vulnerabilities that result from cooperative technology (Cui et al., 2022).

Teleoperation

Teleoperation is an important feature of ADS, which encompasses various forms such as remote monitoring, collaborative tactical commands, and fallback minimal risk commands. However, all three forms of teleoperation require extensive information sharing, making them susceptible to significant cybersecurity challenges.

In remote driving, for instance, vehicle perception is shared with the remote driver, who then determines the vehicle's responses, resulting in a two-way communication channel. Collaborative driving, on the other hand, involves sharing the driving task or performance of the DDT among multiple agents, which may require multiple two-way communication channels. Finally, fallback driving is utilized when the automated vehicle can no longer perform the DDT, or when the ADS feature has exited its ODD. Similar to remote and collaborative driving, fallback driving necessitates a minimum two-way communication between the vehicle and the fallback driver.

Enhanced CMV Inspection

The enhanced CMV inspection program is a newly established inspection standard and procedure that governs the inspection of commercial motor vehicles equipped with ADS, approved by the board of directors of the Commercial Vehicle Safety Alliance (CVSA) in 2022. While the current inspection procedure mandates the driver to perform pre-trip and post-trip inspections

of the CMV, the enhanced CMV inspection requires CVSA-trained motor carrier personnel to conduct an enhanced CMV inspection procedure on selected ADS-equipped CMVs from the fleets at the point of origin before dispatch (CVSA, 2022). As per the 2022 CVSA regulations, the ADS-equipped CMV must communicate to law enforcement while in motion that it has passed the origin inspection, its ADS is functioning properly, and it is operating within its ODD.

However, the communication and verification processes between the ADS-equipped CMVs, bypass fixed inspection sites, law enforcement, and remote operators all present potential cybersecurity issues that the fleets should consider.

Platooning

Platooning, or flocking, is an ADS feature involving two or more vehicles that coordinates their performance of the driving task. The feature is expected to increase fuel efficiency and equipment utilization via an automated highway system.

According to Martínez-Díaz et al., "a platoon of connected automated vehicles (CAVs) is defined as a group of CAVs that exchange information, so that they can drive in a coordinated way, allowing very small spacings, and, still, traveling safely at relatively high speeds" (Martínez-Díaz et al., 2021). A connected automated vehicle is any ADS-equipped vehicle with communications to other vehicles or infrastructure.

The safe operation of platooning features depends critically on channels of communication and should be addressed by a cybersecurity analysis of the feature in the broader system that includes the group of ADS-equipped CMVs.

Testing and Validation

Testing and validation of ADS features and their use cases is essential for ADS feature developers, regulators, and researchers. Testing and validation may involve virtual, test track, and on-road testing. In each case, test cases are included to assess each of the cybersecurity or information assurance measures.

CONCLUSION

The future of the ADS-equipped CMV environment remains uncertain, and developing a system that comprises ADSs, non-ADSs, and their communications with infrastructure and operators requires careful consideration of the associated threats. In order to address these challenges, cybersecurity measures must be meticulously evaluated, including an understanding of the information exchanged between these entities, the technologies used to exchange and store this information, and the role this information plays in ensuring safe operation.

We believe that this overview document will be beneficial to CMV fleet owners and operators, policymakers, and other stakeholders. ADS development is constantly evolving, particularly with regard to cybersecurity, and

this paper should be viewed as a starting point for CMV fleets and other interested parties looking to implement effective cybersecurity measures in ADS deployment. Our hope is that this document will assist readers, particularly CMV fleets, in identifying relevant concerns and promising strategies for mitigation.

ACKNOWLEDGEMENT

We would like to thank our project sponsor FMCSA for their continuous support on our research and vision on the topic of transportation safety. In addition, we would like to thank our industry partner and ADS developer, Pronto. AI, for their discussion and input on this paper. We would also like to thank our colleagues at VTTI for their valuable contributions and guidance, including Rich Hanowski and Andrew Krum.

REFERENCES

Automotive Information Sharing and Analysis Center (n.d.) *Best practices: Automotive ISAC*. Available at: https://automotiveisac.com/best-practices/.

Cui, G. et al. (2022) 'Cooperative perception technology of autonomous driving in the internet of vehicles environment: A review', *Sensors*, 22(15), p. 5535. Available at: https://doi.org/10.3390/s22155535.

CVSA announces new enhanced CMV inspection program for Autonomous Truck Motor Carriers. CVSA. (2022, October 7). Retrieved January 31, 2023, from https://www.cvsa.org/news/new-enhanced-cmv-inspection-program/.

Cybersecurity and Infrastructure Security Agency (2019) *What is cybersecurity? Security Tip (ST04-001)*. Available at: https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information.

Kim, S., Shrestha, R. (2020). Introduction to Automotive Cybersecurity . In: Automotive Cyber Security. Springer, Singapore. https://doi.org/10.1007/978-981-15-8053-6_1.

Martínez-Díaz, M. et al. (2021) 'Platooning of connected automated vehicles on freeways: A bird's eye view', *Transportation Research Procedia*, 58, pp. 479–486. Available at: https://doi.org/10.1016/j.trpro.2021.11.064.

National Highway Traffic Safety Administration (2018) *Cybersecurity research considerations for heavy vehicles*. Available at: https://deepblue.lib.umich.edu/bitstream/handle/2027.42/151379/UMTRI-2018-10.pdf.

National Highway Traffic Safety Administration (2022) *Cybersecurity best practices for the safety of modern vehicles. cybersecurity best practices for the safety of modern vehicles, updated 2022*. Available at: https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf.

National Institute of Standards and Technology (n.d.) *Cybersecurity framework*. Available at: https://www.nist.gov/cyberframework.

SAE International (2021) Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Available at: https://saemobilus.sae.org/content/J3016_202104.

SAE International/International Organization of Standardization. (August 2021) Road vehicles – Cybersecurity engineering. Available at: https://saemobilus.sae.org/content/iso/sae21434/.

Serban, A. C., Poll, E., & Visser, J. (2018). A standard driven software architecture for Fully Autonomous Vehicles. 2018 IEEE International Conference on Software Architecture Companion (ICSA-C). https://doi.org/10.1109/icsa-c.2018.00040.

Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles. SAE MOBILUS. Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles (n.d.). https://saemobilus.sae.org/content/J3216_202107?_gl=1*11bcrdr*_ga*MTc4OTA3Mjg5NC4xNjg3Njk4OTQy*_ga_HMVR9L7XWD*MTY4NzY5ODk0MS4xLjEuMTY4NzcwMDM0NS4wLjAuMA.

The White House. (February 24, 2021) *Executive Order on America's supply chain*. Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.