A Holistic Approach on Automotive Cybersecurity for Suppliers

Jose Ángel Gumiel Quintana
Electronics and Communications Unit
Fundación Tekniker
Eibar, Spain
e-mail: jagumiel@tekniker.es

Jon Mabe Álvarez
Electronics and Communications Unit
Fundación Tekniker
Eibar, Spain
e-mail: jmabe@tekniker.es

Jaime Jiménez Verde
Electronic Technology Department
University of the Basque Country (UPV/EHU)
Bilbao, Spain
e-mail: jaime.jimenez@ehu.eus

Jon Barruetabeña Pujana
Mechatronics Area
BATZ Group
Igorre, Spain
e-mail: jbarruetabena@batz.es

***Abstract*— Electronics are increasingly present in automobiles. This has led to a change and automotive parts suppliers are forced to integrate electronic components into their mechanical parts. As if this were not enough of a change, the transition to electronics brings with it other issues, such as cybersecurity. Vehicles are becoming increasingly technological and connected, and car manufacturers are already asking suppliers to ensure cybersecurity. For a traditional supplier, this is something new, and what they often ignore is that it affects not just the product, but the whole organization. Therefore, the purpose of this article is to shine a spotlight on cybersecurity and explain simply, but honestly, the new challenges they face. The automotive industry is a sector that has been able to reinvent itself throughout its history, and in these times of abrupt and accelerated change, it must do so again.**

Keywords - Automotive Engineering; Cybersecurity; Information Technologies; Connected Vehicle.

I. INTRODUCTION

Automobiles have already become computers on wheels. 90% of the technological innovation in vehicles is electronic [1], and the number of electronic elements in cars is predicted to continue to grow [2]. Currently, electronics account for 30% of the total cost of a vehicle, and are expected to account for 50% by 2030 [3].

This is a major disruption. The trend towards the introduction of electronics, software and smart elements is a great opportunity for technology companies, from giants to start-ups, as it allows them to enter a new market [4][5]. On the other hand, it is a threat to traditional suppliers, so-called TIER 1 suppliers, who are forced to renew themselves [4] or be relegated to commodity manufacturers, products with very low cost and little added value.

Many of these well-established suppliers are already aware of this situation and have begun to take steps to integrate electronics into their products [6]. They have some advantages over their new competitors in that they are experts in the design and manufacture of mechanical parts in a variety of materials, they have a good understanding of how the industry works, the timelines and processes for mass-producing parts and delivering them on time, and what is more, they have the prior confidence of the automobile manufacturers, also known as Original Equipment Manufacturers (OEMs).

The integration of hardware (HW) and software (SW) in mechatronic components is not a trivial matter, as it requires knowledge of electronic design and SW development, which is precisely what these companies often lack [7]. In addition, there are a number of well-established regulations that must be complied with [8], as well as new ones that are emerging due to the prevailing needs, such as cybersecurity [9].

Automotive electronic systems are connected to different communication buses and share data with each other, they are not isolated [10][11]. This brings new challenges, as secure communication must be ensured and data must not be compromised [12]. But security goes much further; it starts in the corporation, goes through the design and development of the system, passes through manufacturing, and reaches the vehicle, where it must be robust so as not to endanger other elements, and invulnerable to the passage of time and new technologies.

The purpose of this article is to show that security is a very broad issue, encompassing the whole organization and not just the system developers, and must be ensured throughout the vehicle´s lifetime. Section II explores the differences between safety and security, with particular emphasis on the role of ISO standards in improving both aspects of automotive systems. Section III delves deeper into the topic of cybersecurity, examining its impact on every stage of the automotive product lifecycle, from the office to the end of the vehicle's life. This section is divided into six subsections that examine specific areas of the

 ISBN: ISBNFILL

automotive ecosystem, identifying vulnerabilities and suggesting protective measures. In Section IV, the consequences of potential cybersecurity threats involving outdated vehicles is discussed, examining some vulnerabilities and highlighting the importance of collaboration between OEMs and suppliers. Finally, Section V presents the conclusions of the research and outlines potential areas for future work on the topic.

