sensors

MDPI

Review

Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies

Claudiu Vasile Kifor * and Aurelian Popescu

Faculty of Engineering, Lucian Blaga University of Sibiu, 55024 Sibiu, Romania; aurelian.popescu@ulbsibiu.ro
* Correspondence: claudiu.kifor@ulbsibiu.ro

Abstract: Modern vehicles are increasingly interconnected through various communication channels, which requires secure access for authorized users, the protection of driver assistance and autonomous driving system data, and the assurance of data integrity against misuse or manipulation. While these advancements offer numerous benefits, recent years have exposed many intrusion incidents, revealing vulnerabilities and weaknesses in current systems. To sustain and enhance the performance, quality, and reliability of vehicle systems, software engineers face significant challenges, including in diverse communication channels, software integration, complex testing, compatibility, core reusability, safety and reliability assurance, data privacy, and software security. Addressing cybersecurity risks presents a substantial challenge in finding practical solutions to these issues. This study aims to analyze the current state of research regarding automotive cybersecurity, with a particular focus on four main themes: frameworks and technologies, standards and regulations, monitoring and vulnerability management, and testing and validation. This paper highlights key findings, identifies existing research gaps, and proposes directions for future research that will be useful for both researchers and practitioners.

Keywords: automotive; vehicle; cybersecurity frameworks; cybersecurity standards; cybersecurity monitoring; cybersecurity testing

Citation: Kifor, C.V.; Popescu, A. Automotive Cybersecurity: A Survey on Frameworks, Standards, and Testing and Monitoring Technologies. *Sensors* **2024**, *24*, 6139. https://doi.org/10.3390/s24186139

Academic Editors: Fernando Viadero-Monasterio, Beatriz L. Boada and Maria Jesús López Boada

Received: 30 July 2024
Revised: 18 September 2024
Accepted: 18 September 2024
Published: 23 September 2024

1. Introduction

Over the last 40 years, cars have undergone significant transformations to meet quality, environmental, and safety requirements, as well as to satisfy customer expectations for performance, comfort, and driver assistance. In the 1980s, core electrical systems were introduced alongside anti-lock braking systems (ABSs) and airbags. Between the 1990s and early 2000s, vehicles saw a rise in electronic control units (ECUs) within their electrical architecture, driven by a focus on production efficiency and maintenance, as well as a desire for car customization through functional features. These features could later be updated by replacing ECUs or certain sensors and actuators. As time progressed, the electrical and electronic (E/E) architecture became decentralized. Safety and comfort functions were separated, and vehicle functions were distributed among many interconnected ECUs. Each ECU was capable of processing its own data and communicating with others to implement advanced functionalities [1].

In the late 2000s and early 2010s, connected and autonomous vehicle functions were introduced, transforming vehicle systems from isolated entities into open systems capable of exchanging information with the environment, drivers, and other traffic participants. This shift led to a significant increase in the complexity of the E/E architecture with each electrical subsystem, such as braking, steering, propulsion, infotainment, and connectivity systems, incorporating between two and ten ECUs. These subsystems also began to utilize various communication protocols, including LIN, CAN, FlexRay, and MOST [2]. By the 2010s, advanced driver assistance systems (ADASs) had entered the market, featuring

technologies such as emergency braking systems, lane-keeping assist systems, park assist systems, predictive forward collision warning systems, and autopilot functionality.

Today, vehicles are becoming increasingly connected through diverse communication channels, necessitating secure access for authorized users, the protection of driver assistance and autonomous driving data, and ensuring data integrity to guard against misuse or manipulation. Despite the advantages offered by these new technologies, there have been numerous intrusion incidents reported in recent years, highlighting the vulnerabilities in current systems [3–6].

Original Equipment Manufacturers (OEMs), international standard organizations, and customers face significant challenges in reducing cybersecurity risks throughout the development, production, and operation of vehicles. To maintain and enhance the performance, quality, and reliability of vehicle systems, software engineers must overcome major hurdles, including in communication diversity, software integration, testing complexity, compatibility and core reusability, safety and reliability assurance, data privacy, and software security [7]. Mitigating cybersecurity risks across these domains is a difficult challenge that requires practical solutions.

To address these challenges, establishing specific norms to standardize vehicle development, validation, and manufacturing processes has become a critical step. In 2016, the Society of Automotive Engineers (SAE) published SAE J3061, a guideline for developing secure automotive systems [8]. One of the key principles of this guideline is that cybersecurity must be integrated into the design of features from the outset, rather than being appended at the end of the development process. In 2021, the World Forum for Harmonization of Vehicle Regulations, a working group within the Sustainable Transport Division of the United Nations Economic Commission for Europe, published UN Regulation No. 155 [9]. According to this regulation, each OEM must establish and maintain a Cyber Security Management System (CSMS) to address organizational processes, responsibilities, and governance related to cybersecurity. The goal is to protect vehicles from cyber threats and attacks. OEMs are required to identify risks associated with vehicle technologies and implement measures to safeguard against them. These risk management processes must be demonstrated when OEMs seek vehicle type approval from validation authorities.

