Trucking Fleet Concept of Operations for Automated Driving System-equipped Commercial Motor Vehicles

Chapter 5.8 Data Transfer and Cybersecurity Best Practices

Authors: Jin, X., Argueta, O., Griffor, E., Terranova, P., Stojanovski, O., Krum, A.

Partners: Pronto.ai

VIRGINIA TECH
TRANSPORTATION
INSTITUTE

PRONTO

July 2024

Abstract

Automated Driving Systems (ADS) are set to revolutionize the transportation system. In this project, the research team led by the Virginia Tech Transportation Institute developed and documented a concept of operations (CONOPS) that informs the trucking industry, government agencies, and non-government associations on the benefits of ADS and the best practices for implementing this technology into fleet operations.

The sections of Chapter 5 provide guidance on a range of topics for fleets to consider and apply when preparing to deploy ADS-equipped CMVs in their fleet. The topics cover fleet-derived specifications, ADS installation and maintenance, ADS inspection procedures, driver-monitor alertness management, insuring ADS-equipped trucks, identification of ADS safety metrics/variables, ADS road assessment, and data security/transfer protocol and cybersecurity best practices.

This section provides an overview of cybersecurity best practices and data transfer protocols for the developer's ADS. While it touches on some cybersecurity measures used internally by the developer for ADS development and service operations, the primary focus is on topics directly relevant to end users adopting ADS technologies. Specifically, this document addresses cybersecurity from the perspective of a commercial motor vehicle (CMV) fleet equipped with ADS, rather than from an ADS developer's standpoint.

The scope of this section includes general guidelines for understanding cybersecurity, the relationship between mixed fleets (both conventional and automated trucks) and cybersecurity, and how fleets can tailor these guidelines to their specific systems. The intended audience is those operating mixed fleets for commercial purposes.

The following chapter has been extracted from the final report. For access to the full report, see this link: https://www.vtti.vt.edu/PDFs/conops/VTTI_ADS-Trucking_CONOPS_Final-Report.pdf

5. GUIDELINES

5.8 DATA TRANSFER AND CYBERSECURITY BEST PRACTICES

This section provides an overview of cybersecurity protocols for the developer's (Pronto) ADS. Although this section includes some aspects of the cybersecurity measures that the developer uses in its internal ADS development processes and service operations, the focus is on topics that are directly relevant to *end users* who adopt ADS technologies. More specifically, the focus is on cybersecurity from the point of view of an ADS-equipped CMV fleet as opposed to an ADS developer.

The section includes general guidelines for understanding what cybersecurity is, how mixed fleets (both conventional and automated trucks) and cybersecurity relate to each other, and how fleets should tailor these guidelines to meet their specific systems; the intended audience includes people operating mixed fleets for commercial purposes. The information in this section addresses cybersecurity topics from a unique angle that has not previously been studied in detail and is continuously evolving. We believe that this will be of practical use to CMV fleets, policymakers, and other stakeholders. Like many new technologies, ADS development continues to evolve at a rapid pace, especially regarding cybersecurity. As such, this section does not focus on technical details for implementation. Rather, it is best viewed as a starting point for CMV fleets and other audiences with a general interest in the practical, real-world implementation of cybersecurity measures in ADS deployment.

The section includes discussions around general best practices for managing mixed fleets based on different aspects of cybersecurity, and specific cybersecurity best practices for mixed fleets, including cybersecurity measures for use cases involving wireless and wired network connections. Also, we discuss general cybersecurity best practices in terms of background information, cybersecurity considerations, and data transfer and security.(1) It should be noted that the terms "cybersecurity" and "security" are both used here. 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 both information(2) and the systems themselves. "Security" is a much broader term that describes the state of being free of danger or threat in general. However, the term "security" will be used interchangeably with the term "cybersecurity" in this section.

5.8.1 Cybersecurity Background on Managing Mixed Fleets

In ADS cybersecurity literature, the focus has been on the internal practices of ADS developers and vehicle manufacturers. This document is a first step toward filling an important knowledge gap in that literature. To date, relatively little attention has been given to the roles, responsibilities, and vulnerabilities of CMV fleets. For ADS technologies to be safely introduced and scaled to CMV fleets, a deeper understanding of cybersecurity topics from the perspective of CMV fleets is critical. Although all ADS developers aim to provide a product that is as safe as possible for CMV fleets, customers have a key role to play in maintaining safe data and network practices.

As technology continues to advance, the transportation industry is witnessing a shift towards mixed fleets, which comprise a combination of conventional trucks and automated trucks, such as those equipped with ADS. This integration of automated trucks into traditional fleets brings numerous benefits, including improved efficiency, reduced fuel consumption, and enhanced safety. However, it also introduces new challenges, particularly in the realm of cybersecurity.

In general, cybersecurity is about protecting information, including when it is stored in memory media, being processed, or in transit across a network. Cybersecurity plays a vital role in managing mixed fleets to ensure the secure and reliable operation of both conventional and ADS-equipped trucks. Conventional and ADS-equipped CMVs both exchange data with other similar vehicles, with the roadway infrastructure, and with a logistics network. However, ADS-equipped CMVs are equipped with high levels of automation that provide more control to the parties handling operational information. Therefore, safety-critical functions on CMVs with ADS features can be manipulated based on the data or through remote actuation.

The integration of automated trucks, which heavily rely on interconnected systems, introduces new vulnerabilities that may not be present in conventional trucks. These vulnerabilities can be exploited by malicious actors to compromise the safety, privacy, and integrity of the fleet's operations. Therefore, it is imperative to develop robust cybersecurity strategies specifically tailored to the unique characteristics and requirements of mixed fleets. We list these new vulnerabilities associated with ADS-equipped CMVs in section 5.8.2.1.

One key aspect of cybersecurity in managing mixed fleets is the integration and compatibility of different vehicle types and technologies. Conventional trucks and automated trucks often have distinct communication protocols, software systems, and security measures. Ensuring seamless interoperability and secure data exchange between these diverse vehicles is crucial for efficient fleet management and mitigating potential vulnerabilities.

Additionally, the cybersecurity focus in mixed fleets extends beyond the vehicles themselves. It encompasses the network infrastructure that facilitates communication between vehicles, fleet management systems, and external entities. The security of these networks is paramount to prevent unauthorized access, data breaches, or disruptions that could impact the entire fleet's operations and compromise the safety of drivers and cargo.

Moreover, the protection of sensitive data generated and exchanged within mixed fleets is of utmost importance. This data includes driver information, vehicle telemetry, maintenance logs, and cargo details. Cybersecurity measures are necessary to safeguard this information from unauthorized access, tampering, or theft, ensuring compliance with data privacy regulations and maintaining the trust of customers and stakeholders.

5.8.1.1 Vulnerabilities in ADS Environments

Software and Communication Vulnerabilities: In the ADS environment (i.e., in an operating environment with ADS vehicles), the complex software systems that power ADS can have bugs, coding errors, or security weaknesses that attackers could exploit. These vulnerabilities can allow unauthorized access, manipulation of data, or control of the vehicle. In 2015, two security researchers exposed the security vulnerabilities in automobiles by hacking into cars remotely, overtaking the cars' various controls from the radio volume to the brakes,(3) and leading to 1.4

million vehicles being recalled from the car manufacturer. In 2020, a Tennessee-based trucking and logistic company was targeted by a new and relatively unknown group of ransomware operators called “Hades” in December, which caused damage to the fleet’s reputation and disrupted operation.(4)

Meanwhile, the information shared among ADS and between the ADS and infrastructure can trigger safety-critical functions on the vehicles. Recent studies have revealed concerns of major risks associated with connected vehicles and AVs as the technology advances; these risks include not only the risk of traditional cyberattacks on the information and running of the vehicle, but also a new breed of attacks around such things as ransomware, Internet of Things (IoT) attacks, and vehicle theft.(5) ADS technology relies heavily on software, communication systems, and other advanced technologies to operate. These systems can be vulnerable to cyberattacks, which can compromise the vehicle’s control systems and compromise the safety and security of the driver, passengers, and cargo. Protecting this information must be included in any cybersecurity strategy for ADS-equipped vehicles, along with vehicle development itself. The vehicle development process is focused on continuous verification and validation. To discover issues early, such as requirements failing or failing to meet objectives, cybersecurity should be a fundamental objective in this process and should be subjected to continuous testing and confirmation.(6)

Sensor Spoofing or Tampering: Sensor spoofing refers to the act of sending falsified or manipulated data to the sensors of an AV. These sensors, including cameras, lidar, radar, and other perception systems, provide crucial information about the vehicle’s surroundings. If an attacker can feed incorrect data to these sensors, the automated system may misinterpret its environment, potentially causing the vehicle to make incorrect decisions. For example, an attacker could send false signals to a vehicle’s lidar sensors, making the system perceive obstacles that do not exist or fail to detect real obstacles like pedestrians or other vehicles. This could lead the vehicle to take unnecessary evasive actions or fail to respond appropriately to an actual threat. Sensor tampering involves physically modifying or interfering with the sensors on a vehicle. This can be done to either disrupt the vehicle’s perception of the environment or to manipulate the automated system’s behavior. Attackers might aim to disable certain sensors or alter their settings to create confusion for the autonomous system. For instance, an attacker could cover or obstruct the cameras or lidar sensors, making it difficult for the vehicle to see its surroundings accurately. Alternatively, attackers might modify the radar sensors’ settings to either exaggerate or diminish the perceived distances to objects, leading to unsafe driving decisions.

Both sensor spoofing and tampering pose serious risks to AVs and the people around them. These attacks can undermine the trust and reliability of automated systems, potentially causing accidents and fatalities. Manufacturers and developers of AV technology must implement robust security measures to detect and prevent such attacks, including encryption, authentication protocols, and redundant sensor systems. As with software vulnerabilities and communication weaknesses, protecting against sensor spoofing and tampering should be an integral part of the overall cybersecurity strategy for AVs. Continuous testing, validation, and monitoring are essential to ensure the integrity and safety of these advanced technologies as they become more prevalent on our roads.

Physical Access Vulnerabilities: Physical access vulnerabilities arise when attackers can physically interact with the vehicle's hardware, software, or communication systems. This can occur through direct access to the vehicle, its components, or the infrastructure that supports it. Once an attacker gains physical access, they might exploit weaknesses in the vehicle's design or security measures to compromise its functionality or data. For instance, an attacker could gain access to the internal systems of an AV by exploiting a weak point in its physical security, such as a compromised diagnostic port or an insecure software update mechanism. Once inside, the attacker could manipulate the vehicle's software, alter its configurations, or even insert malicious hardware devices that grant control over the vehicle. Physical access vulnerabilities can have far-reaching consequences. Attackers with physical access can potentially take any of the following actions:

- Take Control of the Vehicle: By gaining access to critical systems, attackers might take control of the vehicle's functions, such as acceleration, braking, and steering, which could lead to accidents or intentional harm.

- Steal Sensitive Data: Access to the vehicle's internal systems can expose sensitive data, including personal information about the driver and passengers, travel history, and more.

- Install Malware: Attackers might install malicious software that can compromise the vehicle's security, monitor its activities, or even spread to other connected vehicles.

- Tamper with Safety Systems: Attackers could manipulate safety-critical systems, such as airbags or collision avoidance systems, leading to compromised occupant safety.

To address physical access vulnerabilities, users must take several precautions:

- Physical Security: Utilize robust physical security measures, including secure access points, tamper-resistant hardware, and intrusion detection systems.

- Secure Updates: Implement secure mechanisms for software updates, ensuring that only authorized and authenticated updates are accepted.

- Encryption: Encrypt sensitive data and communications to protect against data theft during physical access attacks.

- Multi-Layered Security: Apply a multi-layered security approach that combines physical, digital, and network security to create a comprehensive defense strategy.

- Continuous Monitoring: Employ real-time monitoring systems to detect and respond to any unauthorized physical access attempts.

As the automotive industry advances toward more automated and connected vehicles, acknowledging and addressing physical access vulnerabilities is crucial to maintaining the safety and security of both the vehicles and their occupants. Like other cybersecurity aspects, the prevention and mitigation of physical access vulnerabilities should be a fundamental component of the overall security strategy for these vehicles. This topic is revisited under the specific cybersecurity best practices section to further elaborate in the context of fleet operations at different locations, in different circumstances, and during different operations.

