Vehicle Electronics and Cybersecurity

Current Interactions, Vulnerabilities, and Recommendations

Dec 2023


EUROPEAN
MOBILITY
GROUP


UTAC

Foreword

Computers are everywhere in modern life and the car is no exception. Indeed, the modern car is a set of moving computers and, as with all computers, keeping them safe from outside interference has become a significant task. Vehicle manufacturers now need to be aware of and plan for security at all stages of a vehicle's life, from its planning through the manufacturing process to its end use on the road. As cars increasingly become automated, ensuring that the electronics are safe and cannot be tampered with is an important societal challenge.

At the same time, strengthened cybersecurity for cars poses complex risks for companies in the European Mobility Group that adapt vehicles for people with disabilities. Making the adaptations that customers need increasingly requires interactions with the vehicle's electronics and computer systems. If these systems are inaccessible to adapters, it may no longer be possible for some people, who drive perfectly safely at present, to benefit from new safety technology or even to drive cars at all. It should be expected that new safety technology in vehicles would facilitate driving and would allow more people with disabilities to access private mobility. If this is to happen it is essential that methods are found to ensure the security of the on-board computers without eliminating access to people with disabilities.

EMG has commissioned this report from UTAC to give members and all involved in adaptation a better understanding of what cybersecurity means and what its implications are for adaptation companies. The report shows that a major challenge for adapters and for EMG is to develop closer cooperation with manufacturers so that the risks of excluding people from driving are minimized. This challenge should also be seen as one for manufacturers to that they also ensure that the car of the future will be more and not less accessible.

EMG would like to thank UTAC for this report and in particular the main author Rafael de Sousa Fernandes.

This report describes how cybersecurity is changing the way electronics operate in a car. It is clear that EMG and its members need to follow these changes carefully and to exchange openly their experiences on adaptations. Dialogue with manufacturers, individually and through their representative organizations, will be essential so that the possibilities of increasingly safe and automated cars will become available to everyone.

DR JACK SHORT
President EMG

Table of Contents

I. Introduction

I.1 Background

The automotive industry has undergone a significant transformation over the years, with a notable shift towards advanced vehicle electronics and communication technologies. As modern vehicles become increasingly connected and integrated with electronic systems, concerns about potential vulnerabilities and cyber threats have risen. This paper aims to explore the intricacies of vehicle electronics and shed light on how these systems are protected. It will also delve into the impact of the latest applicable regulations in terms of cybersecurity.

These advances are primarily made possible by intricate E/E (Electrical/Electronic) architectures that facilitate efficient communication among various vehicle components, ECUs (Electronic Control Unit). However, as vehicles become more interconnected and reliant on digital systems, they become susceptible to potential cybersecurity risks and external interference.

Historically, the automotive industry has been focused on physical safety concerns such as crash protection and occupant safety, or more recently, vulnerable road users like pedestrians or cyclists. However, with the growing integration of complex electronics and communication channels, the focus has now expanded to include cybersecurity as a critical aspect of vehicle safety. OEMs (Original Equipment Manufacturers) must be able to ensure the integrity, confidentiality, and availability of vehicle systems.

I.2 Scope and limitations

The primary purpose of this paper is to provide a comprehensive understanding of how vehicle electronics work and the measures implemented to protect them from interference from external entities. It aims to shed light on the main interactions and communication channels prevalent in today's E/E architectures.

Additionally, this paper aims to highlight the significant influence of legislation on automotive cybersecurity. As governments and regulatory bodies recognize the potential risks associated with connected vehicles, they have imposed guidelines and regulations to enhance the overall cybersecurity posture of the automotive industry. Understanding these regulations and their implications is crucial for stakeholders involved in vehicle manufacturing.

This paper will investigate the potential vulnerabilities that could pose cybersecurity risks and the protection mechanisms implemented to mitigate such risks. Moreover, it will delve into the impact of existing legislation related to automotive cybersecurity, considering how these regulations shape the practices and processes of automotive companies.

However, it is essential to acknowledge the limitations of this paper. Due to the ever-evolving nature of technology and regulations, the information presented may be subject to change. The paper will be based on the knowledge available up to this date. Furthermore, the paper will not divulge specific proprietary information or trade secrets of automotive manufacturers or cybersecurity companies. Instead, it will focus on providing a holistic overview of the subject matter to foster a better understanding of vehicle electronics and cybersecurity in the automotive industry.

II. Vehicle Electronics and communication channels

II.1 E/E architectures in today's vehicles

Today's vehicles are equipped with a multitude of ECUs, each responsible for specific functions, such as engine management, safety systems, infotainment, and driver assistance features. The traditional approach of having dedicated ECUs for each function has given way to more sophisticated and interconnected architectures, such as domain-based and zone-based architectures.

Domain-based architectures group ECUs based on the functions they control, like powertrain, chassis, and body electronics. This allows for better integration and communication within each domain, leading to improved performance and efficiency. On the other hand, zone-based architectures cluster ECUs based on specific zones in the vehicle, like the front or rear end. This approach enables better coordination and communication among different domains, enhancing overall vehicle intelligence and responsiveness. These two approaches are well illustrated by the following figure extracted from this article [1].

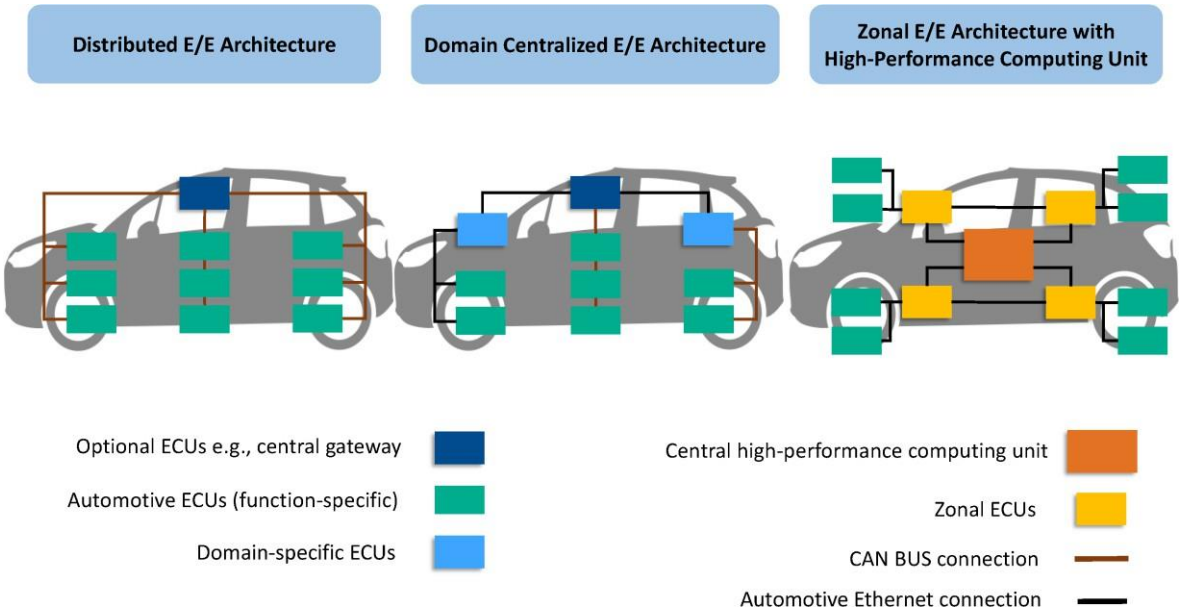


Figure 1: *The figure presents the evolution of vehicle E/E architecture. Distributed E/E architecture was used until 2019, while domain-centralized architecture is today's vehicle architecture. The zonal architecture shows the future car E/E architecture.*