The engineering requirements for managing cybersecurity risks across the concept, product development, production, operation, maintenance, and decommissioning phases of E/E systems in road vehicles are detailed in the ISO/SAE 21434:2021 standard [10]. Starting in July 2024, this standard will apply to all newly manufactured vehicles. A key challenge for OEMs is integrating the new CSMS into the traditional automotive software development lifecycle. In the initial phase of implementing the standard, the CSMS will likely be added as an "add-on" to existing tools. Over time, automotive companies will develop solutions to more seamlessly integrate it into their development processes, similar to how safety requirements under ISO 26262 were eventually integrated [11].

A generic Safety Management System for the automotive industry is introduced in [12], where it is compared with similar systems from aviation, marine, and rail industries. Current safety standards primarily focus on systems controlled by humans. However, to support the development of autonomous vehicles, safety processes need to be updated. To address this, the ISO 21448:2022 standard (Road vehicles—Safety of the intended functionality) [13] was created.

The introduction of these new cybersecurity norms has spurred researchers to critique and suggest improvements to certain requirements [14,15]. Beyond the commercial interest in these norms, researchers are keen to provide solutions and tools to aid their implementation and contribute to the evolution of these regulations over time.

This study aims to analyze the current state of research regarding cybersecurity in general, with a particular focus on four main themes that were revealed by a VOSViewer cluster analysis: frameworks and technologies, standards and regulations, monitoring and vulnerability management, and testing and validation. It also seeks to propose development directions that will be useful for both researchers and practitioners.

2. Automotive Cybersecurity—A Bibliometric Analysis

A comprehensive literature search was conducted using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to identify existing studies and approaches related to cybersecurity in the automotive industry (Figure 1).

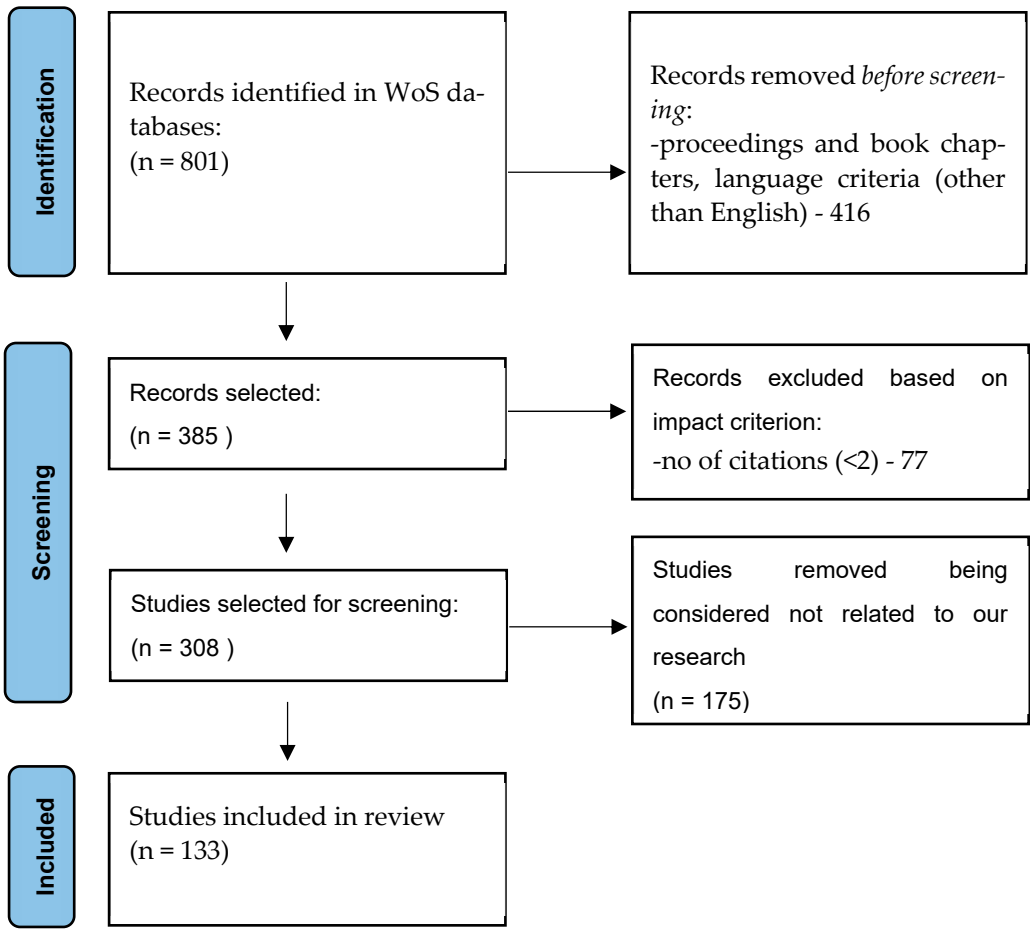

Figure 1. PRISMA flow diagram outlining the study selection process.