Supply Chain Vulnerabilities: In the field of ADS technology, the intricate network of supply chains that contribute to the development and manufacturing of these systems can introduce their own set of vulnerabilities. These vulnerabilities stem from the various components, software modules, and technologies sourced from different suppliers and integrated into the final product. Like software and communication vulnerabilities, supply chain vulnerabilities also pose significant risks to the security and functionality of ADS-equipped vehicles. Within this complex ecosystem, compromised components or software modules introduced at any point in the supply chain can have far-reaching consequences. Malicious actors could potentially insert backdoors, malware, or other forms of malicious code into the components or software, allowing unauthorized access, manipulation of data, or even complete takeover of the vehicle. The interconnected nature of supply chains amplifies these risks, as a vulnerability introduced by a single supplier can propagate across the entire network.

A prominent example of supply chain vulnerabilities came to light in various industries when the SolarWinds incident occurred.(7) This cybersecurity breach exploited vulnerabilities in the supply chain of a widely used network management software, ultimately affecting numerous organizations and government agencies. In the context of ADS, similar attacks on the supply chain could result in catastrophic outcomes, compromising not only the safety of the vehicle's occupants but also the broader transportation ecosystem.

To mitigate these risks, a robust cybersecurity strategy for ADS technology must encompass supply chain security. This involves rigorous vetting of suppliers, ensuring their adherence to security best practices, and conducting thorough assessments of the components and software they provide. Additionally, establishing mechanisms for ongoing monitoring and verification of the components throughout their life cycle is crucial to detect and address vulnerabilities as they arise.

Incorporating cybersecurity into the vehicle development process should extend to encompass the entire supply chain. Just as software vulnerabilities are subject to continuous testing and validation, the components and technologies sourced from suppliers should undergo similar scrutiny. By proactively addressing supply chain vulnerabilities and promoting a culture of security across all stakeholders, the ADS industry can work towards building safer and more resilient ADS.

Lack of Cybersecurity Awareness and Training: When advanced technology meets transportation or safety, a significant challenge always arises from insufficient awareness and training, and this applies to cybersecurity on ADS-equipped CMVs as well. The sophisticated nature of ADS technology demands a heightened level of vigilance and understanding about the potential risks associated with cyber threats; a gap in cybersecurity awareness and training can leave both developers and end users vulnerable to manipulation.

Developers and engineers working on ADS technology may not always have comprehensive knowledge of cybersecurity principles. This can lead to oversights in design and implementation, inadvertently leaving vulnerabilities in the system. Inadequate training can result in coding practices that inadvertently expose entry points for attackers, such as weak authentication mechanisms or improper data handling. This lack of awareness might also lead to underestimating the importance of security features, potentially prioritizing functionality over safeguarding against potential breaches.

Beyond the development stage, users and operators of ADS-equipped vehicles might lack the necessary cybersecurity awareness to make informed decisions. This can range from not recognizing phishing attempts aimed at gaining unauthorized access to the vehicle's systems to failing to install critical software updates that address security vulnerabilities. In some cases, users might unknowingly engage in actions that compromise the security of their vehicles, such as connecting to unsecured networks or using unauthorized third-party software.

To address these challenges, a comprehensive approach to cybersecurity awareness and training is imperative. Developers and engineers must be equipped with a strong foundation in cybersecurity principles and practices. This includes understanding secure coding practices, threat modeling, and risk assessment. Continuous training programs can help ensure that these professionals stay up-to-date with the evolving threat landscape and best practices. Similarly, users and operators of ADS-equipped vehicles need accessible and clear guidance on how to interact with the technology securely. This can involve educating users about the importance of strong and unique passwords, the risks of sharing personal data, and the significance of promptly applying software updates. Moreover, fostering a culture of cybersecurity awareness among the general public can contribute to a safer and more resilient ADS ecosystem.

5.8.1.2 Challenges of ADS-equipped CMV

An ADS-equipped CMV is a commercial vehicle equipped with an ADS feature (see SAE J3016 and J3164).(8) An ADS feature operating a vehicle within its ODD faces challenges in mitigating vulnerabilities, as noted in section 5.8.2.1, and in obtaining the information required for ADS feature functions. These functions include trip and path planning, path management, assessing path plans in the current operating environment, assessing current vehicle and environmental status, and execution of a path plan.

Beyond these challenges are potential functional and safety benefits to a system with the ability to *learn from the vehicle's past decisions* (i.e., recognize similar operating conditions and assess which decisions had a better outcome). However, this capability would require the vehicle to possess and evolve metrics for both safety and function.

Technologies, software, and networking that address each of these ADS-equipped CMV challenges will bring additional dimensions to cybersecurity measures.

As the industry is learning, "as modern vehicles are capable to connect to an external infrastructure and vehicle-to-everything (V2X) communication technologies mature, the necessity to secure communications becomes apparent. There is a very real risk that today's vehicles are subjected to cyberattacks that target vehicular communications."(9) The sensing, communication, and control elements of vehicular communications are important to understand and critical in terms of identifying cyberattacks and presenting the appropriate countermeasures.

5.8.1.3 Challenges of Mixed Fleets

Mixed fleets, which consist of a combination of conventional vehicles and vehicles with advanced technologies (such as autonomous or automated features), can present several challenges due to the coexistence of different vehicle types and technological capabilities. Some of the key challenges of mixed fleets include the following:

- Integration Complexity: Integrating diverse vehicle types with varying technological capabilities into a single fleet can be complex. Ensuring seamless communication, interoperability, and compatibility between different vehicle systems and technologies requires careful planning and technical expertise.

- Operational Variability: Conventional vehicles and advanced technology-equipped vehicles might have different operational requirements, maintenance schedules, and fuel consumption patterns. Fleet managers need to balance these differences to optimize overall fleet efficiency and performance.

- Training and Skill Diversification: Drivers and maintenance personnel need to acquire different skill sets to operate and maintain various types of vehicles. Training programs must be tailored to address the specific needs of both conventional and advanced technology-equipped vehicles, ensuring that all personnel are adequately skilled.

- Maintenance and Repairs: Maintaining and repairing mixed fleets can be challenging due to the differences in vehicle technologies. Advanced technology-equipped vehicles may require specialized diagnostics and repair procedures that conventional vehicles do not need. This could lead to increased maintenance costs and potential delays.

- Data Management: Mixed fleets generate diverse types of data, including vehicle performance data, sensor information, and advanced technology diagnostics. Managing and analyzing this data to derive meaningful insights requires robust data management systems and analytics capabilities.

- Technology Upgrades and Obsolescence: Advanced technologies in mixed fleets can become outdated quickly due to the rapid pace of innovation. Fleet managers need to consider the life cycle of these technologies and plan for upgrades or replacements to remain competitive and compliant with industry standards.

- Regulatory and Compliance Challenges: Different vehicle types may be subject to varying regulatory requirements and standards. Fleet operators must ensure that all vehicles, whether conventional or equipped with advanced technology, meet the necessary compliance criteria.

- Cost Considerations: Integrating advanced technology-equipped vehicles into a mixed fleet can be expensive, from initial procurement costs to ongoing maintenance and training expenses. Fleet managers must carefully assess the return on investment and consider the long-term financial implications.

- Driver Adoption: Drivers accustomed to conventional vehicles might need time to adapt to new technologies. Ensuring a smooth transition and addressing any resistance to change is important for maximizing driver acceptance and efficiency.

- Risk Management: Introducing advanced technology-equipped vehicles brings new cybersecurity and safety risks. Fleet operators must implement robust cybersecurity measures to protect these vehicles from cyber threats, ensuring the safety of drivers, cargo, and other road users.

- Supply Chain and Spare Parts: Managing a mixed fleet requires efficient supply chain management for spare parts and components. Availability of spare parts for advanced technology-equipped vehicles can be challenging, affecting downtime and maintenance schedules.

Navigating these challenges requires strategic planning, effective communication, ongoing training, and a thorough understanding of the specific operational dynamics of the mixed fleet. By addressing these challenges proactively, fleet operators can harness the benefits of mixed fleets while mitigating potential drawbacks.

5.8.2 Cybersecurity Considerations

Designing cybersecurity features requires consideration of access from authorized and unauthorized users and intentional and unintentional attacks on ADS operations. Implementing safe and easily maintained security measures—such as logging, auditing, and recovery—ensures that the ADS can be safely integrated into the CMV fleets, especially when end users lack technical expertise. Stakeholders for CMV fleets must always remain aware that any ADS can be misused or abused. This awareness must be at the forefront when considering how to deploy and manage an ADS-equipped CMV fleet. Potential damage is minimized by implementing a variety of operational safeguards and frequent system audits.

Training on and education about ADS safety measures is critical. System checks are sometimes missed in conventional-only fleets today, as well as best practices not followed, causing incidents to happen. This may become an issue in future ADS-equipped CMVs when deployed in large numbers in mixed fleets. Designing and implementing a robust ADS that can monitor itself, self-audit, and prompt an external audit when needed mitigates the adverse results of human error. An end user who is not completely trained, or who is unsure of the ADS's capabilities, should not endanger others by continuing to interact with the ADS. As such, one key goal for any ADS cybersecurity program should be to have as many built-in automatic safety checks and audits as possible. A CMV fleet that adopts ADS technology needs to understand how these safety checks and reports work. CMV fleets must also develop operational procedures, safeguards, and Emergency Action Plans (EAPs) to respond appropriately to any issues, including contacting the ADS developer when needed through their regular contact and support channels, or escalating when necessary.

Maintaining appropriate user access is another key goal of cybersecurity. Physical or virtual access to the ADS by an internal or external party without approval from the developer or another authorized party is considered "unapproved access." This type of access can result in a loss of control over the ADS. Unapproved monitoring, viewing, editing, or other communications to or from the ADS are all examples of "misuse," which could result in repurposing part or all of the ADS. Inappropriately using the system can cause the ADS to operate outside of its normal safety parameters, which can disrupt workflows and, in extreme cases, harm workers or other road users. Proper access and misuse procedures must therefore be one of the highest priorities for any CMV fleet that adopts ADS technologies.

Cybersecurity should not be considered only 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 truck should be capable 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 MRC. The MRC is a low-risk, reasonably safe operating mode that an ADS-equipped truck attempts to achieve when the truck's ADS fails in a way that renders the vehicle unable to perform the entire DDT. Fleets should adopt the same mindset when it comes to serious cybersecurity breaches—bringing the ADS-equipped truck to a reasonably safe state to prevent the cybersecurity issue from becoming a physical danger to others.

In addition, there are malicious programs 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(10) and the National Institute of Standards and Technology(11) should be followed. Although it is recognized that ADS developers 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).

5.8.2.1 Exposure

Exposure describes where and how the ADS communicates beyond internal communication with its components. As the ADS operates in a constantly changing environment, it relies on a suite of sensors to monitor its surroundings to inform its decisions. The ADS needs to be able to do this accurately and without interference from external actors. Knowing where and with whom the ADS communicates is important for identifying potential risks. Monitoring and using software-based checks to verify the authenticity of communications is an important step in preventing potential attacks and/or data leaks.

The cellular modem, wireless network, or other means of connecting the ADS to the broader internet is one of the greatest exposure risks. In this respect, it is important for trucking fleets to remain vigilant about overall internet cybersecurity risks. Leaving any internet-connected device unsecure and unattended can be a significant threat. Bad actors, hackers, and security researchers dig through the relatively small number of internet protocol addresses probing for connectivity and looking for interesting or exploitable ports. Pronto's system is designed to talk to other vehicles that are equipped with the Pronto ADS, other pre-approved devices, and Pronto engineers' laptops (only through a virtual private network, or VPN). However, the ADS is still open to the rest of the internet during debugging stages, allowing developers access to online resources for development.