II.2 Communication protocols and interactions

Effective communication among ECUs is critical for seamless coordination and functioning of various vehicle systems. Communication protocols act as the language that allows ECUs to exchange information and commands efficiently. Commonly used protocols include Controller Area Network (CAN – ISO 11898), Local Interconnect Network (LIN - l'ISO 17987), and FlexRay (ISO 17458).

CAN is widely used for in-vehicle communication due to its reliability and robustness. It allows multiple ECUs to communicate over a shared bus, enabling real-time data transmission and control. The buses enable the transfer of data, instructions, and control signals between different hardware components, such as the central processing unit (CPU), memory, storage devices, input/output devices, and peripherals.

LIN, on the other hand, is a simpler and more cost-effective protocol suitable for less critical applications like interior lighting control.

As vehicles become more connected, additional communication protocols have emerged to support high-bandwidth data exchange. Ethernet-based protocols, such as BroadR-Reach and Automotive Ethernet, offer faster communication speeds, making them suitable for advanced driver assistance systems (ADAS) and infotainment applications.

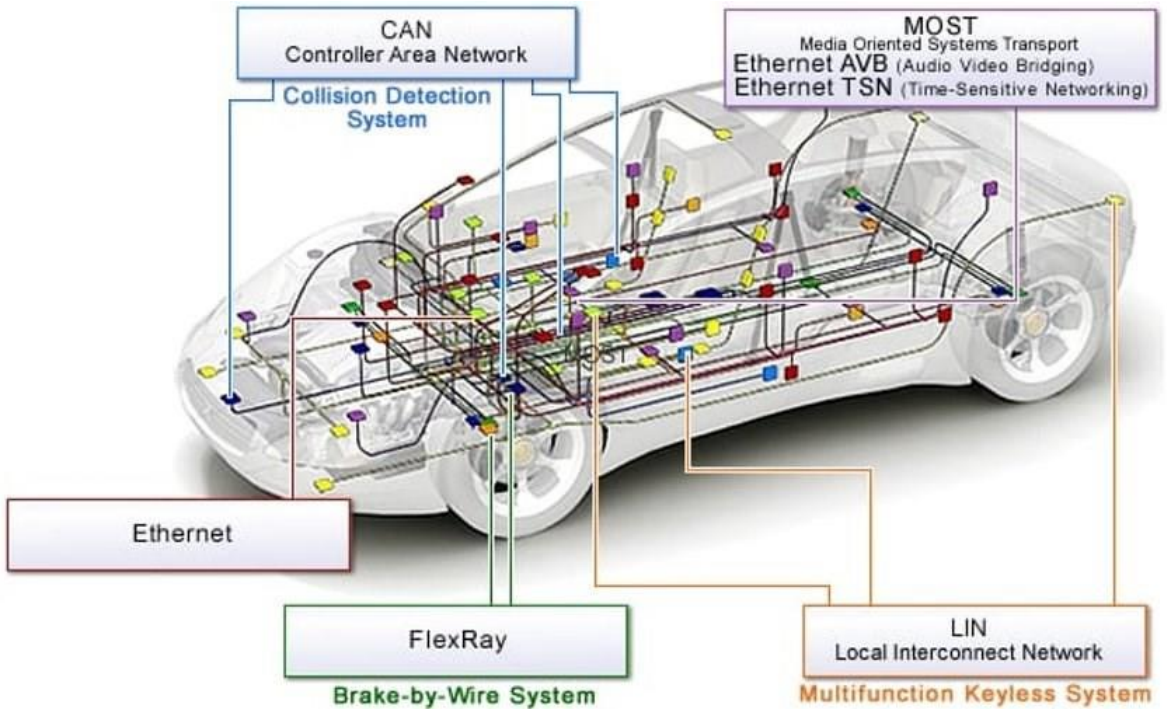


Figure 2: *different communication protocols*

II.3 Vulnerabilities in E/E architectures

While modern E/E architectures provide numerous benefits, they also introduce new vulnerabilities, primarily due to their increased complexity and interconnections. These vulnerabilities can be exploited by malicious actors, leading to potential cybersecurity risks for the vehicle and its occupants.

One common vulnerability is the lack of proper segmentation and isolation between safety-critical and non-safety-critical systems (inside but also outside the car). When the segmentation is not sufficient, and if attackers gain access to a non-critical system, they may find potential pathways to reach critical systems, compromising the vehicle's safety and functionality.

Moreover, the use of standardized communication protocols like CAN makes it easier for attackers to eavesdrop on communications and inject malicious messages into the network. This can lead to unauthorized access, data manipulation, and even remote control of certain vehicle functions (e.g. 2015 or).

Additionally, the increasing reliance on external connectivity, such as Bluetooth, Wi-Fi, and cellular networks, expands the attack surface. Cyber attackers can exploit weaknesses in these communication

channels to gain unauthorized access to the vehicle, compromising sensitive data and control over critical systems.

To address these vulnerabilities, robust cybersecurity measures must be implemented. This includes encryption of communication data, secure authentication mechanisms, intrusion detection systems, and regular software updates to patch known vulnerabilities. Furthermore, incorporating the concept of defense-in-depth can add multiple layers of protection, making it more challenging for attackers to breach the system.

Understanding the intricacies of vehicle electronics and the various communication channels is vital to developing secure and resilient E/E architectures.