The searches were conducted in December 2023 in the Clarivate Web of Science database using the following keyword strings: "cybersecurity" + "vehicle" or "cybersecurity" + "automotive".

From the search results, we identified 801 studies, as follows: 405 proceedings papers, 337 articles, 48 review articles, and 11 documents in other categories (book chapters).

The first article on automotive cybersecurity was published in 2012. However, there has been a significant increase in the number of articles published in recent years. Approximately two-thirds of the total articles have been published within the last three years (Figure 2), reflecting the growing importance of cybersecurity in the automotive sector.

The overwhelming majority of the articles were published in English (793 articles). Only a few articles were available in other languages, including: Spanish, German, and Portuguese.

For the detailed analysis, we focused exclusively on publications classified as Articles and Reviews. To ensure that our analysis concentrated on impactful studies, we introduced an additional filter: articles must have at least two citations, which serves as a minimum level of visibility. This criterion excluded other 77 documents.

After applying this filter, we conducted a title and abstract screening, to further narrow down the studies, removing an additional 175 studies that were deemed unrelated to our research focus. This includes studies primarily centered on areas such as drones,

flying vehicles, and cybersecurity for electric grid management systems used in charging electric vehicles.

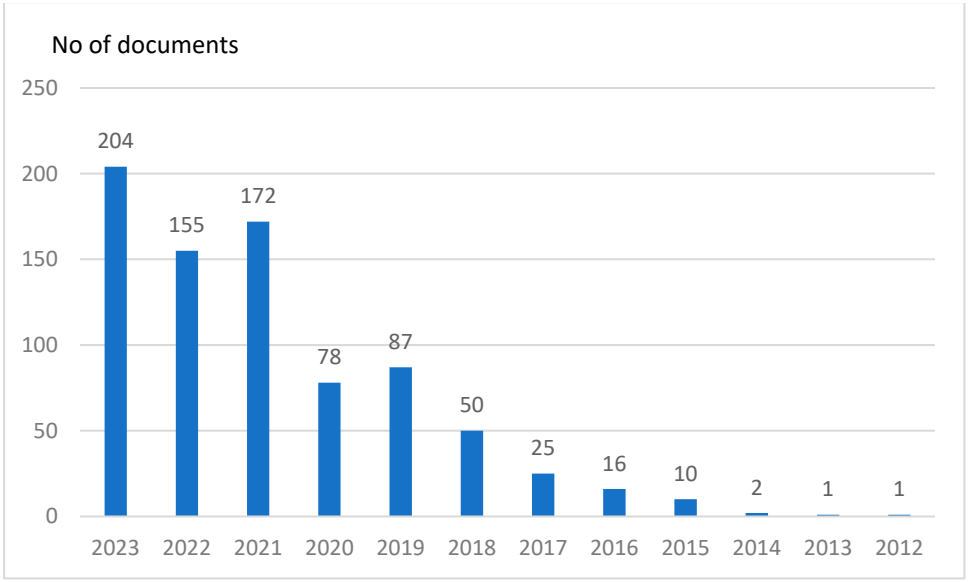

Figure 2. Number of publications per year from the WoS database (based on search: "cybersecurity" + "vehicle" or "cybersecurity" + "automotive").

The 133 articles selected for detailed review were processed using VOSViewer software, version 1.6.20 [16]. This software allowed us to perform a comprehensive analysis of the keywords and themes present in the selected studies, revealing four distinct clusters (Figure 3): Frameworks and Technologies (green, partially overlapped with yellow), Standards and Regulations (purple), Monitoring and Vulnerability Management (red), and Testing and Validation (blue)