Access to the internet is largely unnecessary, as updates and control commands should continue to go through the ADS developer's VPN. Nevertheless, it is critical for the trucking fleet to be vigilant about who has access to manage the VPN and who can communicate across it. This is a critical step in keeping the ADS secure, as unapproved devices could leak data from the VPN and thus be an ingress point for attackers. VPNs are suitable for securing communication channels in mixed fleets, as they ensure data transmitted between vehicles and the central system is encrypted and secure. Zero Trust architecture—also often referred to as Zero Trust Security or the Zero Trust model—on the other hand, provides a comprehensive security approach that encompasses access control, continuous monitoring, and strict user/device verification.(12) This approach can be applied in mixed fleet cybersecurity systems, making it well suited for securing resources and access within mixed fleets while adhering to the principle of least privilege (PoLP). Under Zero Trust architecture, vehicles and devices are never trusted by default; they must authenticate and prove their security posture before accessing fleet resources. According to a 2022 VPN risk report published by *Cybersecurity Insiders*, 80% of companies are in the process of adopting Zero Trust in 2022, and many organizations may use a combination of both VPNs and Zero Trust principles to create a layered security approach.(13)

Internet exposure represents the single biggest ingestion point for downloading or installing malicious code or external parties gaining unauthorized access to the ADS. Careful restrictions, such as authentication verification and access control lists (ACLs) should be used to prevent unauthorized or unintended access to the system.

> <u>Risk Example</u>: During development, an engineer working for an ADS developer needs to host a simple web page from the ADS to monitor whether the system is visualizing correctly. The software package the engineer chooses to install is not listed in a closely monitored repository and contains a malicious ransomware package. The engineer adds the repository and installs a webserver to host the page, but also inadvertently installs the ransomware package. After restarting, the system is encrypted and will not boot or decrypt unless a ransom is paid to the bad actor who inserted the ransomware package.

This scenario can be avoided by carefully vetting allowed devices. Configuring the system to drop or deny unapproved inbound and outbound connections by default—and only allowing pre-approved connections—allows the necessary control over communications to maintain a safe and secure network. This can be achieved by using a simple firewall, implemented as close to the interface to the internet as possible.

Across the local internal network and through the secure VPN tunnel, developers use several standardized protocols, including Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and ZeroMQ Message Transport Protocol (ZMTP), to send commands and receive updates from the ADS. Implementing local firewalls (1) at the router that provides network access and (2) on the main computer of the ADS on the truck itself helps to "harden" system security. A firewall allows or denies traffic based on a policy (e.g., regular web traffic may be allowed on TCP port 80, but remote shell access through port 22 is blocked). More advanced solutions go beyond identifying the port that traffic comes through to also inspecting and verifying the data as it passes through.

Limiting traffic on the internet, or even the local network, ensures that an ADS runs as intended and is not affected by unapproved directions or actions from bad actors. The VPN solution already implements similar features in the network ACLs, where the ADS developer can control which ports are allowed for communication. The VPN should not respond when an unauthorized actor attempts to use a port where they are not allowed. Dropping traffic and not responding is a preferred security posture, as it does not confirm the presence of a system on the other end (which a rejected response would). The less exposure there is overall, the less possibility there is for attacks and fewer items to monitor for potential incidents.

The information coming from GPS and video cameras could also be vulnerable, but the related risks would involve more targeted attacks on the ADS. Unlike the broader internet risks discussed earlier, disrupting the accuracy of the GPS or video system requires a well-organized and skilled attacker who is specifically targeting a particular ADS. While these types of attacks are worrying, they are not as likely as the more common cybersecurity issues. However, when someone tampers with both GPS and video data in a mixed fleet of vehicles, the potential risks can be significant. Manipulating GPS and video data simultaneously can lead to severe navigation errors, disrupt route planning and monitoring, aid thieves in tracking and intercepting cargo, cause complex liability and legal challenges, expose sensitive information about vehicle occupants, drivers, and cargo, and ultimately damage the fleet's reputation for reliability, safety, and security.

All the above scenarios are means of protecting ADS-critical information in transit. This information, of course, needs to be protected when being processed and when being stored, either on the ADS or at the fleet control center.

5.8.2.2 Access

Wireless Access to ADS: Wireless access to ADS plays a fundamental role in enabling communication, data sharing, and control within mixed fleets of vehicles. However, it also presents unique cybersecurity challenges and considerations. Wireless access facilitates real-time communication between vehicles, infrastructure, and centralized fleet management systems. It enables the exchange of critical information, such as vehicle status, sensor data, GPS coordinates, and operational instructions. This communication is vital for managing and coordinating mixed fleets efficiently. There are several widely used types of wireless access:

- Cellular Networks: Many ADS rely on cellular networks to transmit data. This includes 4G and 5G networks, which provide high-speed connectivity and low latency, making them suitable for time-sensitive applications.
- Wi-Fi: Wi-Fi connectivity is often used for short-range communications within fleets or at depots. It can be employed for data transfer, software updates, and diagnostics.

- Satellite Communication: In remote or challenging environments, satellite communication provides a reliable means of connectivity for ADS, ensuring that vehicles remain connected even in areas with limited terrestrial network coverage.
- V2X Communication: This technology allows vehicles to communicate with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and more (V2X).

In section 5.8.2.1, cybersecurity software and communication vulnerabilities were discussed that rely heavily on wireless access to ADS. Although wireless access serves as an essential component in modern fleet management and AV operations, it also brings many unique cybersecurity challenges. Without proper security measures in place, malicious actors can potentially compromise the integrity and safety of the fleet. To address these challenges, several cybersecurity solutions are commonly employed. Strong encryption protocols protect data in transit over wireless networks, ensuring its confidentiality even if the data is intercepted. Robust access control mechanisms guarantee that only authorized devices and users can access the ADS wirelessly, including multifactor authentication mechanisms. Intrusion detection and prevention systems (IDS/IPS) continuously monitor for and respond to suspicious activity on wireless networks. Regular software updates, security audits, and penetration testing help identify and mitigate vulnerabilities proactively.

Physical Access to ADS: Physical access to ADS should also be considered when evaluating cybersecurity risks. The installed components should be easy to service but difficult to break into (i.e., preventing unauthorized physical access). Unauthorized physical access could bypass many of the network software restrictions, providing access to the local network the ADS is attached to or direct access to the onboard computer. At a lower level, physical access to the main ADS computer or other additional hardware leaves the system open to the threat of tampering.

To combat this, the bulk of an ADS product should reside in a closed metal (or other ruggedized) enclosure, secured with non-standard security screws to prevent unapproved access. Any physical connections not needed after development and installation should be removed. Exposed physical ports (serial, USB, SATA, Ethernet) pose potential risks for unapproved access to the ADS. Although physical access may not be something that a CMV fleet can constantly monitor in real time, tamper-resistant physical designs, along with tamper tape or seals across physical service or access points, will identify unauthorized access.

Besides physical access to the installed ADS components on the vehicles, physical access to infrastructure including roadside sensors, control units, and charging stations can also be a potential penetration point for cyberattack. Such physical components can provide opportunities to attackers for malicious activities such as data extraction, ADS device tampering/sabotage, and malware injections. Physical security, device tamper detection, secure boot and firmware validation, and the mechanisms to immobilize the vehicle under critical circumstances should all be taken into consideration.

User Account Access: All accounts that are set up for end-user access to an ADS should require strict authentication measures and should be regularly audited. After authentication, a level of access needs to be defined for each account, emphasizing PoLP[14], which refers to a user only receiving the level of access required to perform their job functions. To help manage what tasks each user can perform, the ADS developer should limit the kind of input the user can provide and retrieve from the ADS. This definition of access would span from absolute control over all aspects of the system (limited to senior internal development use only), all the way to read-only access for narrowly defined reporting and monitoring purposes. Starting from the least amount of access and working towards complete access, the developer should gradually add the appropriate amount of access for each user, making sure to add only the properties that are needed to the relevant user's account.

One simplified way to organize the increasing levels of a CMV fleet's access to the ADS could be to define user roles such as Administrator (Admin), Site Supervisor, Senior Foreman, Foreman, Operator, and Monitor. This type of access control is often referred as role-based access control (RBAC).(15) In general, Admins will have the greatest access, including the ability to create and remove accounts, set permissions for different accounts, and monitor the system, but they may not necessarily need access to set a destination and command the vehicles to drive. The Admin account level should only be given to trusted users who have shown proficiency in using the ADS and fully understand its capabilities and limitations, as this access level carries the most responsibility. Site Supervisors oversee and have access to most of the controls at the deployment locations and will need proficiency in the deeper workings of the system. A Foreman could handle journey planning and programming specific routes for the trucks to drive, as well as oversee a group of Operators who are running and supervising a particular ADS operation. A Monitor would only be able to access accounts and view what is happening within the ADS-equipped trucks.

> Risk Example: A disgruntled employee maliciously uses their system access to try to cause the ADS truck to cause harm. They program an unsafe path, but the vehicle correctly perceives a collision threat and refuses to proceed. The disgruntled employee uses their user account to repeatedly override the ADS's built-in protections (which keep activating) in the hopes of forcing the vehicle to crash.

There are several ways to avoid or mitigate this type of (extreme) incident. The ADS could be programmed with a limited number of overrides in a set period. After exceeding the criterion overrides, a higher-level account approval is needed to approve the override. Any override should be logged, audited, and monitored to ensure that someone with a high-level classification is notified of the incident.

Along with limiting who can operate the ADS (via user accounts) and setting levels of access (permission properties), CMV fleets should also implement a schedule of when systems can operate and when and where individual accounts are allowed to run them. A GPS coordinates check should be implemented to limit any access by devices that are not near sites authorized to send commands to the ADS-equipped truck. In addition to requiring individual user accounts, shared device use should be discouraged, as shared devices reduce the visibility and accountability for who was operating or connected to the ADS at a specific time. Multiple accounts might be used on the same device, but only one account should be logged in at a time. Lastly, standard password rules (eight or more characters long, three of the four [alpha, num, symbol, special] categories used) and password rotation should be employed (see the Cybersecurity and Infrastructure Security Agency password guidelines(16).

> Risk Example: An operator lets another member of their family use their phone (that includes the ADS control app). That family member opens the control app and starts a program, causing the truck to engage in a work mode without supervision or interrupting in-progress work.

These types of “accidental” or negligent risks are likely to be more common than malicious “hacks,” especially when ADS trucks are deployed at scale. Fortunately, these risks are also mitigated in a straightforward manner that is within the capability of sophisticated CMV fleets that would adopt ADS trucks. A time lock can prevent use of any ADS-related program if the operator is off duty. In addition, geofencing (using GPS) can limit where the control app is run in relation to the ADS truck. It should not be possible to operate any sort of device that controls the ADS without some form of authentication.

Beyond the accidental or negligent access of a user account, one must also consider the possibility of a high-level account being compromised, whereby commands are maliciously sent to the ADS from a third party. To protect against this type of situation, each account should have the ability to safely command vehicles to go to an MRC and/or flag an action for review. A master intent and audit log of all running vehicles should be published as a tab in all controls of the ADS. This tab should have a clear description of the planned truck’s path, what accounts activated the path, when all actions were taken, and the number of overrides performed.

For end users who control the ADS by means of a mobile device (iOS, Android, etc.), device security is of utmost importance. Securely logging into the app should require a username and password, in combination with multifactor authentication. Just as lower access accounts should be time locked out of running programs, access to the app must be reauthorized whenever a user turns their focus away or the device sleeps. At a regular interval, a password reentry should be required, regardless of the sleep or focus status of the app. Multiple accounts might be used on the same device, but only one account should be logged in at a time.

Passwords should also be kept secure. Having a pre-authorized account and password would be the easiest way for a bad actor to compromise the system. Standard password rules and rotating any passwords in use during development at regular intervals promotes regular auditing of all development devices in use. Leaving “stale” computer configurations in any part of the product life cycle makes the ADS an easier target. ADS developers can prevent this by setting a lifespan for a configuration. If a system has not been updated in a certain number of days, it should retire itself automatically or sunset itself until updated.

It should also be noted that while predefined passwords and access are easy to deploy in a small development environment, they may pose a significant vulnerability at larger scales. If the same password and account is used across multiple systems, then only one system needs to be attacked for all systems to be vulnerable. Moving towards a certificate-based authentication system would make the system easier for development engineers to access and make the system more secure overall. Certificates can be set to expire at specific dates and/or times, limiting the possibility of credentials being captured and used by bad actors.

5.8.2.3 Security Assurance Opportunities

This section discusses the opportunities to assure cybersecurity via the fleet's policy so that potential cyberattack can be minimized or eliminated in advance.