II. SAFETY & SECURITY

Safety and security are two distinct, but closely related concepts [13]. While safety focuses on preventing accidents, injuries or fatalities through the design and operation of the vehicle, security aims to protect the vehicle and its occupants from unauthorized access, theft, or malicious attack. It cannot be ignored that a security breach could also have an impact on the functional safety of the vehicle, putting occupants and other road users at risk. Several standards have emerged to address the growing concern for vehicle safety and security. One is ISO 26262, which came out in 2011. This is about functional safety. In a nutshell, the standard helps to classify the electronic system according to the severity, exposure, and repeatability of its risks, and urges to take different measures, depending on the category of the system, to make it safe. The standard applies to the entire project lifecycle and includes activities and deliverables for documentation and traceability. In 2018 the second version of this standard was released, and already anticipated the security issue, including common methods for functional safety and cybersecurity [14] to ensure the protection of vehicles from malicious attackers. This already hinted at the concern for cybersecurity, and the close relationship it has with functional safety despite being different areas. Both are collaborative elements that require comprehensive system engineering [11].

On the other hand, and more recently, ISO/SAE 21434, which deals with cybersecurity, appeared in 2021. Analyzing the standard, it resembles a compendium of best practices, because cybersecurity is not something generic; each protocol, each electronic system and each SW module may require a different approach.

Unlike other standards, such as ISO 16750, where the tests to be performed and the pass ranges are detailed, these are not defined. A study must be conducted to analyze the system, and tests to validate and verify the operation of the system must be previously defined, both for functional safety and cybersecurity.

III. FOCUS ON CYBERSECURITY

Security refers to protecting critical system assets from threats and mitigating their impact on the system [11]. These assets can be anything of value, either to the company or to the final product. If vulnerabilities exist, they can be exploited by malicious users or attackers.

There has been a gradual process of digitization in companies [15]. For example, customer communications are often on-line, information generated is stored digitally in repositories and databases, and production control can be done remotely. At the same time, in-vehicle communications have evolved [16], users demand wireless connectivity for their devices and OEMs can remotely update their vehicles' SW. All this makes it clear that cybersecurity must cover the entire lifecycle of an automotive component, from the concept phase to the end of the vehicles' life.

Although it may appear to be a topic that has already been addressed at the academic level, it has been observed that TIER 1s are unaware of the implications and costs to their business of implementing the concept of cybersecurity [17]. In some cases, lack of knowledge and prejudice lead them to believe that it is something trivial and easy to implement. In addition, it has been observed that some OEMs have the same lack of knowledge and ask for fuzzy requirements in their Request for Quotation (RFQ), which can be very vague cybersecurity specifications [18] or exaggeratedly high for the type of product. To illustrate how cybersecurity encompasses not only the product, but the entire organization, development processes, and the entire product lifecycle, the following is a breakdown of the areas in which security must be ensured in an automotive company.

A. Cyb-Sec at the Office

Cybersecurity is a culture. Employees must be educated on the subject and embrace the fact that security starts with them. In the automotive industry, sensitive customer data is at stake [19]. Competition is fierce, and OEMs try to differentiate themselves from each other in terms of design, quality, and innovation. Therefore, confidentiality must be ensured, and a secure working environment must be in place.

It is not uncommon for companies in this sector to have access control at the entrance to their facilities. These systems allow access only to authorized personnel and keep a record of entry and exit times.

In the office, the Information and Communication Technology (ICT) department must ensure the security of the network infrastructure. Part of their job is to implement preventive measures to avoid unauthorized access, modification, deletion and theft of resources and data, including industrial espionage [20]. These security measures may include authentication, access control, application security, firewalls, Virtual Private Networks (VPNs), behavioral analysis, Intrusion Detection and Prevention Systems (IDPS) and wireless security.

The international standard ISO 27001 addresses this issue. It ensures the confidentiality and integrity of data and information, as well as of the systems that process them, allowing the organization to assess the risks and implement the necessary controls to mitigate or eliminate them. This may be combined with periodic internal audits.

 ISBN: ISBNFILL

There are some best practices that can help secure communications.