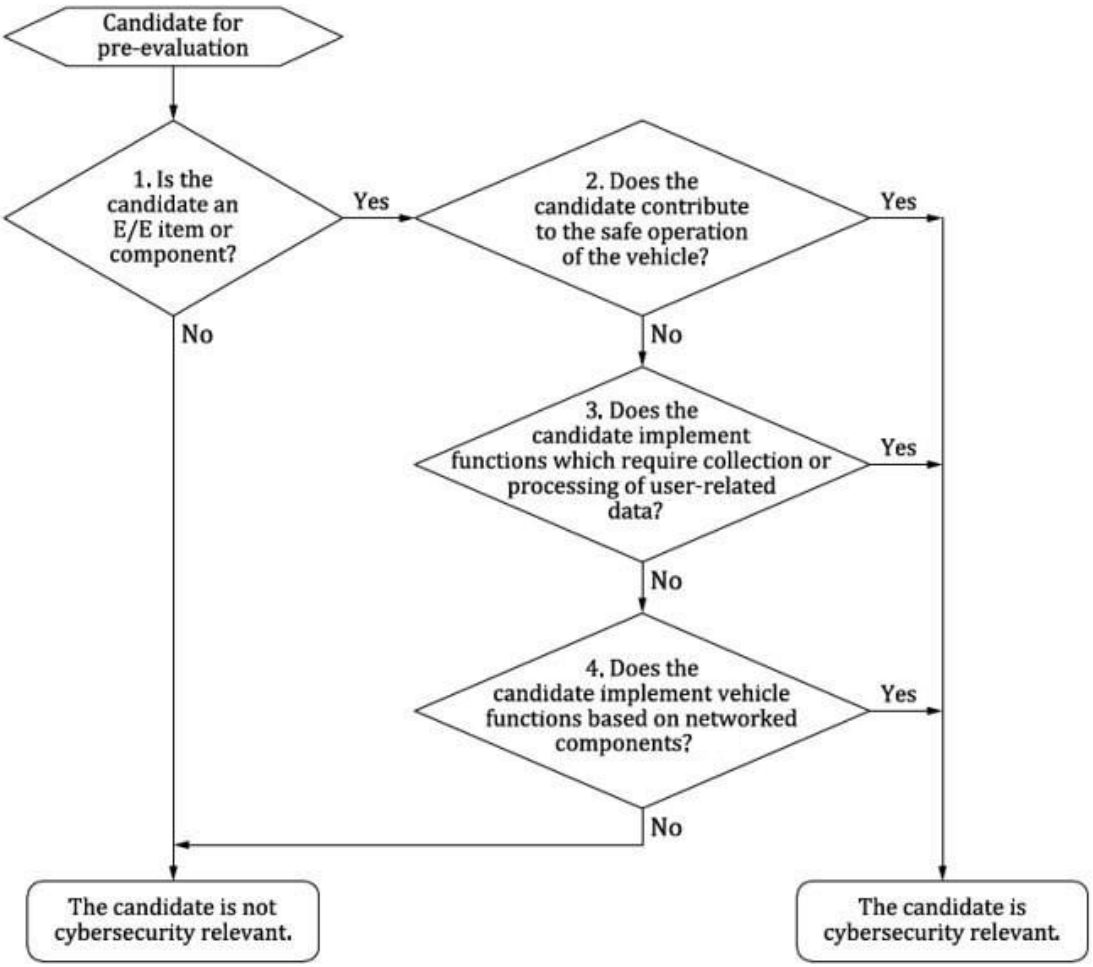


Figure 3: *example of typical reasoning to identify whether there is a cyber impact*

III. Legislation on automotive cybersecurity

III.1 Overview of current regulations

One of the major milestones in Cybersecurity regulation was the publication of the regulation on Cybersecurity and Cybersecurity Management System (UNR155) by the United Nations Economic Commission for Europe (UNECE) and which entered into force on January 22, 2021. This regulation is applicable to M and N category vehicles with regard to cyber security. It also applies to category O vehicles if they are equipped with at least one ECU and vehicles in categories L6 and L7, if equipped with automated driving functions of level 3 or higher.

Furthermore, this regulation became mandatory inside the European Union through the application of the regulation (EU)2019/2144 (GSRII) on "type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users" since the 6th July 2022 for new types of vehicles and will be mandatory for all types of vehicles from the 6th July 2024 on.

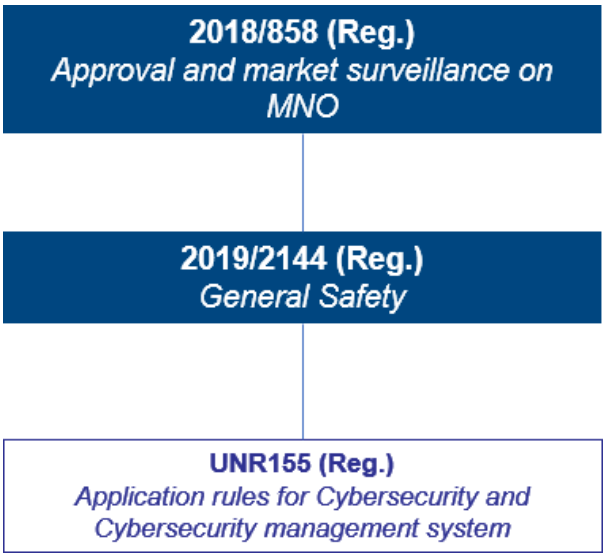


Figure 4: *links between texts in Europe*

This regulation is divided into two mains parts, on the one hand, the Cyber Security Management System (CSMS) requirements and on the other, Vehicle Type requirements are the two key components of the UNR155. The focus of the CSMS requirements is on the processes that the OEM must develop and deploy during the entire lifecycle of the vehicle. The assurance that the OEMs have correctly applied the defined processes is then the main focus of the vehicle type requirements. Definition of roles and responsibilities, security risk management, determining necessary controls, configuration management, vulnerability analysis and incident response, postproduction patch management, and supply chain interaction are among the processes listed as necessary under the UNR155.

By complying with this regulation, the OEM should therefore be able to react to current and evolving cyber threats and vulnerabilities, take every necessary monitoring measure regarding the authorities but also demonstrate that cyber threats and vulnerabilities which require a response from the vehicle manufacturer can be mitigated within a reasonable timeframe.

As for the second-stage manufacturers, they should be aware of the need to communicate with the OEM to ensure that all the due activities related to the CSMS and cyber architecture of the OEM are considered, so that the impact of any modification would be clearly identified without endangering the cyber concept of the vehicle.

Today, in Europe, the approval of multi-stage vehicles is regulated by annex IX of the EU2018/858 which states that the satisfactory operation of the multi-stage type-approval requires joint action by all the manufacturers concerned. To that end, suitable arrangements must exist between the relevant manufacturers for the supply and interchange of documents and information, so that the completed type of vehicle meets the technical requirements of all the relevant regulatory acts.

EU2018/858, Annex IX, §1.2: "Each manufacturer involved in a multi-stage type-approval shall be responsible for the approval and conformity of production of all systems, components or separate technical units manufactured or added by that manufacturer to the previously built stage. The manufacturer of the subsequent stage shall not be responsible for objects that have been approved in an earlier stage, except where that manufacturer modifies relevant parts to such an extent that the previously granted type-approval becomes invalid."