Training and Education: As mentioned under section 5.8.2.1, addressing the vulnerability caused by lack of cybersecurity awareness and training can involve educating users about the importance of strong and unique passwords, the risks of sharing personal data, and the significance of promptly applying software updates. Moreover, fostering a culture of cybersecurity awareness among the public can contribute to a safer and more resilient ADS ecosystem. When assuring cybersecurity, it is critical for the employees to have a clear understanding of how certain procedures should be performed and how to handle data safely. This requires thorough and easy-to-follow training supported by a thorough and concise cybersecurity policy from the fleet's management. This section discusses the importance of cybersecurity training and education of employees, such as building knowledge of cybersecurity and ADS and providing clear instructions on how certain procedures should be performed.

Training and education play a pivotal role in enhancing the cybersecurity resilience of ADS. Comprehensive training and education programs not only empower developers, engineers, and users with the knowledge needed to identify and address potential vulnerabilities but also foster a culture of cybersecurity awareness that extends throughout the ADS ecosystem. This security assurance opportunity provides benefits in multiple ways:

- Skill Enhancement: Cybersecurity training equips professionals with the skills to identify, assess, and mitigate vulnerabilities and threats specific to ADS technology. Developers and engineers learn to integrate security measures into the design and development stages, reducing the chances of vulnerabilities being introduced into the system. By staying current with the latest cybersecurity techniques and tools, professionals can proactively defend against emerging threats.

- Risk Mitigation: Educated professionals are better equipped to perform threat modeling, risk assessment, and vulnerability analysis. This proactive approach enables the identification of potential attack vectors and the implementation of appropriate safeguards, reducing the likelihood of successful cyberattacks.

- User Empowerment: Users and operators of ADS-equipped vehicles need to understand how to interact with the technology securely. Education empowers users to make informed decisions, such as recognizing suspicious behavior, managing software updates, and practicing safe driving habits while using autonomous features.

- Cultural Shift: Establishing a culture of cybersecurity awareness is essential. Comprehensive education programs help create a mindset where cybersecurity is prioritized at all stages of ADS development and use. This cultural shift fosters a collective responsibility for security among all stakeholders.

There are multiple feasible methods to implement training and education effectively, such as collaborating with cybersecurity experts, academic institutions, and industry leaders to develop comprehensive curricula that cover a range of topics, from secure coding practices to incident response strategies. Providing certification programs or awareness campaigns can stimulate and encourage people to voluntarily gain understanding of cybersecurity, and certifications can serve as a milestone for knowledge building and skill levels. Hands-on training can also help employees translate theoretical knowledge into real-world scenarios through simulations and labs, and it can provide invaluable experience in dealing with security incidents and rehearsal for EAPs. Meanwhile, cybersecurity is a rapidly evolving field. It will benefit stakeholders to implement continuous learning programs that encourage professionals to stay updated with the latest trends, vulnerabilities, and countermeasures. In addition, advocating for regulatory frameworks that require a minimum level of cybersecurity training and awareness for professionals working with automated systems is also recommended.

By investing in robust training and education initiatives, and with knowledgeable professionals and informed users, the risk of cyber threats affecting the safety and functionality of ADS can be substantially reduced.

Integrate Rulemaking for Facility Access and Device Security: Physical facility access and individual login devices are crucial elements that demand dedicated rulemaking to fortify security measures. Implementing regulations in these areas can establish a comprehensive defense strategy that not only prevents unauthorized physical access but also safeguards against unauthorized device usage.

Comprehensive security stands as a cornerstone of ADS cybersecurity. The introduction of rulemaking covering facility access and individual login devices bolsters defense mechanisms, reducing potential vulnerabilities and avenues for cyberattacks. This holistic approach acknowledges that safeguarding ADS technology encompasses both the digital and physical realms. Furthermore, rulemaking is essential to mitigating insider threats, as unauthorized facility access by malicious insiders could lead to severe breaches. Establishing regulations ensures that only authorized personnel gain entry to critical systems, significantly minimizing the risk posed by insider attacks.

The significance of end-to-end security in ADS cannot be overstated. Rulemaking in physical facility access and individual login devices contributes to an integrated cybersecurity framework. By enforcing stringent access control policies and advocating for multifactor authentication, organizations can prevent unauthorized access and enhance user verification. Biometric verification methods, like fingerprints and facial recognition, further strengthen security measures. Regular audits and inspections of physical access points and devices are vital to identifying vulnerabilities and maintaining compliance with security protocols. This proactive approach complements digital cybersecurity efforts, creating a more resilient defense against potential threats.

Collaboration and continuous improvement are key aspects of successful rulemaking. Partnering with regulatory bodies and industry experts helps establish standardized guidelines that align with evolving technological advancements. By fostering a culture of vigilance through training and awareness programs, personnel become more proactive in identifying and addressing potential facility security risks. Additionally, incident response protocols ensure a coordinated approach in case of security breaches or compromised devices.

Monitoring of Facility, Property, Driver States, and Vehicle Information: When systems are under cyberattack through physical or wireless sources, abnormal behavior inside the system might be the key to detecting such an attack. This section discusses the importance of developing a visually observable mechanism that monitors the system at all times to report any detected cyberattack to the system or the human users. Such a monitoring function should have access in all aspects of the fleet's operations.

Developing and embedding a visually observable monitoring system within mixed CMV fleets provides an additional layer of cybersecurity that enhances the overall safety and integrity of the fleet. This system acts as a vigilant watchdog, constantly monitoring all systems for signs of cyberattacks. Its rapid detection capabilities enable early intervention and response, crucial for mitigating potential threats before they escalate. By offering real-time visibility into the fleet's status, the system empowers human operators to make informed decisions and respond effectively, preventing false positives from causing unnecessary actions.

In the context of mixed CMV fleets, where various levels of automation coexist, a visual monitoring system builds trust among drivers, fleet managers, and passengers. It reassures stakeholders that cybersecurity is actively maintained, promoting confidence in the safety of the fleet's operations. Additionally, the system aids in regulatory compliance by providing visible evidence that cybersecurity standards are being upheld, simplifying reporting and audits.

Mixed fleets should have a unified fleet management platform developed that is capable of integrating the monitoring system and overseeing both automated and non-automated vehicles. Standardized communication protocols must be established to ensure compatibility with the system. Visual alerts should be user-friendly, displayed on dashboards or conveyed through notifications to drivers and fleet managers. Data fusion and analysis should provide a comprehensive cybersecurity overview by integrating data from various vehicle systems and sensors.

Human intervention remains crucial, thus facilitating bidirectional communication between the monitoring system and human operators. Operators must be equipped to validate alerts and make informed decisions based on real-time information. Training sessions should be conducted to familiarize drivers and fleet managers with the system's features and proper response procedures. Secure data transmission is paramount to prevent unauthorized access or tampering.

As the fleet evolves, scalability should be a design consideration, and fleet operators should ensure that the system is updated regularly to address emerging threats and incorporate new security measures. Striking a balance between cybersecurity and privacy is essential, ensuring that driver and passenger privacy is maintained while enabling necessary monitoring capabilities. Incorporating a visually observable monitoring system into mixed CMV fleets establishes a robust cybersecurity framework. With rapid detection capabilities, real-time awareness, and human intervention, this system bolsters security measures and promotes a safer environment for both automated and non-automated vehicles.

Internal Cybersecurity Team Risk Assessment: NHTSA released its *Cybersecurity Best Practices for the Safety of Modern Vehicles* in 2022, an update to its 2016 edition.(17) 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." This document places significant emphasis on the necessity of a comprehensive cybersecurity risk assessment process that aligns with the entire life cycle of the vehicle while keeping the safety of vehicle occupants and other road users at the forefront. This directive reflects the evolving nature of vehicle technology, highlighting the imperative to ensure the security of increasingly connected and AVs. In this complex landscape, robust risk assessments conducted by internal cybersecurity teams serve as a cornerstone for identifying vulnerabilities, evaluating potential threats, and implementing effective mitigation strategies.

The importance of internal cybersecurity team risk assessment for mixed CMV fleets is multifaceted. Firstly, it enables the comprehensive identification of potential vulnerabilities that may affect different vehicle models within the fleet. This tailored approach ensures that mitigation strategies are focused and relevant, addressing specific risks faced by each type of vehicle. Moreover, risk assessments prevent systemic vulnerabilities from propagating by considering the fleet as a cohesive ecosystem. This prevents a single vulnerability from compromising the security of the entire fleet.

In alignment with the guidance from NHTSA(18), risk assessments should span the entire life cycle of the fleet. Collaboration with vehicle manufacturers, technology providers, and regulatory bodies is crucial to ensure that assessments encompass the full spectrum of technological components. Through scenario-based analysis, internal teams can anticipate potential cyber threats and vulnerabilities, enhancing their ability to proactively address risks before they materialize.

To implement effective internal cybersecurity team risk assessment in mixed CMV fleets, a combination of factors comes into play. Regular audits and testing of implemented security measures validate their effectiveness and relevance. Integrating threat intelligence feeds into the system allows stakeholders to stay updated on evolving threats. Training and awareness programs for fleet personnel, drivers, and operators foster a culture of security consciousness, enhancing the overall effectiveness of risk assessment measures. Ensuring alignment with industry standards and regulations guarantees that risk assessment methodologies remain robust and relevant.

Internal cybersecurity team risk assessment is a critical aspect of the cybersecurity strategy of mixed CMV fleets. Its role in identifying vulnerabilities, prioritizing mitigation, and fostering a proactive approach contributes significantly to the overarching goal of establishing a safer and more secure transportation ecosystem.

Penetration Testing and Review: Penetration testing and reviews are vital in proactively identifying vulnerabilities, assessing the resilience of security measures, and fine-tuning defenses to effectively protect both autonomous and non-autonomous vehicles. By simulating real-world cyberattacks and conducting assessments, penetration testing and reviews contribute significantly to the overarching goal of maintaining a robust and secure fleet.

Penetration testing and reviews allow for the proactive identification of potential vulnerabilities that adversaries could exploit. By simulating diverse cyberattack scenarios, internal cybersecurity teams gain valuable insights into the fleet's weak points, enabling targeted mitigation strategies. Moreover, penetration testing and reviews help validate the effectiveness of existing security measures. Identifying gaps in the defense architecture allows prompt corrective actions, bolstering the overall cybersecurity posture.

To effectively implement the penetration testing and reviews, fleet managers must first define a comprehensive scope that includes all types of vehicles, communication protocols, and potential attack vectors. They should collaborate closely with third-party security experts who bring an external perspective to the assessment and conduct both black-box and white-box testing(19) to replicate different attack scenarios, testing not only the system's robustness but also the organization's response to breaches. After testing, they should perform an in-depth review of the findings, prioritizing vulnerabilities based on potential impact and likelihood. Fleets should implement timely and targeted mitigation measures, addressing identified weaknesses. To ensure continuous improvement, they should also conduct regular follow-up assessments to validate the effectiveness of implemented changes and identify new vulnerabilities that may arise due to evolving threat landscapes. Lastly, stakeholders should foster a culture of learning and awareness within the fleet, sharing insights and lessons learned from penetration testing and reviews with personnel, drivers, and operators. This helps develop a collective understanding of potential threats and cultivates a sense of ownership in maintaining cybersecurity.

5.8.2.4 Failure and Recovery

An ADS failure is an unexpected cessation of operations for unexplained reasons. A failure may be the result of a bad configuration, software or hardware bug, or intentional disruption of service. Just as hardware must be operated with a "fail-safe" mentality, the software must also "fail safely." If the ADS detects an interruption of regular operations, it should be able to restart itself and safely continue its job. However, if the ADS cannot safely continue its job, it needs to enter an MRC failure state. This includes failures related to cybersecurity.

Robust monitoring systems, with the ability to evaluate the severity of the failure, should be implemented to observe the ADS and determine if any action is necessary. There are different types of cybersecurity failures, from "small concern" to "immediate halt." The severity of the incident and the frequency of the incident should be considered when classifying these failures. Depending on deployment site and ODD, the scale may shift and need to be determined by a supervisor at the truck fleet and the ADS developer.