- **Network segmentation:** This is an effective way to prevent potential intruder exploits from spreading to other parts of the internal network. It is possible to create different subnetworks; some typical examples are a subnetwork for employees and another one for visitors and external devices (such as personal laptops or smartphones) or subnetworks for different workgroups in the organization [21].
- **Firewall:** It is a network security system that monitors and controls incoming and outgoing network traffic. It allows to establish a barrier between a trusted network and an untrusted network. By applying rules, a firewall can allow or deny incoming and outgoing traffic from different IP addresses, protocols and ports [21].
- **Demilitarized Zone:** Creating a demilitarized zone (DMZ) can also be a good idea. This is a subnetwork that lies between the public Internet and private networks. It allows the enterprise to access untrusted networks, while ensuring the security of its private Local Area Network (LAN). Services are exposed, but the middle layer protects sensitive data on the intranet with a firewall that filters traffic [22].
- **Network devices protection:** A primary way to improve network infrastructure security is to harden devices such as routers, access points, servers, etc. Measures can include restricting physical access and, in some cases, protecting them from threats such as fire or water. In the digital realm, secure user access should be ensured, strong administration passwords should be used, device configurations should be backed up and devices should be tested regularly.
- **Access to information:** The organization must provide a secure way to store and access information. There are confidential projects that contain data that should not be accessible to all employees [20]. An information system based on user permissions could prevent read and write access to sensitive documentation. Similarly, the use of version control systems, such as Git or SVN, can increase productivity while maintaining confidentiality.
- **VPN:** This is often the preferred solution to allow remote workers to establish a secure connection to the corporate network. It creates a secure tunnel between the remote worker's computer and the corporate network [23]. It can be used both for accessing company resources remotely as well as for protection when using public connections, as the traffic is encrypted [24]. The main security problem is if an intruder gains access to the virtual network. The knowledge of authentication protocols helps to solve this problem. Today, it is even possible to introduce a double authentication factor by receiving a unique and temporary key on the mobile phone to verify the authenticity of the person who wants to connect, thus rejecting imposters.
- **Updated software:** Keeping SW up to date is important. Developers work hard to maintain compatibility and fix bugs and security vulnerabilities.

Despite the efforts of the ICT department to secure the work environment, this is pointless if employees are not aware of the importance of cybersecurity. There are actions that are solely up to them, such as using strong passwords and renewing them regularly, being suspicious of emails containing hyperlinks or suspicious files or managing documents with appropriate backups, among others.

B. Cyb-Sec in the Development Phase

Automakers are already starting to hold TIER 1 suppliers accountable for cybersecurity. Although this is new, it will soon become a common requirement due to the integration of electronic systems in the car and connectivity. Therefore, HW, and SW engineers will have to develop the project with the concept of cybersecurity in mind.

The way of ISO/SAE 21434's breaks down development is similar to the functional safety standard in that there is still a concept phase and a product development phase. It also adds a section on operations and maintenance during the post-development phase, indicating that there may be incidents, corrections, and updates. Unlike ISO 26262, the cybersecurity standard does not distinguish between HW and SW but is understood as a system. The following are some of the tasks that must be performed when developing a new product.

1) Concept definition

This part details the requirements for the concept phase. Its main objectives are:

1. **Define the item, the operational environment, and its interaction with other items:**
   This is an initial activity in which a preliminary study and design of the architecture is carried out according to the description of the item, an analysis of the known interactions with other components and some assumptions about its operating environment.
2. **Specify cybersecurity goals and cybersecurity claims:**
   Next, an analysis of the item is conducted. Cybersecurity engineers must perform a Threat Analysis and Risk Assessment (TARA). This consists of a matrix to identify potential threats and their likely attack vector, classify them according to their characteristics and their impact on security, operational, privacy and financial issues, and obtain an impact level. It also evaluates the knowledge required by the attacker to execute the identified attack. Ultimately, the aim of this document is to define cybersecurity goals to make a system robust and reliable against hackers and intruders. For those familiar with ISO 26262, this will remind them of the

 ISBN: ISBNFILL

Hazard Analysis and Risk Assessment (HARA) document.

While a threat analysis focuses on how an attacker might exploit vulnerabilities to gain access to resources or sensitive data, threat modelling tries to identify potential threats to the item's ecosystem and its periphery, as well as any vulnerabilities that could be exploited by those threats. Performing this work is also encouraged.