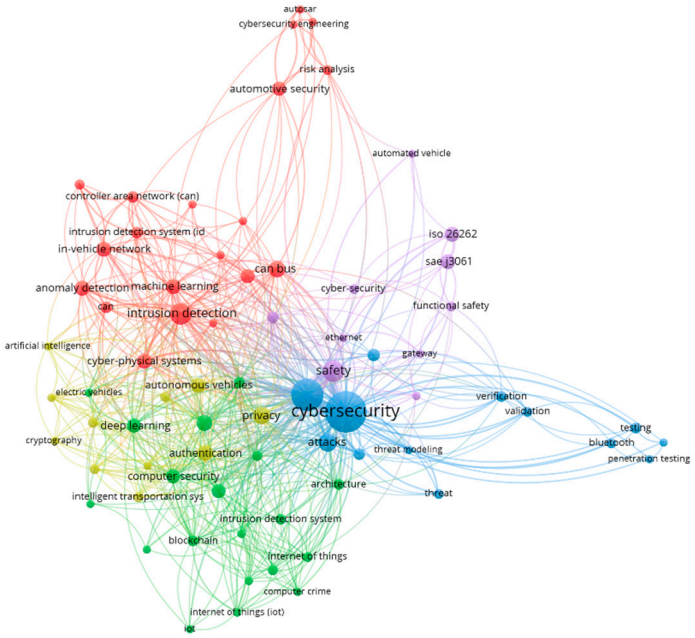

Figure 3. VOSViewer clusters for automotive cybersecurity paper keywords.

These clusters provided a structured foundation for our detailed literature review in the following sections.

3. Literature Review

3.1. Frameworks and Technologies for Cybersecurity

3.1.1. CS Frameworks

To tackle cybersecurity challenges, OEMs must adapt their governance, culture, processes, and technologies. Several articles suggest the need for a Systems of Systems (SoS) or framework approach to effectively implement CSMS and detect and mitigate threats [17,18]. A SoS approach should encompass not only the vehicle and its components, but also the cloud where vehicle data are stored, interactions with other vehicles (such as in platooning functions), road infrastructure (Vehicle-to-Road communication systems), and charging stations for electric vehicles.

Z. El-Rewini proposes a three-layer cybersecurity framework—encompassing sensing, communication, and control layers—to provide a comprehensive understanding of security threats [19]. Among these, the communication layer is identified as the most vulnerable, with the potential for significant damage.

In another study, V.K. Kukkala et al. [20] present an architecture related to Connected and Autonomous Vehicles (CAVs) and identify various vulnerabilities that could affect these systems, suggesting also possible solutions. Malware detection techniques are categorized here into signature-based, behavior-based, cloud-based, heuristic, and machine learning (ML) approaches. The authors recommend that future research on combating malware attacks should focus on lightweight cryptographic authentication, firewall systems, deep learning (DL) using offloading computation mechanisms, and software-defined security [21].

A. Khalid et al. [22] introduced the Framework for Analysis, Comparison, and Test of Standards (FACTS), which comprises four key steps: analyzing stakeholders (including government entities, battery manufacturers, battery management system (BMS) manufacturers, and OEMs), assessing their technical requirements through Threat Analysis and Risk Assessment (TARA), comparing various standards, and validating these standards using testing methods such as fuzz testing and penetration testing.

In a similar vein, S. Khalid Khan et al. [23] propose a conceptual System Dynamics (SDs) model for evaluating the cybersecurity of CAVs. This model integrates various elements such as the CAV communication framework, secure physical access, human factors, penetration levels, regulatory laws, policy frameworks, and trust across the CAV industry and the public. A Casual Loop Diagram, a method derived from system theory, is used to model the structure of SD, and to clarify the relationships between its variables.

Aldhyani et al. [24] developed a high-performance system using a ML approach to protect vehicle networks from cyber threats. Their proposed security solution was validated using a real vehicle network dataset that includes attack types like flooding, spoofing, replay attacks, and benign packets. This model can be integrated into some ECUs as software packets or, more realistically, as a dedicated Intrusion Detection System (IDS).

Wang et al. [17] designed a framework to analyze the performance of CAV platoons in various driving environments. This model aids in developing new cybersecurity requirements for emerging ECUs and crafting test scenarios for system validation.

Chandwani et al. [25] identify current security challenges and recommend solutions for mitigating cyber threats to electric vehicles and their onboard charging systems. As a use case, 6.6 kW onboard charger topologies are presented along with their potential threat vectors and corresponding countermeasures. These include: security measures for the CAN protocol (over MAC), FPGA (Field-Programmable Gate Array)-based protection, and hardware-based defense mechanisms such as short-circuit protection, digital signal processing for digital filters, and intelligent data processing algorithms for sensor signals. Additionally, Hafeez et al. [26] offer a practical solution to spoofing attacks within In-Vehicle Networks (IVNs) through ECU Fingerprinting using Parametric Signal Modeling.