Due to that requirement, ensuring the right cooperation between the second-stage manufacturer and the OEM is key here to avoid any additional issues with the initial approval issued in accordance with the UNR155.

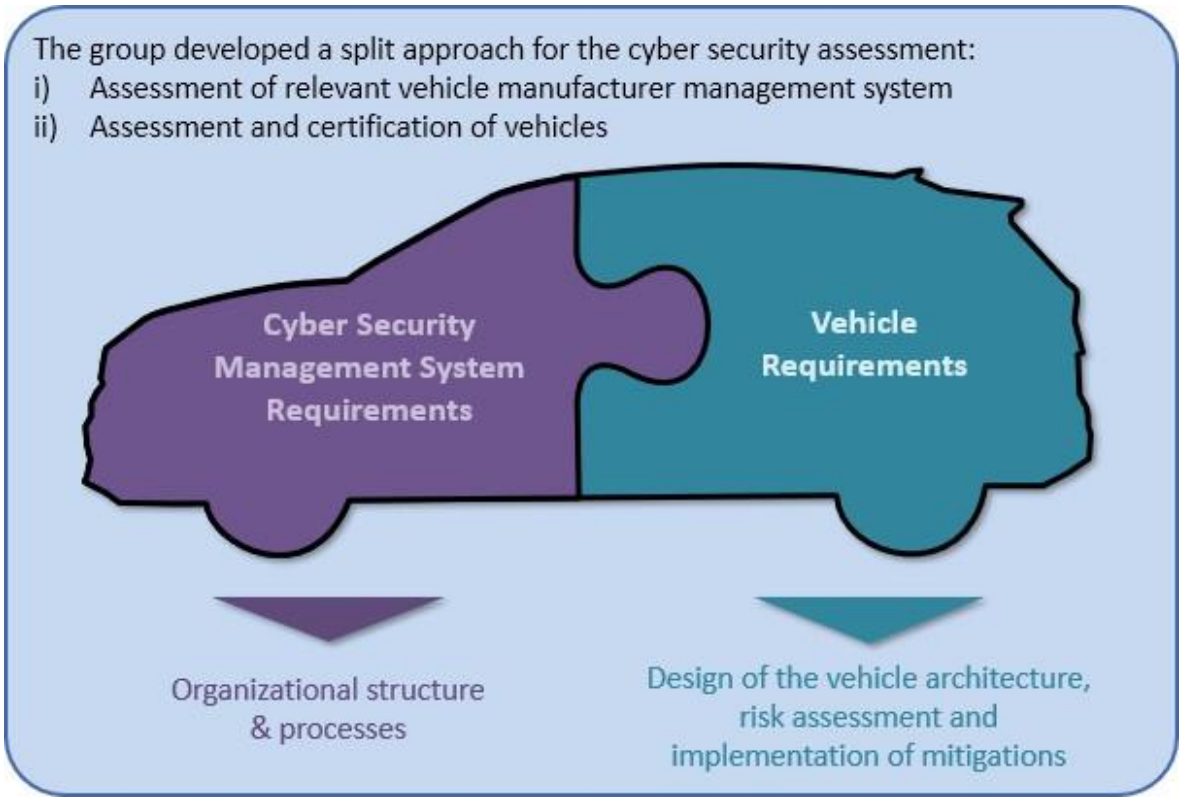


***Figure 5**: UNR155 Structure*

III.2 Impact of cybersecurity legislation on vehicle electronics

The introduction of cybersecurity legislation has significantly influenced vehicle electronics' design, development, and manufacturing processes. Automotive manufacturers and suppliers are now required to incorporate cybersecurity as a fundamental aspect of their entire vehicle development lifecycle; from the development phase to the post-production phase.

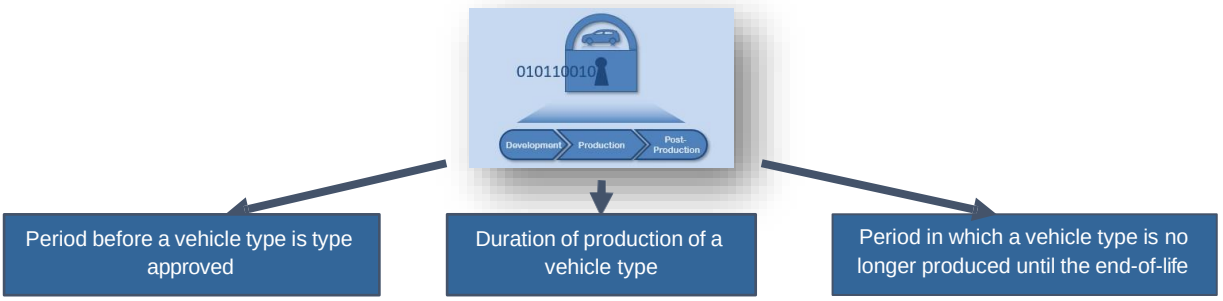


***Figure 6**: Phases of the lifecycle impacted.*

Most of the time, OEMs integrate parts that come from third-party suppliers. These pieces (ICs, ECUs, infotainment systems, particular software, etc.) consist of both hardware and software components. Given this, OEMs rely only on their interactions with supply chain suppliers.

Thus, the OEM must set clear security needs to be then thoroughly presented to the providers before being verified to see if the obtained components actually satisfy the requirements.

Even though we are here talking about a certification process to obtain the CSMS certificate, no prior certification is formally required in order to receive a CSMS certification. However, if the manufacturer is certified to any relevant standard related to cybersecurity management systems, it can only facilitate obtaining of a CSMS certificate.

Relevant standards include, but are not limited to:

– ISO/SAE 21434 Road vehicles – Cybersecurity engineering;

– ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation;

– ISO/IEC 15408 Information technology – Security techniques – Evaluation criteria for IT security;

– ISO/IEC 27000-series;

– ISO 31000-series;

– ISO 9001 – Quality management systems

It is also interesting to note that the legislation has prompted the adoption of over-the-air (OTA) software update capabilities, allowing manufacturers to deploy security patches and software updates remotely, addressing vulnerabilities and enhancing the vehicle's security without requiring physical recalls. The impact here is indirect but still to be considered when determining the right components for the right architecture.