3. **Specify cybersecurity requirements and allocate them to the item or to the operational environment:**

   Based on the above activities and once the threats and cybersecurity goals have been identified, the next step is to establish requirements to meet those targets. That is, what measures will be taken to mitigate the risks and protect the asset against potential attacks.

2) Product Development

During this phase, the cybersecurity specifications must be defined. For this purpose, the HW and SW architectures of the system must also be described, although these may be modified to meet the security goals.

At the HW level, details are needed such as the communication protocol that the component will use to connect to the vehicle or the role of the item. This is important because a point-to-point communication protocol does not have the same security measures as a multiplexed or wireless protocol. The same is true for the role; the measures change if the item is a master or a slave, as well as if it is only responding to requests or sending commands to other systems.

There are also HW components, such as the Trusted Platform Module (TPM) that ensure the authenticity of the device or that the component's firmware has not been tampered with by a third party. This enables SW integrity reporting and cryptographic key creation and management. The applications are varied, but it is used to have a secure identification between the ECU and the component, as well as to identify against the deployment of updates to the system. For example, if an attacker modifies the firmware, the key will change, and the component will no longer be recognized by the vehicle as a trusted system.

Implementing cybersecurity in SW can be done in several ways. e.g., SW design patterns such as modularity, abstraction or layering contribute to system robustness. Similarly, domain separation and process isolation are two measures that limit privilege escalation and access to certain data and resources, making it more difficult for an attacker to gain control of the system. Simplicity and minimization also play a critical role; the easier it is to use and communicate, the easier it is to detect vulnerabilities, and if the system has only the necessary features, without extras, it will be less vulnerable because fewer violations will go undetected.

When the electronic design is mainly based on sensor integration, it is also necessary to ensure that the sensors can be calibrated and that the EEPROM can be locked so that it cannot be tampered with. The same applies to other procurement elements.

3) Cybersecurity Validation

This is the process that validates through testing the assumptions that were made in the previous stages [11]. These tests consist of emulating or simulating cyberattacks and testing the effectiveness of the security measures implemented, thus validating their functioning.

To validate the design there are several types of tests. Some of them will be mentioned and briefly explained below.

- **Penetration test:** Evaluates an application's attack surface for potential SW weaknesses that, if left unaddressed, could lead to exploitable vulnerabilities. This could result in remote code exploitation or sensitive information exposure. The way is to take over the device or application. It is usually combined with a vulnerability scan of the perimeter, where the system is located.
- **Vulnerability scan:** It is a SW that detects certain vulnerabilities in a device, such as well-known public vulnerabilities and configuration errors that pose a high risk of compromise within a network or system. For example: Remote Code Execution (RCE), Data Exposure, Denial of Service (DoS) vulnerabilities, etc.
- **Security scan:** Checks for misconfiguration, such as unencrypted files, unpatched systems, inadequate firewall or use of weak cryptographic methods or suites.

There is another type of analysis that requires knowledge of the communication protocol used by the device. In this way, it is necessary to check that the communication cannot be interrupted, that the identity of the device or sensor cannot be impersonated and that there is no repudiation by other systems. For certain applications, it must also be ensured that the data is protected against attacks (such as man-in-the-middle, eavesdropping or spoofing) or that data cannot be manipulated [11].

4) Product Maintenance

Over time, new technologies and tools emerge, hackers acquire new knowledge and discover new vulnerabilities, and systems that were once secure can become susceptible to attacks.

Connectivity has enabled cars with Over-The-Air (OTA) updates, which not only improve the performance and functionality of a vehicle already on the road, but also make it possible to fix bugs and security breaches on the fly.

When a security vulnerability or bug is discovered in the SW, it should be fixed and securely, quickly, and seamlessly updated without the need to visit the vehicle maintenance shop or garage [11]. The supplier must now ensure that its part is secure and respond to any incidents. The upside is that, although they have an additional role in maintaining safety and security, in some cases they may be able to avoid

 ISBN: ISBNFILL

a recall, because there are issues that could be resolved remotely with a SW update to the component.