Sabaliauskaite et al. [27] examined the interdependencies between safety and cybersecurity, exploring how safety measures impact cybersecurity and vice versa. They developed the TOMSAC methodology for managing trade-offs between automotive safety and cyber-

security. This includes cases of conditional dependency (where a safety requirement is a prerequisite for security), antagonism (where safety and security requirements conflict), and reinforcement (where enhancing safety also improves security or vice versa).

3.1.2. CS Technologies

Model-Based Engineering (MBE)

Model-based engineering is widely used in the automotive industry because of the low costs of SW production, code reusability and the ability to work in complex projects [28]. It is important for model-based development tools to be checked so that they do not introduce cybersecurity vulnerabilities during software creation [10].

MBE also improves testing capabilities and testcases generation and can be easily automated if the SW development is based on MBE. Using model-based testing methods for automotive security testing could help to discover issues earlier than other manual methods (penetration test, for instance) [29–31]. The output of threasts assessment (attack trees) is used to create test cases that are generated automatically. An expanded model-based methodology to test SW updates over-the-air was analyzed by Kirk et al. and effective testcases were derived from attack tree results from security treat analysis [32,33].

MBE and component-based SW engineering (CBSE) can be combined as a cost-effective option to deal with the complexity of the SW. Previous studies suggest to group the subsystem (safety/non-safety systems) in security islands, separated by gateways, integrate cybersecurity HW accelerators in the new processors to sustain message encryption in real-time [28].

Blockchain

Previous studies explored ML and blockchain technologies as cybersecurity defense mechanisms for IVNs [34–36]. ML-based solutions are analyzed based on intrusion/malware detection, topology (centralized or distributed), and technical dimension (traditional ML and DL), while blockchain-based solutions are analyzed based on secure data storage, secure onboard communication, secure data access, consensual protocol (proof of work; proof of stake), and deployment/miner [37,38].

In general, blockchain-based solutions have four applications: secure data access, secure data storage, secure data transmission, and data contribution [38–40]. For data contribution application, it is important to mention CreditCoin, a protocol that was created in order to encourage vehicles to share information in smart vehicle networks [41].

Kim et al. [42] proposed the adoption of current blockchain technology in BMSs (battery management systems), which can be used as a cybersecurity reference for the development of battery systems. Other studies investigate how new blockchain algorithms could solve current automotive challenges, such as growing ledgers, increasing scalability, and reducing complexity and latency [37,38,43].

Blockchain technology could be applied not only in the vehicle development phases but also in production and supply chain management. An interview with three major German industry players highlights the challenges of modern supply chains, including their complexity, geographic dispersion, interconnected networks, and diverse regulatory frameworks. These challenges could be addressed by using blockchain as a public digital platform, enabling real-time, transparent connections between multiple supply chain actors. However, the interviews also revealed a significant barrier to adoption: uncertainty surrounding legal regulations, particularly regarding data privacy [44].

In the post-production (after-sales) phase, a blockchain-based continuous monitoring system can assist OEMs in receiving anonymized field data, reducing concerns related to data trust and security [45]. This system periodically transmits information such as diagnostic data codes, performance metrics, and part authenticity from the vehicle to maintenance servers. The data on these servers can be accessed not only by OEM data analysts but also by vehicle owners, enhancing trust in the vehicle's safety, maintenance quality, and service history [45].

Machine Learning and Deep Learning

The application of AI in vehicle security is promising, but still limited due to big memory consumption and processor resources [46]. For these reasons, AI is planned to be used mostly in cloud systems and less in vehicles where embedded processors are used.

Machine learning-based IDSs were proposed for big data analytics in vehicle networks [47,48], while DL techniques could be used for IDS design [49,50].

In a review of the automotive cyber-attacks, V.K. Kukkala proposed an AI-based IDS in IVNs and VANET environments, particularly for Vehicle-to-Vehicle (V2V) and Vehicle-to-Everything (V2X) communication. AI is used as an in-vehicle IDS (GAN-based IDS; GRU-based recurrent autoencoder; LSTM-based encoder–decoder with self-attention; Temporal CNN with neural attention). There are also solutions recommended for actual cybersecurity challenges: data protection and privacy; tamper-proof AI; secure integrated circuit supply chain [20]. In another review, S. Rajapaksha et al. focus on AI-based IDS solutions for CAN communication, highlighting the limitations of these approaches and discussing the security challenges inherent to AI models [46]. Supervised and unsupervised learning (ML or DL) have to be combined with rule-based techniques to cover the complete range of cybersecurity threats. The conclusion of the review is that host-based IDSs are not a practically solution for vehicles (ECU HW limitation), but network-based IDS can be introduced like a separate ECU in vehicles or like a virtual IDS in the cloud (less feasible regarding real-time requirements).