IV. Protection mechanisms

IV.1 Hardware-based security measures

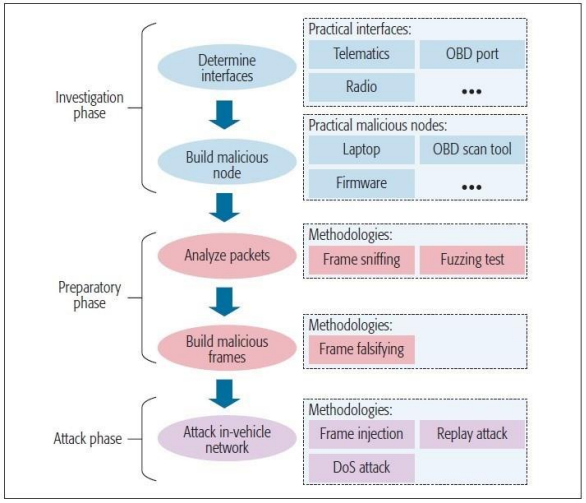
Hardware-based security measures are essential components of safeguarding vehicle electronics from external interference. These mechanisms are designed to provide physical protection and resistance against tampering, unauthorized access, and other potential threats.

Examples of hardware-based security measures in the automotive industry might include:

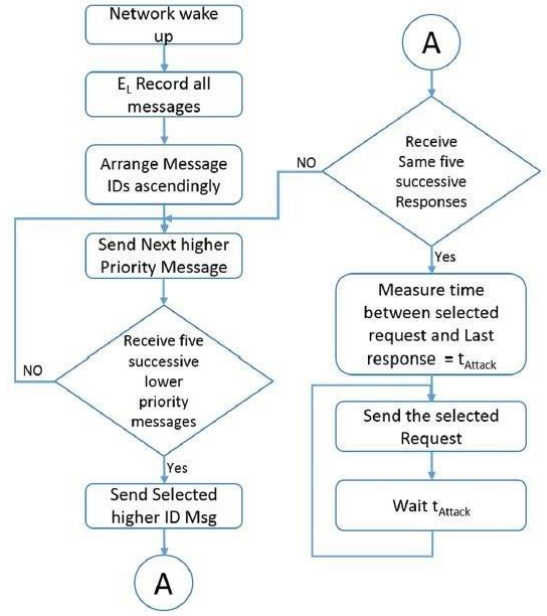
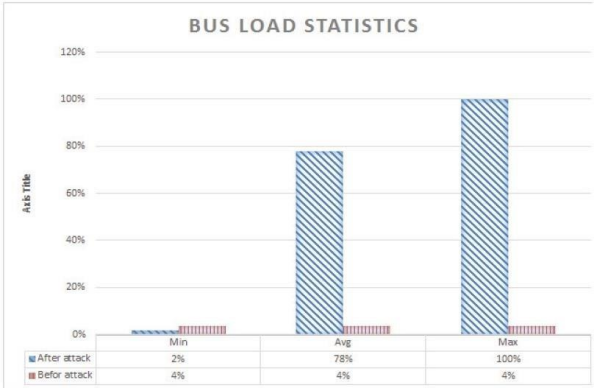
- Secure Boot Process: This mechanism ensures that only trusted and authenticated software is allowed to run on the vehicle's ECUs. During the boot-up process, cryptographic checks are performed to verify the integrity and authenticity of the software before it is executed. This prevents unauthorized or malicious code from being loaded onto the vehicle's ECUs, thereby reducing the risk of unauthorized access or tampering.
- Hardware Encryption: Sensitive data stored in the vehicle's electronic systems, such as cryptographic keys or personal information, can be encrypted using specialized hardware components. This encryption makes it extremely difficult for unauthorized individuals to access or decipher the information, even if they gain physical access to the vehicle's electronics.
- Secure Communication Protocols: Hardware-based security extends to communication channels within the vehicle. Secure protocols with encryption and authentication mechanisms ensure that data exchanged between different ECUs or external devices are protected from eavesdropping and tampering. For instance, the CAN bus, commonly used in vehicles for communication between ECUs, can be fortified with hardware-based security measures to prevent unauthorized manipulation of the data.
- Physically Unclonable Functions (PUFs): PUFs are unique physical properties of hardware components that can be used to generate secure keys or identifiers. They are nearly impossible to replicate, ensuring the authenticity of hardware and establishing secure communication between components.
- Tamper-Resistant Hardware: Certain critical hardware components can be designed with tamper-resistant features. If someone tries to physically access or manipulate these components, they trigger mechanisms that erase sensitive data or render the component inoperable. This deters tampering and protects against physical attacks.

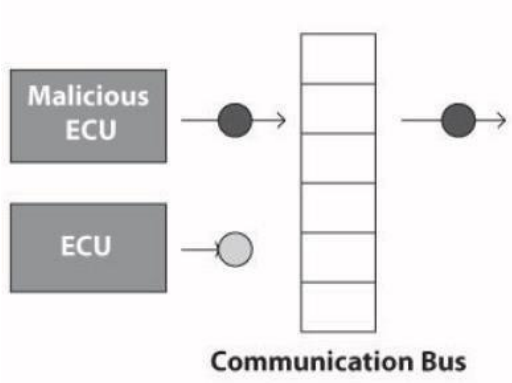
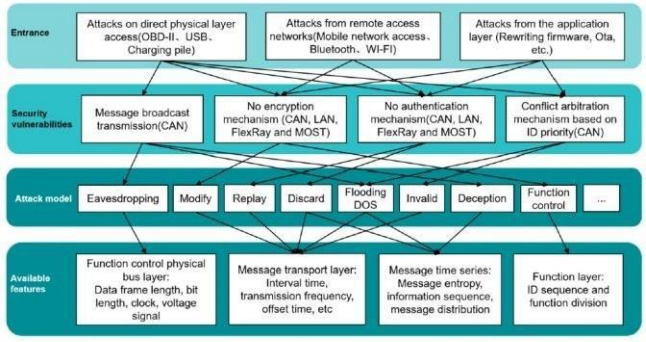
One of the fundamental hardware-based security measures is the use of secure microcontrollers and Trusted Platform Modules (TPMs). These specialized microcontrollers are equipped with built-in security features, such as the ones mentioned above.

Finally, and since these hardware issues should be one of the main concerns of second-stage manufacturers, the next pages of this report outlines examples of vulnerabilities that could affect CAN. It is important to keep in mind that the CAN protocol has several intrinsic vulnerabilities, such as broadcast transmission, no authentication, no encryption, ID-based priority scheme and available interfaces. These vulnerabilities make IVNs vulnerable to malicious attacks. This can occur mainly when any of the component connected to the CAN bus is corrupted and it can send information that the other equipment won’t be able to verify due to this lack of security mechanisms.