Therefore, a secure online SW update is required for every ECU in the autonomous and connected vehicles [11].

C. Cyb-Sec at the Testing Department

Automotive suppliers' typically have departments or laboratories dedicated to testing and measuring parts, whether they are prototypes, pre-series, or final products. Physical security measures are in place to protect know-how and intellectual property. In most cases, the site is protected by walls that prevent visibility from the outside, as well as having access control so that only certain people within the organization are allowed to enter.

However, not all security is physical, but the know-how of the ICT department is also relevant here. Because of the information handled in these facilities, some security measures are taken into consideration. For example, the organization may provide operators with digital cameras, so that they do not use their connected smartphones to take pictures nor videos of the products or tests. This department may be under a different subnetwork to further control communications with the outside world [21]. When storing sensitive test and prototype information, it is essential to have a system for managing backups, which can be stored and encrypted.

Protecting this information is important. An attacker could use it for a variety of purposes, such as industrial espionage, plagiarism, dissemination of results or defamation. On the other hand, backups are also important because in some cases there is information that may be requested by the OEM to solve problems or improve parts.

D. Cyb-Sec at the Production Line

The production line is the place where parts are manufactured and assembled in series to be shipped to the customer. Nowadays the lines are highly automated and quality control is performed on every part that is produced.

In this case, cybersecurity must also be considered. In many projects, the electronics are engraved or finished on the line. The SW is loaded, the sensors are calibrated, the device is configured with some data and finally, the EEPROM is locked so that the electronics cannot be manipulated again by third parties.

A security breach on the production line could affect manufacturing in several ways. For example, an attacker could remotely access the operation of the machines, obtaining data and parameters, changing settings, and even stopping manufacturing. It could cause devices to be programmed incorrectly, or to write off parts that should be rejects.

This could impact business and customer relationships. For these reasons, the ICT department will need to control communication and access as it does in other areas of the organization. When data is recorded on devices, a subsequent check should be made to ensure that the recording is correct and, as a last step, the device should be locked so that it cannot be recorded again.

Usually, a record is kept of the parts that come out and their characteristics. It is in the interest to protect this data and store it properly, with the desired encryption measures.

E. Cyb-Sec in the Vehicle

After the entire design and manufacturing process, the final product reaches the OEM, who installs it in the vehicle and sells it to the public. If the analysis has been carried out well, the system should be secure and not pose a risk to other elements of the vehicle.

On the other hand, the OEM also has certain cybersecurity responsibilities, as it sends commands to different systems, has access ports to ECUs, such as OBD-II, and in some cases can collect information about the performance and operation of its vehicles [11]. Some measures can be applied by the carmaker, such as secure boot process, IDPS or communication encryption.

If vehicle usage data is collected, it must be anonymized, without driver information, and the transmission paths must be secure. Alfa Romeo is a pioneer in providing a complete history of car telemetry data, guaranteeing its authenticity thanks to Non-Fungible Token (NFT) technology and digital certificates. The first vehicle in using NFT and blockchain technology will reach the market in 2023. It will be able to record data on vehicle’s manufacture, mileage, electric battery cycles, overhauls, part changes, etc. This will provide complete and tamper-proof traceability over the vehicle's lifetime [25].

F. Beyond the Vehicle

This subsection is intended to make the reader aware that safety goes beyond the digital and that poor design can compromise the integrity of the driver.

Today's cars are equipped with Advanced Driver Assistance Systems (ADAS). Some of them are based on computer vision and include in-vehicle video cameras, proximity sensors, RADAR, and LIDAR technologies.

These technologies are sometimes unobtrusive, but they are already being used in some vehicles to achieve a certain degree of semi-autonomous driving. It should be kept in mind that the environment in which the car moves, the real world, can also be hacked.

There are methods an attacker can use to provide wrong information to the vehicle. McAfee Advanced Threat Research conducted research that revealed these risks. Manipulating road signs with small stickers caused the car to misinterpret them. Similarly, using a magnet to place numbers on speed signs, it was possible to mislead the vehicle about the maximum speed of the road [26], posing a serious threat to occupants and road users. Another hack is the phantom attack [27], which consists of projecting images onto the road surface. Cars could be tricked into recognizing fake pedestrians or signals, and even non-existent lanes.