The integration of AI in the automotive industry has led to a need for innovative methods to validate self-learning systems. By combining the benefits of scenario-based testing with metamorphic relations—especially for generating test inputs and creating test oracles—it is possible to mitigate functional and security risks [51].

Cybersecurity and Safety Relationship

C.W. Lee, S. et al. applied a cybersafety method (System Theoretic Process Analysis -STPA and STPA-Sec) to analyze safety and security hazards. Later, STPA and CHASSIS (Combined Harm Analysis of Safety and Security for Information Systems) methods were compared. Both methods (STPA and CHASSIS) were applied to the Mobility-as-a-Service (MaaS) and Internet of Vehicles (IoV) cases, focusing on the OTA feature. Their results show that the STPA method (analyzing the system taken as a whole) identified additional hazards and more effective requirements compared to CHASSIS [52].

The fuzz testing method is increasingly being applied in automotive projects for cybersecurity specifications at the system test level. However, in some cases, this method can also be employed for functional and safety-related objectives during early development stages, such as unit testing and integration testing [7].

Possible effects of network-induced delays (resulted from Denial-of-Service cyberattacks) for autonomous vehicles could affect driving safety and comfort. For such a case, Viadero-Monasterio et al. propose a multi-input multi-output method for path tracking control, a method that could attenuate the safety effects for network delays of millisecond order [53].

Secure Onboard Communication (SecOC)

The AUTomotive Open System ARchitecture (AUTOSAR) partnership created and established an open and standardized software architecture for automotive ECUs [54]. In 2017, the first specification for secure onboard communication (SecOC) [55] was released, describing a practical approach of how secure in-vehicle communication can be achieved. Instead using a shared key between sender and all receivers, a secret pair consisting of a public key and a secret key is used. In this way, the receiver has the possibility to check the authenticity of sender and also the integrity of the received data. Nowadays, SecOC is implemented by almost all OEMs, and SecOC is used not for all CAN messages, but only for safety-critical and cybersecurity-relevant messages. SecOC implementation requires periodic resynchronization phases, and its implementation across various embedded

systems demands significant computational power. Later on, similar specifications were released over AUTOSAR group for secure hardware extensions, crypto stack, secure diagnostics [56] and secure logging, identity and access management, intrusion detection system manager [57], secure updates, and trust platforms.

Internet of Things (IoT)

The Internet of Things is increasingly being integrated into the automotive industry, primarily through intelligent sensors [58]. Designed to be lightweight, Message Queue Telemetry Transport (MQTT) was the easiest IoT data communication protocol adopted in the automotive sector.

Previous studies analyzed the impact of adding the Transport Layer Security (TLS) protocol to MQTT communication, with positive results observed in networks with lower busloads [59]. The implementation of TLS and MQTT in automotive networks permit now the secure software update Over-The-Air. Shin et al. [60] propose a novel firmware over-the-air (OTA) update method, MQTree, which combines the MQTT protocol with Merkle tree-based blockchain verification to enhance the efficiency of software updates. The study demonstrates that MQTree performs well against spoofing, man-in-the-middle, and duplicate update attacks. However, to address denial-of-service threats, the addition of a firewall to the system is necessary.

Previous studies regarding IoT analyzed the potential risks to data privacy that can be introduced by this technology, and explored ML and DL solutions to mitigate these risks [61,62]. The conclusions were that current solutions are still in the early stages, and indicated that IoT architecture based on deep neural networks could be adapted for use in cyberattack monitoring systems or IDSs.

Automotive Ethernet (AE)

To meet the automotive industry's requirements for electromagnetic compatibility and immunity, a new Ethernet standard was developed: 100Base-T1, which supports full-duplex operation over a single twisted pair [63]. Previous studies have shown that Automotive Ethernet is gaining traction in vehicle networks due to its high data transfer speeds and enhanced cybersecurity features [64]. These studies also identified security vulnerabilities in Ethernet communication and presented potential countermeasures. De Vincenzi et al. experimentally compared four cybersecurity solutions (SecOC, TLS, Internet Protocol Security, and Media Access Control Security—MACSec) implemented on data link layers of AE [65]. None of the compared solutions excelled in all operation steps. In systems where speed is the most important element, the combination of Advance Encryption Standard and HMAC solutions seems to be the best choice, while in the context where the security is the priority, a combination of Advance Encryption and MACSec provides a good compromise between security and timing.

Two ongoing projects are focused on enhancing the safety properties of automotive Ethernet within the scope of Time-Sensitive Networking (TSN) profiles: IEEE P802.1DG and IEEE P802.DU [66].