Recovery should be as fast as possible, as the risk of a stopped vehicle in an MRC may also be a hazard to other vehicles or people. Keeping at least one baseline software image on the system in a protected partition or disk could serve as an absolute fallback boot option. This baseline image should always be able to start the ADS and command the vehicle to safely come to a stop. A second "boot" image should exist that would store the latest good configuration changes and run the ADS during regular operation. A third "staging" image should be used to house any settings that need to change. Maintaining these separate images should allow the ADS to restart in a known good and safe configuration every time, even if it is not the desired configuration for a particular job.

It is critically important to ensure that restarting services while the vehicle is in operation does not lead to a cascade of issues. Each service that runs on the main computer should be able to do so as independently and modularly as possible. Although the ADS will need the coordination of many subsystems and services, smooth transition between failure and recovery can be the difference between operations that run for a long time and those that require frequent, in-person maintenance.

5.8.2.5 Emergency Action Plan

An EAP holds immense importance for a CMV fleet due to its role in managing cybersecurity incidents. In today's environment where cyber threats can disrupt operations, compromise data, and undermine safety, having a well-structured EAP is essential for the fleet's resilience. This strategy outlines a comprehensive plan for responding to cybersecurity incidents and breaches involving CMVs. Its significance lies in its ability to help fleet personnel navigate the challenges posed by cyber threats and minimize their impact on operations, safety, and reputation.

Developing an effective EAP requires a systematic approach that integrates various elements. First and foremost, the fleet needs to conduct a thorough risk assessment specific to its CMVs and operational context. This assessment identifies potential vulnerabilities, threat vectors, and areas of concern that might be targeted by cyber attackers. Stakeholder involvement is critical during this phase, encompassing fleet managers, drivers, IT professionals, and cybersecurity experts. Their collective insights and expertise provide a well-rounded understanding of the potential risks and appropriate response strategies.

The heart of the EAP lies in its documentation. The fleet should create a comprehensive plan that outlines procedures for different types of cybersecurity incidents. These procedures cover incident detection, escalation, containment, recovery, and communication protocols. By clearly defining these steps and the responsibilities of various personnel, the fleet can ensure a coordinated response, minimizing confusion and improving overall effectiveness.

A crucial aspect of EAP is its communication strategy. Timely and accurate communication is vital during cybersecurity incidents to prevent further damage and coordinate efforts. The plan should establish communication channels within the fleet and define how and when to communicate with external parties, such as technology vendors, law enforcement, regulatory authorities, and customers.

Training and awareness play a pivotal role in the successful implementation of the EAPs. Fleet personnel must be educated on the plan's details, their roles, and the actions they need to take during different incident scenarios. Conducting regular drills and exercises helps familiarize everyone with the EAP and enhances their ability to respond effectively during real incidents.

There is no panacea that solves all security problems, and the EAP is not a static document but a dynamic framework that requires regular review and updates. As technology evolves and new cyber threats emerge, the fleet should refine and adapt the plan to stay effective. Collaborating with cybersecurity experts, technology vendors, and industry associations can provide valuable insights into best practices and emerging trends. By systematically developing, implementing, and refining the EAP, the fleet demonstrates its commitment to cybersecurity preparedness, safeguarding its operations, reputation, and the trust of stakeholders in the ever-evolving landscape of digital threats.

5.8.2.6 Life Cycle

To maintain and continually improve cybersecurity, ADS will need to evolve through several clearly defined stages of its life cycle. These stages define different levels of severity in maintaining cybersecurity, from fairly low in early development to very high in customer deployment. During the development stage of an ADS, the focus is on building and refining its capabilities. In this stage, it is essential to lay the groundwork for cybersecurity. While free and open network and system communication may be necessary to facilitate development, implementing security policies in a well-controlled environment is also crucial. This early attention to security sets the stage for a secure future. As part of this stage, ADS developers should establish a framework for secure software updates. Even at this early stage, considering how updates will be securely delivered and verified is important.

As the ADS progresses to the testing stage, more stringent cybersecurity measures should be enforced. Access control should include certificate authentication for access, ensuring that only authorized personnel can make changes. Communication should occur through secure channels, such as a VPN, to protect data during transit. Additionally, an audit schedule should be established to monitor for any anomalies. This is also the stage where the communications critical to running the ADS are defined, and extraneous methods are blocked or removed. It is vital to implement testing and verification of software updates to ensure they do not compromise the system's security.

In the deployment stage, the ADS should be ready to operate autonomously with robust cybersecurity measures in place. Access should be tightly controlled, debugging ports should be closed (and possibly sealed), and unnecessary communication methods and wireless networks should remain disabled unless required for specific functions. Software updates are critical at this stage to address vulnerabilities and improve performance. The ADS should be capable of securely communicating updates to authorized parties, ensuring that its software remains up to date and resilient against emerging threats.

The service stage represents a period when the ADS might require maintenance or updates while in operation. Some previously disabled communications may need to be re-enabled for servicing purposes. This is where the importance of secure software updates becomes evident. If the ADS enters the service stage due to internal system issues, it should automatically return to the deployment stage after a successful audit and safety engineer approval. Regular service stages should also include software audits and testing to ensure the ADS's ongoing security.

The end-of-life stage is a critical consideration. Here, the ADS may be nearing obsolescence, making it vulnerable to cyberattacks due to discontinued support and security updates. Meanwhile, the regulatory and legal risks of using outdated operating systems can result in breach of contract, failure to meet industry standards, and a series of other liability issues.(20) It is essential to plan for the secure retirement of older ADS by building in safeguards, such as a maximum run-time limit, to ensure the systems do not operate without mandatory updates. This stage highlights the importance of secure software updates, even as ADS approach the end of their operational life.

5.8.2.7 CMV Fleet Expectations

As described above, good management practices with respect to authorized user accounts at a CMV fleet are critical. In addition, control and tracking of the physical access to the ADS-equipped truck are also important components in a CMV fleet's cybersecurity approach. It is critical that CMV fleets have the highest standards of security for all their networks. Regularly reviewing and updating the security systems is a simple and effective way to mitigate most threats.

Before deploying ADS technologies at a site, ADS developers should talk with the personnel at the CMV fleet partner to ensure that they understand the capabilities and the safety requirements for deploying an ADS. The devices the CMV fleet uses to control and supervise ADS-equipped trucks should only be used for this purpose. Other unapproved applications or functions should not be installed on the device without the approval of the ADS developer. As the device will need an internet connection to communicate with the ADS-equipped truck, the ADS developer might need to monitor this connection and block most other traffic. CMV fleets should not attempt to circumvent these restrictions, as they are in place to keep the ADS safe. Any device, whether personal or deployed, that connects with the ADS should not share access with unauthorized personnel. Using devices that are unprotected, unlocked, or unattended is akin to leaving the keys to the truck accessible to anyone.

5.8.3 Data Transfer/Security

Data resides in multiple states, including data in storage, data being processed, and data in transit. Data and information are vulnerable in all three states, and there are protective cybersecurity measures appropriate to each. In this section, we discuss protecting information in each of these states. We also discuss several information assurance measures, including data sharing rules, data logging, and data auditing.(21)

5.8.3.1 Data Storage

Data storage is a critical component of data security and cybersecurity for mixed CMV fleets. One fundamental practice is encryption at rest, which involves encrypting data before storing it in databases, servers, or storage devices.(22) This ensures that even if an attacker gains physical access to the storage, the data remains unreadable without the encryption key. Fleets should implement industry-standard encryption algorithms, like Advanced Encryption Standard 256 encryption, which is a symmetric encryption algorithm that uses a 256-bit key to convert plain text or data into a ciphertext.(23) While encryption is essential for data security, it is equally important to store encryption keys securely and restrict access only to authorized personnel.

Access control is another crucial aspect of data storage security. Preventing unauthorized individuals from accessing sensitive data is essential. Access control limits data access to those with a legitimate need for it, reducing the risk of data breaches. Implementing RBAC, as mentioned in section 5.8.3.2, is a common practice, where permissions are assigned based on job roles. Regularly reviewing and updating access privileges as job roles change is vital, as is monitoring and auditing access logs to detect and respond to unauthorized access attempts.

Secure backups are essential not only for data recovery in case of hardware failures or cyberattacks but also for data security. Securely storing backups in off-site locations or encrypted cloud storage protects against data breaches. Data retention policies, which define how long data should be stored and when it should be securely deleted, are critical for compliance with regulatory requirements. Developing clear data retention policies, automating data deletion processes, and regularly reviewing and updating these policies as regulations evolve ensures data is managed securely and compliantly.

Data masking or data anonymization techniques are essential for protecting sensitive data while maintaining its utility, especially in non-production environments or for testing purposes.(24) These techniques transform sensitive data so that it is of little or no interest to unauthorized users but still remains usable to those who need it. Secure disposal of data is equally important. When data is no longer needed, it must be securely disposed of to prevent data breaches. Data wiping or disk shredding methods are used to securely delete data from storage devices before disposal, and any decommissioned hardware must be thoroughly cleaned of sensitive data.

5.8.3.2 Data Processing

Data being processed by components of an ADS is also subject to multiple threats, including unauthorized access and modification, processing errors, and presence of unexpected software components. It involves several key practices aimed at maintaining data integrity, identifying anomalies, and safeguarding against cybersecurity threats.

One crucial practice is data validation. This involves implementing routines to validate and cleanse incoming data to ensure its accuracy and integrity. Doing so reduces the risk of malicious or erroneous data affecting fleet operations. Data validation routines check for inconsistencies, missing values, and outliers, ensuring that only reliable information is processed. This practice is particularly important when dealing with real-time data from various sources, such as vehicle sensor data.

Another essential practice is anomaly detection.(25) Anomaly detection algorithms are used to identify unusual patterns or behaviors in data. This is vital for promptly detecting potential cybersecurity threats or system malfunctions. By continuously monitoring data for deviations from expected norms, fleet operators can identify and respond to suspicious activities in real time. This proactive approach is essential for maintaining the data security and reliability of CMV fleets.

Furthermore, secure data processing includes a focus on secure APIs.(26) If data is shared through APIs, it needs to be protected with robust authentication mechanisms, rate limiting, and security tokens. API security ensures that data is exchanged securely between different systems and applications and prevents unauthorized access or tampering with data during transit. Fleet operators should also continuously monitor data processing pipelines for signs of unusual activity or unauthorized access. This includes setting up alerts and notifications to respond promptly to potential breaches or issues. Real-time monitoring not only helps detect cybersecurity threats but also ensures that the fleet operates smoothly and efficiently. Once again, logging, tagging with validating information, and performing audits pre and post processing can help identify whether modification or processing errors have occurred.

5.8.3.3 Data In Transit

Secure data transit practices are designed to safeguard information as it moves between vehicles, central systems, and external entities. One of the fundamental principles in this context is encrypted communication (e.g., Google[27]). Data in transit should always be encrypted using strong cryptographic protocols. Encryption ensures that data remains confidential and cannot be intercepted or tampered with by unauthorized parties. Secure Socket Layer and Transport Layer Security are commonly used encryption protocols for establishing secure connections.[28]

VPNs are important tools for ensuring secure data transit in CMV fleets. VPNs protect data as users interact with apps and web properties over the internet, and they can keep certain resources hidden.[29] This is particularly vital when CMV fleets need to transmit data over untrusted or public networks, such as the internet. VPNs establish a secure path for data to travel, ensuring its confidentiality and integrity throughout the process.

Meanwhile, secure APIs are also essential tools when facilitating secure communications within CMV fleet infrastructure. APIs (as mentioned in 5.8.4.2) enable the exchange of data between systems and applications. Secure API practices involve implementing strong authentication mechanisms, such as API tokens or Open Authorization (OAuth) tokens. Rate limiting and access controls are also essential to prevent misuse or unauthorized access. API security guarantees that data is exchanged securely, maintaining data integrity.

Certificate-based authentication serves as a robust means of verifying the identities of devices and users involved in data transit. Each device or user is issued a digital certificate, which is used to authenticate them during data exchange. This practice ensures that only trusted entities can access and transmit data. By employing certificate-based authentication, CMV fleets mitigate the risk of unauthorized access and data breaches.