 ISBN: ISBNFILL

IV. The Aging of the Connected Vehicle: Cybersecurity Concerns

In 2022, the average age of the European car fleet was around 12 years [28]. Looking back a decade ago, cars have changed significantly, especially in terms of connectivity. Although vehicles then already had a lot of electronics, it was nothing compared to all the systems that are included today, and they lacked wireless connectivity to the outside world. As a result, there were fewer potential entry points for cyber threats, which made them inherently more secure. If the mechanics of the purchased vehicle were good and maintenance was adequate, an old vehicle could be in service for many years, well beyond its average useful life. In such a case, the driver would have to forgo the new safety features that a new car could provide.

More than 400 million connected vehicles are expected to be in use by 2025 [29], and each vehicle will produce 25GB of data per hour [30]. Several factors, including the widespread adoption of smartphones and the availability of high-speed mobile data networks, have led to the emergence of the connected vehicle. Some modern cars offer online services such as OTA SW updates, real-time traffic information, and remote diagnostics. Users also demand connectivity to their smartphones, allowing them to make and receive calls in the car, interact with GPS systems, read instant messages, and communicate with the infotainment system via voice commands using a voice assistant. Users also want to receive notifications on their phones about the status of the vehicle, whether to remind them when the car needs to be refueled or recharged, or when the next service is due. These applications can also collect data on schedules, routes, driving habits and even the installed updates [31]. As for the car itself, in some cases it may record user information for configuration purposes, such as customized views on the dashboard or preset settings for the position of seats and mirrors. This has made vehicles more vulnerable to cyberattacks by providing more entry points for malicious actors to exploit [31]. In addition, the emphasis on adding new features and connected functions has sometimes come at the expense of security, as it has been considered a secondary concern.

Electric Vehicles (EVs) also pose cybersecurity challenges, both in the car and in the power grid. For example, new home charging stations include features such as remote control of charging methods, which can be convenient but also make these devices more vulnerable [30]. In addition, Kaspersky cybersecurity researchers identified vulnerabilities in an EV charging station that could allow an attacker to damage the home power grid. The security threats ranged from stopping the vehicle charging process to setting the station to maximum current flow, which could lead to a fire [32].

As technology evolves, so does the risk of cyberattacks. With the rise of connected vehicles, the risk of cybersecurity threats is a growing concern. In the future, as today's modern, connected cars age, they may become more vulnerable. This is because the vehicles' SW and security systems are likely to become outdated and will no longer receive updates or patches from the manufacturer. As a result, the car may be more susceptible to hacking and data breaches, which can jeopardize the privacy and safety of its occupants and other road users. In addition, the car's HW components may become less reliable and secure as they age, increasing the risk of malfunctions and physical threats to the car's systems. Suppliers and OEMs must work together to address this issue and commit to designing and manufacturing safe, secure, and reliable systems.

V. Conclusions and Future Work

Cybersecurity is increasingly present in all areas. Every day, a lot of digital data is generated and spread through various channels. Sometimes this data contains sensitive information that needs to be protected.

Automotive is not different. Cybersecurity has also reached this industry and is set to be a growing trend. There are currently a lot of electronic systems connected to the vehicle's ECUs. Different communication protocols coexist inside the car for every need, both wired and wireless. All these communications must be secure and so must the in-vehicle devices.

Connectivity has made it possible for smartphones to be linked to the vehicle. Similarly, the car carries other wireless communication systems, such as GPS, 4G/5G mobile communications (to receive OTA updates or make emergency calls) or radio signals (to detect the car key or transmit tire pressure). For the future, there is talk of Drive-by-Wire, ADAS, autonomous driving and, with smart cities, Vehicle-to-Everything (V2X). This makes it necessary to secure the vehicle.

The question that remains is what will happen to the connected vehicle in the future. As a current vehicle ages, security vulnerabilities may emerge. When they are identified, it should be the responsibility of the manufacturer or supplier to provide support and fix them with an update. This will be difficult in many cases, especially if these parts are no longer manufactured and support is withdrawn. The digitization of the automotive sector will bring with it numerous cybersecurity challenges.