Data Privacy Challenges

Unlike the IT domain, where security risks mainly target data privacy and confidentiality, the automotive sector—particularly for autonomous vehicles—places a strong emphasis on functional safety. M. Benyahya conducted a review of cybersecurity and data privacy concerns for autonomous vehicles, highlighting the need for greater involvement from automotive stakeholders [67]. Technical mitigation solutions, such as data anonymization and encryption, should be incorporated during case study and implementation phases of vehicle development. Despite ongoing advancements in Zero Knowledge Theory as a method for encrypting private data, there is still a gap in legislative measures, particularly the absence of a trusted authority for secure key exchange between different users [68].

A privacy manager was developed as a technical solution for data privacy, aiding applications by filtering specific data in real-time to support the implementation of privacy functions [69]. This approach was validated using two scenarios: platooning and silence testing, with GPS position data from the vehicle serving as the test input.

Mobility as a Service (MaaS) applications impose strict requirements for data privacy. Kong et al. [70] explore a privacy-preserving solution for driver monitoring using blockchain technology, specifically encryption with public keys. The practical aspect of the study demonstrates the feasibility of this approach, though it highlights that the most time-consuming phase is data transfer between the vehicle and the cloud. Additionally, a limitation of the method is its scalability, particularly when handling real-time data acquisition from multiple vehicles.

Cloud Cybersecurity Solutions

A review of the cybersecurity requirements for cloud-supported connected vehicle (CV) applications identified six key categories: confidentiality, integrity, privacy, authentication, accountability, and availability. Several cybersecurity challenges were highlighted, including the authentication of high mobility nodes, trustable V2V communication, vehicle location validation, securing in-vehicle network (IVN) communication, and data privacy in the cloud. Future research directions include exploring Infrastructure as Code, integrating blockchain with AI, leveraging quantum computing for machine learning, utilizing 5G for secure and faster communication, heterogeneous wireless networking, and network function virtualization [43].

3.2. CS Standards and Regulations

ISO 26262 was the first standard developed for managing functional safety in automotive applications [71]. Its primary goal is to establish a uniform approach for OEMs to address safety considerations.

The increasing complexity of high connectivity interfaces, shared services, and advanced autonomous vehicle features has necessitated a shift in the development of the E/E systems, emphasizing the need for enhanced cybersecurity measures. In 2018, a revised version of ISO 26262 [11] was released, introducing significant updates such as improved management of safety anomalies, more detailed objectives, references to cybersecurity, and additional requirements for trucks, buses, and trailers. This was preceded by the introduction of SAE J3061 in January 2016, the first global cybersecurity standard for the automotive industry [8].

Recently, the automotive sector has placed a stronger emphasis on cybersecurity while continuing to address safety functions. New standards, norms, and guidelines are being developed to establish unified requirements for both cybersecurity and functional safety and to provide practical tools for their implementation. Table 1 provides a summary of the most relevant standards, norms, and guidelines in this field.

Table 1. Standards, norms and guideline for functional safety and cybersecurity.

Standard/Norm/Guideline	Name
ISO 26262:2011 [71]	Road vehicles—Functional safety
AUTOSAR (2014) [72]	AUTOSAR safety solutions
SAE J3061:2016 [8]	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
ASPICE (2017) [73]	Automotive SPICE Process Reference and Assessment Model
ISO 26262:2018 [11]	Road vehicles—Functional safety
TR-68 (2019) [74]	Technical reference. Autonomous vehicles (Singapore Standards Council)
ISO/TR 4804:2020 [75]	Road vehicles—Safety and cybersecurity for automated driving systems—Design, verification and validation

Table 1. *Cont.*

Standard/Norm/Guideline	Name
SAE J3061:2021 [76]	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
ISO/SAE 21434:2021 [10]	Road vehicles—Cybersecurity engineering
ASPICE for Cybersecurity (2021) [77]	Automotive SPICE for Cybersecurity
UN R155 (2021) [9]	Cyber security and cyber security management system
UN R156 (2021) [78]	Software update and software update management system
UN R157 (2021) [79]	Automated Lane Keeping Systems
ISO 21448:2022 [13]	Road vehicles—Safety of the intended functionality
AUTOSAR (2022) [80]	AUTOSAR cybersecurity solutions
ISO/PAS 5112:2022 [81]	Road vehicles—Guidelines for auditing cybersecurity engineering
ISO/SAE 24089:2023 [82]	Road vehicles—Software update engineering

Previous studies explored the integration of safety and cybersecurity for risk management and system/software validation [83–85]. ISO 21434 provides a structured framework for cybersecurity, detailing a uniform development process, specific requirements and specifications, and a standardized language for communicating and managing cybersecurity risks among stakeholders [86,87].

A cybersecurity development lifecycle model, incorporating both ISO 21434 and Cybersecurity ASPICE requirements, has been proposed and implemented in automotive pilot projects, such as those involving electric power steering systems [88]. This model emphasizes threat modeling and vulnerability analysis as fundamental components.