Article/Paper	Tar-get	Type of threat	Impact on AV perception	Illustration	Security countermeasures (proposed by the authors)[1]
In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions, 2017 [12]	CAN	- Frame sniffing - Frame falsifying - Frame injection - Replay attack - DoS attack	- Confidential-ity - Integrity (false detection of obstacles, add false ECU) - Availability (undetected objects)		- Enhancing In-Vehicle Network Security by Encryption and Authentication - Separating Potential Attacking Interfaces from In-Vehicle Networks

[1] Based on the sensors models under study (with possibly specific characteristics/performance compared to sensors with similar technology)

Replay Attack on Lightweight CAN Authentication Protocol, 2017 [13]	CAN	- Replay attack	- Integrity (False detection of obstacles)	 	- Enhancing Lightweight Authentication Protocol (LCAP) against the replay attack with a three-stage solution: o Refusing duplicate channel requests o Reconstruct the channel request message in such a way that represents both sender and receiver ECU IDs o Create a challenge-response procedure

In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions, 2015 [14]	CAN	- Control override	- Integrity / availability (change priority of ECU messages, add false ECU)		- Use of Firmware update Over the Air (FOTA) to remove OBD-II port
An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles, 2022 [15]	CAN	- Frame sniffing - Message playback - Camouflage - DOS attack - Sniffing	- Integrity - Confidentiality	 **Figure 3.** Relationship between attack entry, security vulnerability, and exploitable features of intrusion detection in vehicle networks.	Building a more secure vehicle CAN network intrusion detection system through an advanced machine learning algorithm to improve threat detection. Still some research in progress on this subject: Data encryption (e.g., with lightweight AES) Message authentication (e.g., TESLA, MAuth-CAN, one-way hash chain)

<table>
<tr>
<td>S2-CAN: Sufficiently Secure Controller Area Network, 2021 [16]</td>
<td>CAN</td>
<td></td>
<td>- Confidentiality and authenticity</td>
<td>
Table 1: Comparison with related approaches
<table>
<tr><th></th><th>Protection</th><th>Algorithm</th><th>HW/SW</th><th>Bus Load</th><th>Latency</th><th>MAC Length</th><th>Security Level</th></tr>
<tr><td>CaCAN [28]</td><td>Authenticity + Freshness</td><td>SHA256-HMAC</td><td>HW+SW</td><td>+100%</td><td>+2.2-3.2μs</td><td>1 Byte</td><td>2^7</td></tr>
<tr><td>IA-CAN [21]</td><td>Authenticity</td><td>Randomized CAN ID + CMAC</td><td>SW</td><td>+0%</td><td>8bit: +72ms
32bit: +150μs</td><td>1-4 Bytes</td><td>2^7-2^{31}</td></tr>
<tr><td>vatiCAN [33]</td><td>Authenticity + Freshness</td><td>SHA3-HMAC</td><td>SW</td><td>+16.2%</td><td>+3.3ms</td><td>8 Bytes</td><td>2^{63}</td></tr>
<tr><td>TESLA [34]</td><td>Authenticity + Freshness</td><td>PRF+HMAC</td><td>SW</td><td>+0%</td><td>+500ms</td><td>10 Bytes</td><td>2^{79}</td></tr>
<tr><td>LeiA [37]</td><td>Authenticity + Freshness</td><td>MAC</td><td>SW</td><td>+100%</td><td>N/A</td><td>8 Bytes</td><td>2^{63}</td></tr>
<tr><td>CANAuth [41]</td><td>Authenticity + Freshness</td><td>HMAC</td><td>HW+SW</td><td>+0%</td><td>N/A</td><td>10 Bytes</td><td>2^{79}</td></tr>
<tr><td>S2-CAN</td><td>Confidentiality + Authenticity + Freshness</td><td>Circular Shift + Internal ID Match</td><td>SW</td><td>+0%</td><td>+75μs</td><td>N/A</td><td>~ 2^{49}</td></tr>
</table>
</td>
<td>- Enable a trade-off between performance and security</td>
</tr>
</table>

***Figure 7**: Some focus areas examples*

IV.2 Software-based security solutions

Software-based security solutions complement hardware-based measures by providing an additional layer of defense against outside interference. These solutions focus on protecting the vehicle's software and firmware from unauthorized modification, malware, and other cyber threats.

To illustrate this concept, following are some examples of possible measures to put in place:

- Code Signing and Verification: Software-based security solutions can involve digitally signing the software code and firmware used in a vehicle's ECUs. Digital signatures serve as cryptographic markers that confirm the authenticity and integrity of the code. When the software is loaded, the system checks the digital signature to ensure that the code has not been tampered with or altered since it was signed. For instance, if a malicious actor tries to inject unauthorized code into the vehicle's software, the absence of a valid digital signature would prevent the code from executing.
- Intrusion Detection Systems (IDS): Software-based IDS continuously monitor the vehicle's software environment for unusual or suspicious activities. These systems analyze software behavior, network traffic, and other indicators to identify potential cyber threats. For example, if an ECU's software starts behaving abnormally, such as attempting to access unauthorized resources, the IDS can trigger an alert or take preventive actions to mitigate the threat.
- Secure Software Updates: Manufacturers can deliver patches, updates, and new features to vehicles remotely (or not), ensuring that the software remains up-to-date and resistant to known vulnerabilities. These updates can be digitally signed to verify their authenticity before installation.
- Application Whitelisting: This involves allowing only approved and trusted software applications to run on a vehicle's systems while blocking all others. By maintaining a whitelist of authorized software, the vehicle's security is reinforced against unauthorized or potentially malicious applications trying to execute.

Regular code reviews, static analysis, and dynamic testing are essential in identifying and addressing security flaws during the development process.

IV.3 Cryptographic techniques

Cryptographic techniques are a fundamental pillar of protection against outside interference in vehicle electronics. Cryptography involves the use of mathematical algorithms to secure data, communications, and authentication processes.

End-to-end encryption is crucial for securing communications between different vehicle systems and external entities. By encrypting data while in transit, even if intercepted, the information remains unreadable and unintelligible to unauthorized parties.

Public Key Infrastructure (PKI) is another well-known cryptographic technique well known and employed to establish secure communication and trust between different entities within the vehicle ecosystem. The public key can be shared openly and used by other entities to encrypt data before sending it. The private key, on the other hand, remains securely with the key owner and is used to decrypt the received data. This process ensures that only the intended recipient can access the encrypted information. Another scenario could be an ECU that needs to authenticate with the central vehicle management system. The ECU presents its digital certificate (containing its public key) to the management system. The management system uses the PKI infrastructure to verify the authenticity of the certificate, ensuring that the ECU is a trusted and authorized component.

By using digital signatures, manufacturers can verify that the data or software comes from a trusted source and has not been tampered with during transmission.

IV.4 Network segmentation and isolation

By dividing the vehicle's network into separate segments or zones, each with its specific access controls and security policies, the OEM can prevent attackers from going through the entire network at once.

Secure gateways and firewalls are deployed to control traffic flow and filter potentially malicious data packets. This helps prevent unauthorized access and protects sensitive data from being exposed too easily.

Furthermore, network isolation is employed to separate safety-critical systems from non-safety-critical systems. This ensures that even if non-critical systems are compromised, attackers cannot directly access or manipulate safety-critical functions, enhancing the overall resilience of the vehicle's electronics.