Acknowledgment

This work has been partially supported by the grant 'Ayudas para el desarrollo de proyectos de I+D mediante la contratación de personas doctoradas y la realización de doctorados industriales, programa BIKAINTEK 2019', by the Department of Economic Development, Sustainability and Environment of the Basque Government.

References

[1] C. Hammerschmidt, "Innovation in the car: 90% comes from electronics and software," eeNews Europe, Apr. 29, 2014. https://www.eenewseurope.com/news/innovation-car-90-comes-electronics-and-software (accessed Feb. 09, 2023).

 ISBN: ISBNFILL

[2] P. Mohankumar, J. Ajayan, R. Yasodharan, P. Devendran, and R. Sambasivam, "A review of micromachined sensors for automotive applications," Measurement: Journal of the International Measurement Confederation, vol. 140, pp. 305–322, 2019, doi: 10.1016/j.measurement.2019.03.064.

[3] Statista, "Car costs - Automotive electronics costs worldwide 2030," 2019. https://www.statista.com/statistics/277931/automotive-electronics-cost-as-a-share-of-total-car-cost-worldwide/ (accessed Jan. 25, 2023).

[4] X. Ferràs, E. Tarrats, and N. Arimany, "Disruption in the automotive industry: A Cambrian moment," Business Horizons, vol. 60, no. 6, pp. 855–863, 2017, doi: 10.1016/j.bushor.2017.07.011.

[5] A. Simonazzi, J. Jorge Carreto Sanginés, and M. Russo, "The future of the automotive industry: dangerous challenges or new life for a saturated market?" Institute for New Economic Thinking Working Paper Series, pp. 1–34, Nov. 2020, doi: 10.36687/inetwp141.

[6] O. Burkacky, J. Eichmann, M. Kellner, P. Keuntje, and J. Werra, "Rewiring car electronics and software architecture for the Roaring 2020s," McKinsey Center for Future Mobility, no. August, 2021.

[7] J. Á. Gumiel, J. Mabe, J. Jiménez, and J. Barruetabeña, "Introducing the Electronic Knowledge Framework into the Traditional Automotive Suppliers' Industry: From Mechanical Engineering to Mechatronics," Businesses 2022, Vol. 2, no. 2, pp. 273–290, Jun. 2022, doi: 10.3390/BUSINESSES2020018.

[8] European Automobile Manufacturers' Association (ACEA), "The Automotive Regulatory Guide." 2021.

[9] ISO/SAE, "ISO/SAE 21434:2021. Road vehicles — Cybersecurity engineering." 2021.

[10] R. Hegde, S. Kumar, and K. S. Gurumurthy, "The Impact of Network Topologies on the Performance of the In-Vehicle Network," International Journal of Computer Theory and Engineering, no. January, pp. 405–409, 2013, doi: 10.7763/ijcte.2013.v5.719.

[11] S. Kim and R. Shrestha, Automotive Cyber Security: Introduction, Challenges, and Standardization. Singapore: Springer Singapore, 2020.

[12] A. Martínez, K. A. Ramírez, C. Feregrino, and A. Morales, "Security on in-vehicle communication protocols: Issues, challenges, and future research directions," Computer Communications, vol. 180, no. September, pp. 1–20, 2021, doi: 10.1016/j.comcom.2021.08.027.

[13] G. Costantino, M. De Vincenzi, and I. Matteucci, "In-Depth Exploration of ISO/SAE 21434 and Its Correlations with Existing Standards," IEEE Communications Standards Magazine, vol. 6, no. 1, pp. 84–92, 2022, doi: 10.1109/MCOMSTD.0001.2100080.

[14] C. Schmittner, G. Griessnig, and Z. Ma, "Status of the Development of ISO/SAE 21434," in EuroSPI 2018: Systems, Software and Services Process Improvement, X. Larrucea, I. Santamaría, R. V. O'Connor, and R. Messnarz, Eds. Bilbao: Springer, 2018, pp. 504–513.