To proactively monitor data transit for potential security incidents, CMV fleets should also deploy IDS/IPS. These systems continuously monitor network traffic for signs of unauthorized access or malicious activities.[30] When unusual patterns or threats are detected, IDS/IPS can trigger alerts or take preventive actions. This real-time monitoring helps safeguard data integrity and respond swiftly to potential cybersecurity threats.

5.8.3.4 Data Sharing Rules

Data sharing rules are established protocols and regulations that dictate how data is collected, stored, transmitted, and shared within a system or organization. These rules ensure that data is handled securely and responsibly, reducing the risk of unauthorized access, data breaches, and cyberattacks. By outlining clear guidelines for data sharing, mixed CMV fleets can enhance their overall cybersecurity posture, fostering a safer and more reliable transportation ecosystem.

Data collected from both automated and non-automated vehicles can include sensitive information about vehicle operations, passengers, and locations. To implement effective data sharing rules within mixed CMV fleets, a systematic approach is essential. Fleet operators should begin by defining clear guidelines for the types of data collected, who has access to it, and the purposes for which it will be used. They should collaborate with legal experts and relevant regulatory bodies to ensure compliance with privacy and cybersecurity regulations. Fleets should also develop a data classification system that categorizes data based on its sensitivity, allowing appropriate levels of access and protection.

Encryption plays an essential role in data security. Fleets will need to implement robust encryption protocols for data both at rest and in transit. This safeguards data from unauthorized access and tampering, even if a breach were to occur. Regularly updating encryption algorithms and methods will allow the fleet to stay ahead of emerging threats. They should also incorporate strict access controls to limit data access to authorized personnel only. Fleets should implement multifactor authentication for users accessing sensitive data to enhance verification processes and monitor data access and usage patterns to identify any suspicious activities promptly. Regular audits and assessments are crucial to ensuring ongoing compliance with data sharing rules, so stakeholders should conduct routine evaluations of data handling practices, security measures, and compliance with regulatory requirements. They should periodically review and update the data sharing rules to align with emerging threats and evolving technology. Lastly, fleet managers and operators should educate all stakeholders within the mixed CMV fleet ecosystem about the importance of data sharing rules and cybersecurity practices. Drivers, operators, fleet managers, and personnel should understand their roles in adhering to these rules and promoting a culture of responsible data handling.

5.8.3.5 Data Logging

All ADS-equipped vehicles engage in significant data logging, recording, and making notations to files of different types of events that happen in and around the vehicle. To promote security, the ADS should also keep track of system events, access to the system from any source (CAN, communication/data transfer network, local, etc.), and any potential hardware or software errors. Access to this type of logged data is important, as it can be used to pinpoint where, when, and by whom any setting was changed (in case an incident requires investigation). Besides knowing what happened after the fact, having a dedicated service for monitoring logs and looking for non-standard events can mitigate incidents proactively. Non-standard events could be anything from the system recognizing an object that does not belong in its operating environment to an intermittent loss of GPS signal or network connectivity. Thresholds set in a monitoring system can notify engineers and end users of developing issues and can prevent escalation of issues and potential unexpected downtime.

Log storage should be redundant to prevent any data loss or manipulation. Data backup standards, such as a centralized logging system,(31) will need to be implemented to maintain records of all actions at any particular site. To maintain the integrity of the log, any commands and operations performed by the ADS should be logged internally but should also notify at least two other devices installed at a site.

Copying the logs as often as possible into a mass storage solution, either in the cloud or at a data center, mitigates onboard storage problems and enables auditing of the ADS-equipped vehicles while deployed. Secured internet access is the fastest means of data transfer. When a secure internet connection is unavailable, the CMV fleet would need to support a local transfer of logs during regular service intervals (and before local storage capacity onboard the truck runs out).

5.8.3.6 Auditing

Auditing in data security is all about ensuring the confidentiality, integrity, and availability of data while identifying vulnerabilities, compliance issues, and potential security threats. Before the start of the auditing process, organizations must determine what data and systems will be audited, the goals of the audit (e.g., security assessment, compliance verification), and the specific criteria against which performance will be evaluated. Once the objectives and scope have been determined, one of the first areas assessed during an audit is data access and permissions. Auditors review who has access to data, the level of access they possess, and whether access rights are appropriately granted and revoked. Unauthorized or inappropriate access can lead to data breaches. Data encryption is another critical component of data security audits. Auditors evaluate whether encryption is used to protect sensitive data during transmission and while at rest. Proper implementation of encryption protocols and key management is vital for safeguarding data against unauthorized access.

During these audits, comprehensive logging and monitoring practices are thoroughly examined. Organizations should maintain detailed logs of data-related activities, system events, and user actions. Auditors ensure that logs are consistently generated, securely stored, and regularly reviewed for anomalies or security incidents. In parallel, auditing includes verifying that organizations have established and adhered to data retention policies. These policies define how long data should be stored and when it should be securely deleted, contributing to efficient data management and compliance.

Should a data security incident occur, an audit will assess incident response and recovery capabilities. Auditors evaluate an organization's preparedness to detect, respond to, and recover from incidents like breaches or data loss. Auditing also ensures compliance with regulatory requirements and relevant data security regulations. Furthermore, vulnerability assessment is one of the core components of auditing. Auditors identify potential weaknesses in data security, including software vulnerabilities, misconfigurations, and gaps in security controls. Remediation plans are often developed based on these findings. Employee training and awareness programs are evaluated to ensure that employees are educated about data security best practices. Awareness is key to ensuring that employees understand their roles and responsibilities in maintaining data security.

Lastly, auditing is not a one-time event but rather an ongoing process. Auditors recommend improvements and track the organization's progress in implementing security measures. Continuous improvement is vital to stay ahead of evolving security threats.

5.8.4 Specific Best Practices for Fleet Cybersecurity (Scenarios & Mitigation Strategies)

This section goes beyond generic cybersecurity advice to provide actionable insights for fleets. It focuses on fleet management-specific challenges to ensure the recommendations are directly applicable to stakeholder needs and operational scenarios. By highlighting specific attack scenarios, this section raises awareness of potential threats that fleet operators might not have considered.

5.8.4.1 Cyberattack Through Wireless Connections

Wireless Network Intrusion: Wireless network intrusion is a concerning scenario, as it can happen in seemingly innocuous locations. This type of intrusion refers to cyberattacks that target the wireless networks utilized within connected vehicle fleets. Attackers often target public Wi-Fi networks at rest stops, exploiting unsuspecting drivers and weak network security. Fleet operators need to prioritize the security of wireless connections, implement robust encryption, and educate drivers about the risks associated with connecting to unfamiliar networks, especially when the internet connection is free.

> Scenario: Attackers can infiltrate the fleet's wireless networks, including Wi-Fi and cellular connections, at various points such as rest stops or fuel stations. They may exploit weak security, steal credentials, and gain unauthorized access to fleet systems.
>
> Impact: Unauthorized access can lead to data theft, privacy leaks, manipulation of vehicle functions, or disruption of communication between vehicles and the control center.

Mitigation measures:

- Implement strong encryption protocols to protect data transmitted over wireless networks.
- Enforce strict access control policies to limit who can access the wireless network.
- Deploy IDS to continuously monitor network traffic for any suspicious activities or intrusion attempts.
- Keep network equipment, including routers, access points, and connected devices, up to date with the latest security patches and firmware updates.
- Isolate critical vehicle systems and data from less critical parts of the network.
- Provide cybersecurity training for fleet personnel to raise awareness of the risks associated with wireless network intrusion.
- Develop a comprehensive EAP to address network breaches promptly. This plan should include steps for identifying, containing, and mitigating security incidents.
- Ensure that third-party vendors responsible for providing network hardware and services adhere to strict security standards.

GPS Spoofing and Manipulation: GPS spoofing and manipulation can be more sophisticated than one might think. Attackers can disrupt entire supply chain routes by deceiving vehicles about their location. Ensuring the integrity of GPS data is crucial, and fleet operators should consider implementing GPS signal authentication mechanisms to detect and prevent spoofing.

> Scenario: Cybercriminals can manipulate GPS signals or spoof satellite signals to deceive fleet vehicles about their actual location.
>
> Impact: GPS manipulation can result in incorrect routing, lost cargo, unsafe driving conditions, operational inefficiencies, and financial losses.

Mitigation measures:

- Implement GPS signal authentication mechanisms to verify the authenticity of received GPS signals.
- Regularly perform integrity checks on GPS data to identify anomalies or inconsistencies that may indicate manipulation.
- Educate drivers about the possibility of GPS manipulation and instruct them on verifying routes manually when GPS information appears inaccurate.
- Utilize multiple data sources, such as onboard sensors and external mapping data, to cross-reference and validate GPS information.
- Consider integrating blockchain or tamper-evident technologies into GPS data storage and transmission to ensure the integrity of location data.
- Implement monitoring systems that can detect sudden and unexpected changes in vehicle positions and trigger alerts when inconsistencies are detected.
- Keep GPS navigation software and maps up-to-date with the latest versions to minimize vulnerabilities to known exploits.
- Secure GPS receivers and antennas to prevent physical tampering or unauthorized access.
- Ensure compliance with regulations related to location data accuracy, especially in industries with strict safety and compliance requirements.
- Collaborate with cybersecurity experts and organizations specializing in GPS security to stay informed about emerging threats and best practices.

Cargo Theft at Transfer Points: Cargo theft at transfer points is a cybersecurity scenario that involves cyberattacks targeting cargo tracking and monitoring systems at locations where goods are transferred, such as ports, warehouses, loading docks, and transfer hubs, which should be a serious concern for fleet management. Attackers exploit vulnerabilities in these systems to facilitate cargo theft. Fleet operators must enhance cybersecurity measures at cargo transfer points, employ robust access controls, and consider implementing blockchain or tamper-evident technologies to ensure cargo data integrity.

> Scenario: Cyberattacks can target cargo tracking and monitoring systems at ports, warehouses, or loading docks. Attackers may manipulate cargo data or disrupt tracking systems to facilitate cargo theft.
>
> Impact: Cargo theft can result in significant financial losses, disrupt supply chain operations, and erode trust between fleet operators, customers, and partners, potentially impacting future business relationships.

Mitigation measures:

- Implement strict access controls such as biometrics, access cards, or personal identification numbers at transfer points, limiting entry to authorized personnel only.

- Employ video surveillance and monitoring systems to oversee cargo transfer operations.
- Utilize advanced cargo tracking technologies, such as IoT devices and radio-frequency identification tags, to monitor cargo location and condition in real time.
- Employ tamper-evident packaging and security seals on cargo containers to detect unauthorized access or tampering during transit.
- Consider implementing blockchain technology in the supply chain to provide an immutable and transparent record of cargo movements.
- Conduct regular security audits and vulnerability assessments of transfer points to identify and address weaknesses in physical and digital security.
- Train personnel at transfer points on security protocols, recognizing suspicious behavior, and reporting incidents promptly.
- Collaborate with law enforcement agencies and local authorities to share information on cargo theft trends and facilitate investigations.
- Implement geofencing technology to create virtual perimeters around transfer points. Any movement of cargo outside of these boundaries can trigger alarms and alerts.
- Develop a comprehensive EAP specifically tailored to cargo theft incidents.

Remote Diagnostics Exploitation: Remote diagnostics exploitation refers to cyberattacks that target the wireless connections used for remote diagnostics and maintenance in connected vehicles. These connections enable vehicle manufacturers or fleet operators to access the vehicle's onboard systems and collect diagnostic data, allowing remote troubleshooting, maintenance, and performance monitoring. However, cybercriminals can exploit these connections for malicious purposes.

> Scenario: Attackers may exploit wireless connections used for remote diagnostics and maintenance. They can gain unauthorized access to vehicle systems, tamper with diagnostics, or disrupt critical maintenance procedures.
>
> Impact: Unauthorized access can compromise vehicle safety, lead to operational disruptions, and result in costly repairs.

Mitigation measures:

- Implement robust encryption and secure communication protocols to protect remote diagnostic connections from unauthorized access.
- Implement multifactor authentication for remote diagnostics access to enhance security. This ensures that only authorized personnel can access and control vehicle systems.
- Employ IDS to monitor network traffic and system behavior for any unusual or malicious activities.
- Require fleet personnel to receive training on recognizing and responding to potential cybersecurity threats related to remote diagnostics. They should be cautious about sharing access credentials and report any suspicious activities.