In conclusion, a comprehensive approach to protection mechanisms against outside interference is crucial to safeguarding vehicle electronics from potential cyber threats. Hardware-based security measures, software-based security solutions, cryptographic techniques, and network segmentation and isolation collectively form what is known as the main technical aspect of the cybersecurity concept expected from an OEM demanding to be approved regarding the UNR155.

V. Interactions of second stage manufacturers with vehicle electronics

V.1 Overview of second-stage manufacturers' involvement

Having in mind the previous chapter, one can easily start to foresee the difficulties that a second-stage manufacturer might be confronted with.

Second stage manufacturers are customizing vehicles to meet specific market demands, regional requirements, or individual preferences and needs. These companies often modify and/or retrofit vehicles with additional features, accessories, or specialized equipment.

Due to the large scope of possibilities here, the involvement of second stage manufacturers in vehicle electronics can vary depending on the need for modifications. In some cases, they may focus on interior or exterior enhancements, such as custom upholstery or body kits, which have minimal impact on the vehicle's electronic systems. However, in more complex cases, second-stage manufacturers might integrate new electronic components, infotainment systems, or advanced driver assistance features, necessitating deeper interactions with the vehicle's existing electronics.

V.2 Potential cybersecurity risks related to the customization processes

While second-stage manufacturers aim to provide value-added services to customers, their interactions with vehicle electronics can introduce potential cybersecurity risks. Integration of aftermarket electronic components or systems might, without realizing it, compromise the vehicle's cybersecurity concept.

Second-stage manufacturers may not have access to the original vehicle manufacturer's cybersecurity guidelines or might not have the necessary resources to fully have the necessary vision on the implications of integrating non-OEM electronic components into the existing E/E architecture. As a result, they might overlook potential vulnerabilities, and expose the vehicle to cyber threats.

As previously said the lack of access to original cybersecurity guidelines and the potential oversight of vulnerabilities can lead to unforeseen risks. To address these challenges, collaboration between original vehicle manufacturers, second-stage manufacturers, and cybersecurity experts becomes essential. This collaboration can help establish clear guidelines, provide necessary resources, and ensure that modified vehicles maintain a robust cybersecurity concept while still meeting the needs of their users.

Additionally, second-stage manufacturers might source electronic components or software from third-party suppliers, whose products may not meet the same level of security standards as those employed by original vehicle manufacturers. This opens the door to potential supply chain attacks and the introduction of compromised or malicious components into the vehicle's systems. However, it is once again something that can be coped with by collaborating with the OEM and expecting those third-party suppliers to meet relevant requirements (e.g., ISO 21434)

That being said, the involvement of second-stage manufacturers with vehicle electronics raises challenges in complying with current automotive cybersecurity regulations. While OEMs invest heavily in ensuring their vehicles meet regulatory requirements, second-stage manufacturers will most likely not be able to put the same effort into doing so.

Moreover, second-stage manufacturers may even face difficulties in acquiring access to software updates and security patches from OEMs. This can impede their ability to keep the modified vehicles up to date with the latest cybersecurity enhancements, leaving the vehicles susceptible to known vulnerabilities.

For that reason, and considering the elements that were previously presented, you will find below the three main articulations that can be figured out from the current ongoing regulatory discussions and several activities that would be needed to facilitate the work of the second-stage manufacturers.

V.3 Recommendations for Second-stage manufacturers

V.3.1 Collaboration with OEMs and Cybersecurity Experts

As mentioned earlier, the second-stage manufacturer will need to Create a collaborative partnership between them and the OEMs. This partnership could involve formal agreements or collaborations where OEMs provide necessary software updates, security patches, and relevant cybersecurity guidelines to the second-stage manufacturers through, for example, a dedicated portal or platform where authorized second-stage manufacturers can download the necessary elements. This partnership should emphasize the importance of maintaining the cybersecurity integrity of modified vehicles. To do so, both parties might try to facilitate the sharing of cybersecurity-related information. This could include sharing information about potential vulnerabilities, emerging threats, and recommended cybersecurity practices to mitigate those upcoming vulnerabilities.

But since the effort should go both ways, the second-stage manufacturer should also try to leverage third-party cybersecurity experts to conduct assessments and audits of modified vehicles. These experts can identify vulnerabilities, recommend solutions, and ensure that modifications align with cybersecurity best practices.

Some certifications might also help to grow OEM’s trust; ISO 21434, ISO 24089, ISO 9001, ISO 27001 etc. Continuous training and awareness programs for employees are crucial to ensuring a cybersecurity-aware culture within the company. This, for instance, includes providing cybersecurity training for engineers, technicians, and other personnel involved in the modification processes. Employees should be made aware of emerging cybersecurity threats and the potential risks associated with certain modifications.

V.3.2 Compliance with evolving regulations

By staying ahead of regulatory changes, second-stage manufacturers can demonstrate their commitment to cybersecurity and position themselves as trusted partners in the automotive industry.

In conclusion, second-stage manufacturers' interactions with vehicle electronics bring both opportunities and challenges. And even though the regulation does not give clear guidance for the second-stage manufacturers, they should take into account and be aware of the upcoming regulations in a way that allows them to anticipate the discussions they will have to engage with the OEMs, the technical services and also the type of approval authorities.

Given the additional time to comply with the regulation that has allowed the Commission for Special Purpose Vehicles (SPV), second-stage manufacturers should initiate those discussions as soon as possible and especially with type approval authorities.