[15] K. Felser and M. Wynn, "Digitalization and Evolving IT Sourcing Strategies in the German Automotive Industry," International Journal on Advances in Intelligent Systems, vol. 13, no. 3 & 4, pp. 212–225, 2020.

[16] A. G. Marino, F. Fons, and J. M. M. Arostegui, "The Future Roadmap of In-Vehicle Network Processing: a HW-centric (R-)evolution," IEEE Access, vol. 0, no. July, pp. 69223–69249, 2022, doi: 10.1109/ACCESS.2022.3186708.

[17] F. Luo, X. Zhang, Z. Yang, Y. Jiang, J. Wang, M. Wu et al., "Cybersecurity Testing for Automotive Domain: A Survey," Sensors, vol. 22, no. 23, 2022, doi: 10.3390/s22239211.

[18] C. Bordonali, S. Ferraresi, and W. Richter, "Shifting gear s in cyber security for connected cars," McKinsey & Company, 2017.

[19] T. Królikowski and A. Ubowska, "TISAX - optimization of IT risk management in the automotive industry," Procedia Computer Science, vol. 192, pp. 4259–4268, 2021, doi: 10.1016/j.procs.2021.09.202.

[20] D. Cappelli, A. Moore, and R. Trzeciak, "Insider Theft of Intellectual Property," in The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Pearson Education, 2012, pp. 61–98.

[21] N. Mhaskar, M. Alabbad, and R. Khedri, "A Formal Approach to Network Segmentation," Computers and Security, vol. 103, p. 102162, 2021, doi: 10.1016/j.cose.2020.102162.

[22] S. N. Nikoi, C. Adu-Boahene, and A. Nsiah-Konandu, "Enhancing the Design of a Secured Campus Network using Demilitarized Zone and Honeypot at Uew- kumasi Campus," Asian Journal of Research in Computer Science, pp. 14–28, Jan. 2022, doi: 10.9734/ajrcos/2022/v13i130304.

[23] P. J. Ezra, S. Misra, A. Agrawal, J. Oluranti, R. Maskeliunas, and R. Damasevicius, "Secured Communication Using Virtual Private Network (VPN)," in Cyber Security and Digital Forensics - Proceedings of ICCSDF 2021, K. Khanna, V. V. Estrela, and J. J. P. C. Rodrigues, Eds. Springer Singapore, 2022, pp. 309–319.

[24] M. Fadzil, A. Kadir, M. Afif, D. Azmi, A. Nazari, and M. Rose, "Secure Communication over Virtual Private Network," vol. 35, no. 10, pp. 2129–2132, 2017, doi: 10.5829/idosi.wasj.2017.2129.2132.

[25] E. Babetto, "Blockchain ed Economia Circolare: Tracciabilità e Sostenibilità," Università di Padova, 2022.

[26] S. Povolny, "Model Hacking ADAS to Pave Safer Roads for Autonomous Vehicles," McAfee Blog, 2020. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/model-hacking-adas-to-pave-safer-roads-for-autonomous-vehicles/ (accessed Nov. 18, 2022).

[27] B. Nassi, Y. Mirsky, D. Nassi, R. Ben-Netanel, O. Drokin, and Y. Elovici, "Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks," in Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, Oct. 2020, no. Report 2020/085, pp. 293–308, doi: 10.1145/3372297.3423359.

[28] European Automobile Manufacturers' Association (ACEA), "Average age of the EU vehicle fleet, by country." 2022.

[29] Statista, "Size of the global connected car fleet in 2021, with a forecast for 2025, 2030, and 2035, by region," 2021.

[30] Z. Pourmirza and S. Walker, "Electric Vehicle Charging Station: Cyber Security Challenges and Perspective," 2021 9th IEEE International Conference on Smart Energy Grid Engineering, SEGE 2021, pp. 111–116, 2021, doi: 10.1109/SEGE52446.2021.9535052.

[31] D. Colombo, "How I got access to 25+ Tesla's around the world. By accident. And curiosity.," Medium, 2022. https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by-accident-and-curiosity-8b9ef040a028 (accessed Jan. 25, 2023).

[32] D. Sklyar, "ChargePoint Home security research," Kaspersky Lab Security Services, 2018.

 ISBN: ISBNFILL