- Regularly update vehicle software and firmware to patch known vulnerabilities. This reduces the risk of exploitation through outdated software.
- Isolate remote diagnostics systems from critical vehicle control systems. This segmentation prevents attackers from moving laterally through the network if they gain access.

Telematics System Vulnerabilities: Telematics systems are the lifeblood of fleet management, providing critical insights into vehicle performance, location, and driver behavior. Safeguarding these systems is essential to maintain accurate data and operational efficiency. Employing data integrity checks and secure communication channels can mitigate this risk.

> Scenario: Fleet telematics systems, which provide real-time vehicle data, are susceptible to cyberattacks. Attackers can manipulate telematics data to provide false information about vehicle performance or location.
>
> Impact: False telematics data can lead to data manipulation, privacy leaks, misinformed decision-making, route deviations, and compromised safety.

Mitigation measures:

- Regularly update telematics system firmware and software to patch known vulnerabilities and improve security.
- Implement strong authentication mechanisms and access controls to ensure that only authorized users can access and manipulate telematics data.
- Encrypt telematics data during transmission and storage to protect it from interception and tampering.
- Incorporate the ability to revert to the prior firmware version if an over-the-air update fails or introduces vulnerabilities and use false injection mitigation methods such as redundant verification safeguards.(32)
- Deploy IDS to continuously monitor telematics system traffic for any suspicious activities or intrusion attempts.
- Use secure communication protocols to protect data transmitted between vehicles and the central control center.
- Provide cybersecurity training for personnel who interact with or manage telematics systems to raise awareness of potential risks and threats.
- Evaluate the security practices of telematics system vendors and choose vendors that prioritize cybersecurity.
- Isolate telematics systems from critical vehicle control systems to limit the potential impact of a breach.
- Develop an EAP specifically tailored to telematics system breaches. This plan should outline steps for identifying, containing, and mitigating security incidents.

- Ensure compliance with relevant data privacy and security regulations, especially in industries with strict safety and compliance requirements.

IoT Device Exploitation: IoT device exploitation involves cyberattacks that target the interconnected devices and sensors that are an integral part of connected vehicle fleets. These devices collect data on vehicle performance, environmental conditions, cargo condition, and driver behavior, providing valuable insights for fleet management, but they can be entry points for cyberattacks. Attackers exploit vulnerabilities in IoT devices to compromise data integrity or gain unauthorized access. Fleet operators should prioritize securing IoT devices through firmware updates, network segmentation, and regular vulnerability assessments.

> Scenario: Fleets often employ IoT devices for cargo tracking and monitoring. These devices can be targeted by attackers seeking to tamper with cargo data or disrupt the IoT network.
>
> Impact: Unauthorized access can lead to data manipulation, cargo mismanagement, operation delays, privacy concerns, and potential theft.

Mitigation measures:

- Regularly update IoT device firmware and software to patch known vulnerabilities and enhance security.
- Implement strong authentication mechanisms and access controls to ensure that only authorized users can access and manipulate IoT device data.
- Encrypt data transmitted by IoT devices to protect it from interception and tampering.
- Deploy IDS to continuously monitor network traffic involving IoT devices for any suspicious activities or intrusion attempts.
- Evaluate the security practices of IoT device vendors and select vendors that prioritize cybersecurity.
- Isolate IoT device networks from critical vehicle control systems to limit the potential impact of a breach.
- Provide cybersecurity training for personnel who interact with or manage IoT devices to raise awareness of potential risks and threats.
- Develop an EAP specifically tailored to IoT device breaches. This plan should outline steps for identifying, containing, and mitigating security incidents.
- Ensure compliance with relevant data privacy and security regulations, especially in industries with strict safety and compliance requirements.

5.8.4.2 Cyberattack Through Physical Connections

Physical cyberattacks involve malicious actions targeting connected vehicles and their systems when they are stationary, undergoing maintenance and repair, or making stops at various locations. Such attacks involve malicious actions targeting connected vehicles through physical connections. Attackers may exploit vulnerabilities in vehicle systems or access points to compromise data integrity, gain unauthorized control, or plant malware. The attack vectors encompass all the physical connections that could be established between the vehicle and an external attacker (direct access attacks[33]) using access points such as the on-board diagnostic (OBD) port, the USB and jack connections, and the vehicles' chargers.

Physical cyberattacks typically happen when the vehicle is stationary during events such as maintenance and repair, rest and fuel stops, cargo transfer at different locations, charging at electric charging station, and inspection at truck stops. Physical cyberattacks when the vehicle is not stationary are more challenging but not impossible, but the attack vector usually still revolves around gaining physical access to the vehicle's OBD port.

Maintenance and repair activities could be performed either by ADS vehicle operator personnel or a third party, but in any case, these activities may require establishing physical connection with the vehicle network, which brings the possibility of cyberattacks. Attackers exploit vulnerabilities in vehicle systems, diagnostic tools, or network connections to compromise data integrity, gain unauthorized control, or implant malware. In a collision, there may be damages to components responsible for protection against cyberattack, potentially leaving vulnerabilities that hackers could exploit.[34] In fact, NHTSA suggests considering the resilience of cybersecurity measures to crashes as a key component of CMV fleet security.[35] Routine maintenance is planned maintenance to the vehicle and system usually performed by a third party. These activities encompass a range of tasks such as inspections, diagnostics, tune-ups, and component replacements. Physical connections through the OBD-II port are often required during the operations.

With incidents during rest and fuel stops, if the attackers have identified the fleet's predefined rest stop locations and have access to the vehicle GPS data, they can arrive at a stop ahead of the fleet vehicles. They can potentially pose as a maintenance crew or a fellow driver to gain physical access to the vehicles; once they gain physical access to a vehicle, they can install a small malicious device within the vehicle's OBD port. Such devices usually contain a wireless transmitter and allow the attackers to capture sensitive data relating to the vehicle, the driver, and the cargo; it may even grant them remote access into the vehicle's systems to manipulate vehicle functions. Attacks can happen during cargo transfer at different locations and truck inspections at truck stops in similar structures. Attackers using this strategy usually start with knowledge preparation to get familiar with the fleet's schedule and predefined locations, using forged identification and impersonation to bypass security with different methods and different levels of social engineering tactics (as fellow driver, uniformed inspection officer, crew members, contracted workers, etc.), then physical installations through the vehicle's OBD port.

Electric vehicle (EV) battery management systems (BMS) within a mixed fleet require regular charging at charging stations to maintain their operational range. Charging stations are essential infrastructure for EVs, and fleet operators rely on them to keep their EVs powered. An attacker with knowledge of the fleet's EV charging schedules can potentially gain access to the infrastructure of commonly used charging stations during low-visibility hours along fleet routes, then install malicious hardware within the charging infrastructure with the intent to activate during fleet charging sessions. During charging, the attackers may manipulate charging parameters, such as voltage levels, to damage the BMS or gain access to sensitive data or vehicle functions.

Impact: These attacks can result in data tampering, vehicle damage, malware injection, operation disruption, cargo theft through cargo diversion, financial loss, and reputation damage.

Mitigation measures:

- Promote secure vehicle lockdown and physical security awareness; implement mechanisms to lock down vehicles during stops and train drivers and operational personnel to recognize suspicious activities and report potential security threats. Encourage personnel to lock the doors, secure the keys, and park the vehicle in secure locations.[36]
- Limit access to parked vehicles during rest stops and employ security personnel or surveillance systems to monitor the area; establish rigorous inspection procedures for vehicles during rest stops to detect and remove unauthorized devices.
- Isolate the diagnostic port (OBD) used to identify vehicle broken parts from the vehicle network via firewalls and/or gateway modules. It may be useful to isolate the vehicle bus(es).
- Disconnect the component(s) under repair from the vehicle network during service and reconnect only after services are completed.
- Identify and select reputable charging station providers and inspect stations for signs of tampering or unauthorized access.
- Train personnel to inspect hardware, vehicles, and infrastructure for signs of tampering or damage.
- Explore the option of blocking message transmissions between the OBD-II port and the vehicle network when third parties are present. One way to address this is by equipping fleet vehicles with mechanisms to detect attacks and implementing cryptographic solutions to monitor frame injection, allowing for remote security updates upon attack detection.[37] However, it is generally important that cybersecurity measures designed to safeguard data must ensure the integrity of vehicle maintenance procedures while concurrently monitoring non-maintenance-related information.
- Ensure that cybersecurity measures recover and are back to their nominal state, check for any compromised software, evaluate the integrity of cryptographic systems, and verify that communication channels remain secure.
- Implement robust physical security controls at maintenance and repair facilities, including surveillance, access control, and secure storage for diagnostic tools and software.
- Conduct regular security audits of maintenance facilities to identify vulnerabilities and weaknesses in physical security.
- Establish procedures to verify the integrity of diagnostic devices and software used during maintenance to detect unauthorized modifications.
- Ensure secure communication protocols are in place for transferring data between vehicles and maintenance facilities to safeguard data integrity during service operations.

- Develop a comprehensive EAP tailored to address physical cyberattacks during maintenance and repair. The plan should include procedures for identifying, containing, and mitigating security incidents.
- Evaluate the security practices of maintenance service providers and select vendors that prioritize cybersecurity and data protection.
- Ensure compliance with industry-specific regulations and standards related to cybersecurity and data privacy in the maintenance and repair process.

5.8.4.3 Customized Vehicle Parts from Third-party Providers

Customized vehicle parts from third-party providers can introduce both opportunities and risks for fleet management. Customized vehicle parts have had their design modified to meet the needs of the fleet owner or operator. These customized components are typically designed to enhance vehicle performance, functionality, or aesthetics. Security measures that applied to the original parts may no longer be effective protections for the custom design. Many customized vehicle parts include embedded software for functionality enhancements that may involve vulnerabilities in the software, which attackers could exploit to gain unauthorized access to the vehicle's systems or to introduce malware. In extreme cases, the provider may have knowingly introduced other threats. The supply chain for customized parts may introduce risks, as attackers can target the production or distribution process to inject malicious code or compromise the integrity of the components. Customized parts with communication modules, such as GPS trackers or telematics systems, may be susceptible to cyberattacks. Attackers could compromise these modules to intercept sensitive data or manipulate vehicle behavior. Cyber risk in the supply chain was one of the topics of a recent Presidential Executive Order on U.S. supply chains.(38)

Additionally, hardware interoperability is a necessity in the heavy-vehicle sector. Third-party parts may not seamlessly integrate with the existing vehicle software and systems, potentially leading to compatibility issues that cybercriminals could exploit to disrupt vehicle operations or compromise security. Heavy vehicle components often originate from various suppliers, which therefore necessitates cohesive system integration. SAE J1939, which specifies the communication network protocol, facilitates interoperability and flexibility among different components,(39) but further cybersecurity measures are necessary to accommodate this need for flexibility.

To mitigate cybersecurity risks from customized third-party parts, fleets should consider these measures:

- Prior to integrating third-party components, conduct thorough security assessments of the embedded software and communication modules. Look for vulnerabilities and work with providers to address any identified issues.
- Choose third-party providers with a strong commitment to cybersecurity. Verify that they follow best practices in software development, employ secure coding standards, and regularly update their software to patch known vulnerabilities.
- Test customized parts for compatibility with existing vehicle systems and software. Ensure that any integration does not introduce weaknesses that could be exploited.

- Stay vigilant about security updates and patches for customized components. Ensure that providers offer timely updates to address newly discovered vulnerabilities.
- Employ strong encryption protocols for data transmitted to and from customized parts with communication capabilities. Protect sensitive information from interception during transit.
- Implement strict access controls to limit who can interact with customized parts. Unauthorized access should be prevented through robust authentication and authorization mechanisms.
- Collaborate with providers to establish supply chain security measures. Verify the integrity of components at each stage of production and distribution to prevent tampering.
- Develop a comprehensive EAP specific to cybersecurity incidents involving customized parts. Clearly define procedures for detecting, containing, and mitigating cyber threats.
- Provide cybersecurity training to fleet personnel to raise awareness about the risks associated with customized components and how to recognize and report potential cyber threats.