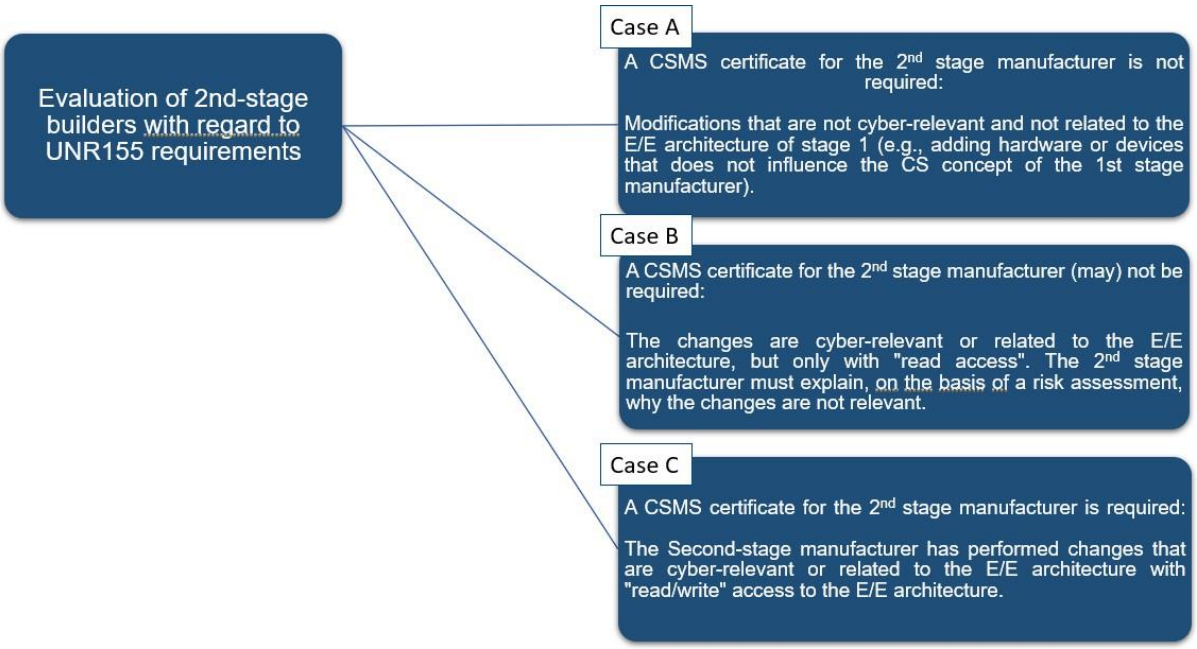


***Figure 8**: Expected compliance for second stage manufacturers with regard to UNR155 requirements*

This diagram shows three cases:

- Case A: A CSMS certificate is not required if the 2nd-stage manufacturer has only made changes that are not cyber-relevant and not related to the E/E architecture of the OEM (e.g., adding hardware or devices that do not influence the CS concept of the OEM).
- Case B: A CSMS certificate may not be required if the 2nd-stage manufacturer has made changes that are cyber-relevant or related to the E/E architecture, but only with "read access". The 2nd stage manufacturer must explain, on the basis of a risk assessment, why the changes are not relevant regarding the cybersecurity of the overall vehicle.
- Case C: A CSMS certificate is required if the 2nd-stage manufacturer has made changes that are cyber-relevant or related to the E/E architecture with "read/write" access to the E/E architecture.

For example, if the 2nd-stage manufacturer has only the ability to read from, but not write to, the E/E architecture; this type of access is less risky than read/write access, as it does not allow the 2nd-stage manufacturer to make changes to the system that could potentially compromise its security. However, it is important to note that even this limited access can pose a security risk. For instance, if the 2nd-stage manufacturer is able to read sensitive data from the system, they could re-use that information.

Therefore, it is important for the 2nd-stage manufacturer to conduct a risk assessment to determine whether or not the changes they have made are relevant to cybersecurity. If the risk assessment shows that the changes are not relevant, then the 2nd-stage manufacturer may not be required to obtain a CSMS certificate.

Here are some examples of changes that might fall into this case B:

- Adding a new sensor that sends data to an existing control unit,
- Changes made to fix a bug,
- Adding a new display to the vehicle.

It is important to note that this is not an exhaustive list, and there may be other types of changes that fall into this category. If you are willing to unsure whether or not a particular change requires a CSMS certificate, it is recommended to contact the relevant type-approval authority and/or associated technical service.

It is important to note that this diagram is a simplified overview of the UNR155 requirements. There are other factors that may affect whether or not a 2nd-stage manufacturer needs to obtain a CSMS certificate, such as the specific nature of the changes they have made and the overall security of the system.

VI. Conclusion

As vehicles become more connected, automated, and technologically advanced, the importance of cybersecurity will only continue to grow.

The emergence of new and sophisticated cybersecurity threats will necessitate continuous advancements in protection mechanisms. Hardware-based security measures, software-based solutions, and cryptographic techniques will need to evolve to stay ahead of potential attackers. Additionally, network segmentation and isolation will play an increasingly critical role in securing the complex and interconnected networks of modern vehicles.

For second-stage manufacturers, the implications are clear – cybersecurity must become an integral part of their modification processes. Collaboration with OEMs and cybersecurity experts will be essential in acquiring the necessary knowledge and resources to comply with evolving regulations. By prioritizing robust cybersecurity measures, fostering a cybersecurity-aware workforce, and staying informed about regulatory changes, second-stage manufacturers can thrive in the future automotive landscape.

In conclusion, the future of vehicle electronics and cybersecurity is intertwined with advances in technology, changes in regulations, and the collective efforts of stakeholders within the automotive industry. By addressing emerging threats, adopting best practices, and embracing cybersecurity as a priority, the industry could reasonably look forward to a future of safe and secure mobility for all.

VII. References

1) Askaripoor, H.; Hashemi Farzaneh, M.; Knoll, A. E/E Architecture Synthesis: Challenges and Technologies. Electronics 2022, 11, 518. https://doi.org/10.3390/electronics11040518
2) ISO 11898-1:2015 Road vehicles — Controller area network (CAN)
3) ISO 17987-1:2016 Road vehicles — Local Interconnect Network (LIN)
4) ISO 17458-1:2013, Road vehicles -- FlexRay communications system, International Organization for Standardization
5) BroadR-Reach Physical Layer Transceiver Specification For Automotive, May 7th 2014:
6) Siemens : https://www.plm.automation.siemens.com/global/fr/our-story/glossary/what-is-automotive-ethernet/109722
7) Election Security Spotlight – Defense in Depth (DiD): https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did
8) Society of Automotive Engineers (SAE). (2021). J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.
9) UNECE. Regulation No. 155 - Cyber Security and Cyber Security Management Systems
10) ISO/SAE 21434:2020. Road vehicles — Cybersecurity engineering.
11) ENISA, “Good Practices For Security Of Smart Cars,” 2019.
12) Jiajia Liu, “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions,” *IEEE Network*, pp. 50-58, September/October 2017.
13) P. Noureldeen, M. A. Azer, A. Refaat and M. Alam, “Replay attack on lightweight CAN authentication protocol,” *12th International Conference on Computer Engineering and Systems (ICCES)*, 2017.
14) Paul Carsten, “In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions,” *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, 2015.
15) Tian Guan, “An Overview of Vehicular Cybersecurity for Intelligent,” *Sustainability 2022*, 2022.
16) Mert D. Pesé, “S2-CAN: Sufficiently Secure Controller Area Network,” *The University of Michigan, ACSAC ’21, December 6–10, 2021, Virtual Event, USA*, 2021.

Disclaimer:

This report, titled "Vehicle Electronics and Cybersecurity: Current Interactions, Vulnerabilities, and Recommendations", has been prepared for informational purposes only. The contents of this report are intended to provide an overview of the current state of cybersecurity regulations applicable in the automotive sector as of the knowledge cutoff date in September 2023.

Readers are strongly advised to verify and update the information contained in this report to ensure compliance with the most recent cybersecurity regulations and legal requirements.