These measures to mitigate risks from customized parts, or parts that have been modified, are part of the cybersecurity efforts to protect the supply chain, and it is essential that fleet owners and operators consider them as an integral part of their overall cybersecurity strategy.(40)

5.8.4.4 Specialized ADS Use Cases

There are many specialized use cases associated with ADS features. This subsection considers the cybersecurity needs of a few representative cases, including cooperative perception, teleoperation, platooning, and their testing and validation.

Cooperative Perception: Cooperative perception plays an important role in enhancing the safety and efficiency of mixed fleets, especially in the context of cybersecurity scenarios. It involves the exchange of sensing and perception data between ADS and infrastructure elements, such as control centers and roadway infrastructure, to improve situational awareness and reduce uncertainty. However, while cooperative perception offers substantial benefits, it also introduces potential cybersecurity risks that need careful consideration. As noted above, cybersecurity measures will need to address the cyber vulnerabilities that result from cooperative perception.(41)

One critical concern is the integrity of the shared data, as malicious actors may attempt to compromise it by injecting false information or manipulating sensor inputs, potentially leading to hazardous situations. Additionally, communication links enabling cooperative perception can be vulnerable to interception or tampering, exposing the data to unauthorized access and posing risks such as data leakage or eavesdropping. A 2022 study on cooperative perception and control supported infrastructure-vehicle systems pointed out the importance of requiring high-bandwidth communication without any delay when transmitting sensing data and ensuring the real-time performance and robustness of the perception and control methods.(42) This means the attackers could potentially introduce a noticeable delay or service lag in the network and cause damage to the hardware or software system, interrupt operations and the supply chain, cause personnel harm, or result in property, financial, and reputational loss.

Furthermore, the potential for denial-of-service attacks threatens the functionality of ADS by disrupting cooperative perception, while identity spoofing can allow attackers to impersonate infrastructure elements, giving them access to sensitive cooperative perception data or letting them manipulate traffic information, further exacerbating safety and security hazards.

To mitigate the cybersecurity risks associated with cooperative perception in mixed fleets, general cybersecurity best practices should be followed. Fleet operators and infrastructure providers should prioritize secure communication protocols, employing encryption and strong authentication mechanisms to safeguard data during transmission. Data authentication techniques, including digital signatures, can help verify data integrity and authenticity, preventing tampering or injection attacks. Additionally, deploying IDS to monitor communication channels for anomalies, enforcing access control measures, ensuring redundancy and diversity in data sources, and maintaining secure update procedures are vital steps to fortify cooperative perception security. Comprehensive EAP, cybersecurity training, regular security auditing, and regulatory compliance efforts round out a robust cybersecurity strategy, ensuring that cooperative perception continues to advance fleet safety while mitigating the associated cybersecurity risks.

Teleoperation: Teleoperation, in the context of mixed fleet management and the operation of connected and autonomous vehicles, refers to the remote control and supervision of vehicles by human operators. It is an ADS feature that includes several variants such as remote, collaborative, and fallback driving. All three examples of teleoperation require extensive information sharing and, as such, present significant cybersecurity challenges. In the case of remote driving, vehicle perception is shared with the remote driver, and the remote driver determines the vehicle responses (i.e., two-way communication). Collaborative driving involves sharing of the driving task, or performance of the DDT, between multiple agents and thus potentially requires multiple two-communication channels. Fallback driving occurs when the AV can no longer perform the DDT or when the ADS feature has exited its ODD. As with the previous two examples of teleoperation, fallback driving requires a minimum two-way communication between the vehicle and the fallback driver. All these examples depend critically on channels of communication; as such, teleoperation requires a cybersecurity analysis of the features of the broader system that includes the ADS-equipped CMVs and the teleoperator. Again, general cybersecurity best practices discussed in this report should be followed.

Platooning: "A platoon of connected automated vehicles is defined as a group of connected automated vehicles that exchange information, so that they can drive in a coordinated way, allowing very small spacings, and, still, traveling safely at relatively high speeds."(43) Platooning, or flocking, is an ADS feature involving two or more vehicles that coordinates the performance of the driving task of a platoon. The feature is meant to increase fuel efficiency and equipment utilization via an automated highway system. A connected AV is any ADS-equipped vehicle that communicates with 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.

There are several cybersecurity concerns related to platooning. One is communication tampering, due to the fact that platooning relies heavily on V2V communication. Cyber attackers may attempt to tamper with these communications, altering the information exchanged between platoon vehicles. This can lead to misalignment or collisions within the platoon, compromising safety. Another concern is sensor manipulation; attackers may target the sensors of platoon vehicles, such as lidar, radar, or cameras, to provide false data. This could result in the platoon reacting inappropriately to its surroundings, potentially causing collisions or disrupting traffic flow. Access control breaching is yet another concern, where unauthorized access to the platooning system could lead to a cyber attacker taking control of one or more vehicles within the platoon. This scenario presents significant safety risks, as the attacker may manipulate the vehicles' behavior. The last concern is related to data and privacy leaks, which may include vehicle telemetry and position information or driver and fleet information. Protection of this data is essential to maintain the privacy of the fleet and the drivers. With the progression of automated driving and cooperative driving technology, the cybersecurity level of a platoon will advance simultaneously. However, since attackers can cause greater damage and disruption by gaining control access into a platoon than in a single CMV, higher cybersecurity levels and requirements should be emphasized for platoons.

General cybersecurity best practices should be followed for platooning as well, such as deploying an IDS, developing EAPs, secure communication protocols, secure over-the-air updates, employee cybersecurity training, security auditing, and enforcing access control. To conclude, platooning offers substantial advantages in mixed fleet management, but it also introduces cybersecurity scenarios that must be addressed. By implementing robust security measures, including secure communication, sensor redundancy, and access control, fleet operators can reap the benefits of platooning while minimizing the associated cybersecurity risks and ensuring the safety of their operations.

[1] National Highway Traffic Safety Administration. (2022). Cybersecurity best practices for the safety of modern vehicles. https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf

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

[3] Greenberg, A. (2015, July 21). Hackers remotely kill a Jeep on the highway—with me in it. Wired. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] Tabak, N. (2020, December 28) 5 defining cyberattacks on trucking and logistics in 2020. https://www.freightwaves.com/news/5-defining-cyberattacks-on-trucking-and-logistics-in-2020

[5] Monteagudo, J. (n.d.). Cyber security for connected and autonomous vehicles. Cyber Startup Observatory. https://cyberstartupobservatory.com/cyber-security-connected-autonomous-vehicles/#:~:text=be%20unlimited%2C%20new%20threats%20and,Botnet%20Armies)%20and%20vehicle%20theft

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

[7] U.S. Government Accountability Office. (2021, April 22). SolarWinds cyberattack demands significant Federal and private-sector response (infographic). https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic

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

[9] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

[10] Automotive Information Sharing and Analysis Center. (n.d.). Best practices: Automotive ISAC. https://automotiveisac.com/best-practices/

[11] National Institute of Standards and Technology. (n.d.). Cybersecurity framework. https://www.nist.gov/cyberframework

[12] IBM. (n.d.). What is zero trust? https://www.ibm.com/topics/zero-trust#Take+the+next+step

[13] Cybersecurity Insider. (2022). VPN risk report. https://www.zscaler.com/resources/industry-reports/2022-vpn-risk-report-cybersecurity-insiders.pdf

[14] Cyberark (n.d.). Principle of least privilege. https://www.cyberark.com/what-is/least-privilege/#:~:text=The%20principle%20of%20least%20privilege,perform%20his%2Fher%20job%20functions

[15] National Institute of Standards and Technology. (n.d.). Role-based access control (RBAC). https://csrc.nist.gov/glossary/term/role_based_access_control

[16] Cybersecurity and Infrastructure Security Agency. (2009). Choosing and protecting passwords: Security Tip (ST04-002). https://www.cisa.gov/uscert/ncas/tips/ST04-002

[17] National Highway Traffic Safety Administration, 2022.

[18] National Highway Traffic Safety Administration, 2022.

[19] Hamilton, T. (2023, July 15). Difference between Black Box and White Box testing. Guru99. https://www.guru99.com/back-box-vs-white-box-testing.html

[20] ITconvergence. (n.d.). Risks of using outdated operating system. https://www.itconvergence.com/blog/risks-of-using-outdated-operating-system/#:~:text=Limited%20Security%3A%20Outdated%20operating%20systems,put%20your%20privacy%20at%20risk

[21] U.S. Department of Transportation. (2020). Data for Automated Vehicle Integration (DAVI). https://www.transportation.gov/av/data

[22] IBM. (2021, July 16). Data At Rest Encryption. https://www.ibm.com/docs/en/strategicsm/10.1.3?topic=security-data-rest-encryption

[23] National Institute of Standards and Technology. (2023, May 9). Advanced Encryption Standard (AES). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197-upd1.pdf

[24] Simpson, J. (n.d.). Data masking and encryption are different. IRI Tota Data Management. https://www.iri.com/blog/data-protection/data-masking-and-data-encryption-are-not-the-same-things/

[25] Amazon Web Service. (n.d.). What is anomaly detection? https://aws.amazon.com/what-is/anomaly-detection/

[26] Fortinet. (n.d.). API security standards. https://www.fortinet.com/resources/cyberglossary/api-security#:~:text=Application%20programming%20interface%20(API)%20security,the%20sensitive%20data%20they%20transfer

[27] Google. (n.d.). Encryption in transit. https://cloud.google.com/docs/security/encryption-in-transit#:~:text=Encryption%20in%20transit%20defends%20your,commonly%20provided%20by%20third%20parties

[28] Lord, N. (2023). Data protection: Data in transit vs. data at rest. FORTRA. https://www.digitalguardian.com/blog/data-protection-data-in-transit-vs-data-at-rest#:~:text=For%20protecting%20data%20in%20transit,contents%20of%20data%20in%20transit

[29] Cloudflare. (n.d.). VPN security: How VPNs help secure data and control access. https://www.cloudflare.com/learning/access-management/vpn-security/#:~:text=VPNs%20protect%20data%20as%20users,help%20with%20managing%20user%20access

[30] Juniper Networks. (n.d.). What is IDS and IPS? https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html#:~:text=What%20Can%20You%20Do%20with,reporting%20them%20to%20security%20administrators

[31] Sharif, A. (2022). What is centralized logging? https://www.crowdstrike.com/cybersecurity-101/observability/centralized-logging/

[32] Hodge, C., Hauck, K., Gupta, S., & Bennett, J. (2019). Vehicle cybersecurity threats and mitigation approaches (NREL/TP-5400-74247). National Renewable Energy Laboratory. https://www.nrel.gov/docs/fy19osti/74247.pdf

[33] Kumar, A. D., Chebrolu, K. N. R., & Soman K. P. (2018). A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. arXiv preprint arXiv:1810.04144.

[34] Stachowski, S., Bielawski, R., & Weimerskirch, A. (2019). Cybersecurity research considerations for heavy vehicles. University of Michigan, Ann Arbor, Transportation Research Institute.

[35] National Highway Traffic Safety Administration. (2018, December). Cybersecurity research considerations for heavy vehicles. https://deepblue.lib.umich.edu/bitstream/handle/2027.42/151379/UMTRI-2018-10.pdf

[36] Kumar, A.D., et al. (2018).

[37] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. Vehicular Communications, 23, 100214.

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

[39] HMS Industrial Networks. (n.d.). SAE J1939 - Ixxat. https://www.ixxat.com/technologies/fieldbuses/sae-j1939

[40] The White House. (2021, May 12). Executive order on improving the Nation’s cybersecurity. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[41] Cui, G., Zhang, W., Xiao, Y., Yao, L,, & Fang. Z. (2022). Cooperative perception technology of autonomous driving in the internet of vehicles environment: A review. Sensors, 22(15), 5535. https://doi.org/10.3390/s22155535

[42] Yu, G., Li, H., Wang, Y., Chen, P., & Zhou, B. (2022). A review on cooperative perception and control supported infrastructure-vehicle system. Green Energy and Intelligent Transportation, 1(3), 100023. https://doi.org/10.1016/j.geits.2022.100023

[43] Martínez-Díaz, M., Al Haddad, C., Soriguera, F., & Antoniou, C. (2021). Platooning of connected automated vehicles on freeways: a bird's eye view. Transportation Research Procedia, 58, 479-486. https://doi.org/10.1016/j.trpro.2021.11.064