The introduction of ISO 24089 aims to transform the management of software updates within the automotive sector [82]. Alongside ISO 24089, UN Regulation No. R156 [78] has established a more standardized approach to software update requirements through the Software Update Management System (SUMS).

Schober et al. [89] reviewed the current state of automotive cybersecurity regulations and standards, highlighting the connections and interdependencies among them.

3.3. CS Monitoring and Vulnerability Management

3.3.1. Intrusion Detection Systems

Intrusion Detection Systems (IDSs) have recently been incorporated into automotive architectures alongside cybersecurity risk mitigation strategies. While IDS is not explicitly mentioned in ISO 21434 or R155 regulations, various IDS approaches are frequently analyzed and proposed for detecting attacks, logging incidents, and mitigating threats. Most IDS solutions are concentrated on CAN and Ethernet communication channels [90,91].

IDS functionalities can be implemented either as a separate or dedicated ECU, within the vehicle network (network-based IDS). This could involve a cloud-based software solution that receives data from the vehicle's telematics ECU [92] (cloud network-based IDS), or a software module embedded in one or more high-performance ECUs within the vehicle (host-based IDS) [93]. Currently, OEMs are more inclined to deploy dedicated ECU IDS versions.

In terms of attack detection methods, IDS systems are categorized into signature-based or anomaly-based systems [94]. Signature-based IDS utilize a database of known attack signatures and monitor permissible data exchanges between ECUs. This database requires regular updates, as does the information regarding allowed data exchanges following any ECU software updates. Anomaly-based IDS, on the other hand, monitor changes in physical properties (e.g., voltage, current, busload) of in-vehicle network communications [95,96], or detect anomalies in functional signal values (e.g., GPS signal jumps indicative of spoofing attacks) [97].

Researchers are also focusing on in-vehicle network IDS as a robust defense mechanism against automotive attacks [98]. IDS solutions are being explored for Vehicular Ad-hoc Network (VANET) systems [99], including flow-based IDS that are sensitive to timing and frequency changes of messages, and payload-based IDS that detect modifications to message content [100]. Furthermore, algorithms are being developed to generate real-time model parameters for specific CAN buses, enabling specification-based IDS using anomaly-based supervised learning with real-time models (SAIDuCANT) [101].

Mansourian et al. [102] propose an IDS solution that integrates flow-based and payload-based IDS through three modules: a time-based prediction network, a payload-based prediction error processor, and a Gaussian Naïve Bayes classifier to determine the presence of active attacks.

The data-driven, payload-based method for identifying falsified vehicle functionalities, such as compromised connected vehicle trajectories, has been extensively researched. This method can also be applied to detect safety-critical events [103].

For CAVs requiring communication with external systems like cloud services or road infrastructure (e.g., platooning), developing external or internal IDS supported by firewalls could be beneficial [104,105]. Park et al. [104] demonstrate a method for detecting adware and malware in Android OS-based ECUs. Additionally, a study on the Service-Oriented Architecture (SOA) paradigm [105] presents a combination of firewall, IDS, and Identity and Access Management (IAM) as countermeasures to protect autonomous vehicles.

With the growing intelligence of vehicle sensors, which now perform not just analog-to-digital conversions but also digital signal processing, and the integration of IoT technologies, sensors interact with ECUs using standard communication protocols. Research is underway to identify potential threats introduced by smart sensors, their associated security risks, and methods for cybersecurity monitoring and attack detection at the sensing layer [58].

3.3.2. Security Operation Center

New regulations are requesting OEMs to establish dedicated vehicle security teams responsible for monitoring all sold vehicles and addressing new vulnerabilities discovered in their software. The study referenced in [106] identifies commonalities and differences between Security Operation Centers (SOC) in IT and Vehicle Security Operation Centers (VSOC). It highlights that methods, procedures, and technical solutions from IT SOCs cannot typically be applied directly to VSOCs due to their unique requirements.

In other studies, Fenzl et al. examined various methods for reporting incidents to both internal and external SOCs, focusing on how collaborative security patterns can be developed [107], while Barletta et al. present a methodology that integrates quantum optimization with intrusion detection systems and the National Vulnerability Database. This approach allows intrusion systems to learn from incidents reported and added to the vulnerability database [108].

3.3.3. Threat Analysis and Risk Assessment (TARA)

Wang et al. [109] propose a systematic risk assessment framework that includes a specific risk assessment process and systematic methods. This framework has a similar structure with TARA process mentioned in ISO 21434 [10], and it is based on three standard blocks: risk identification; risk analysis; and risk assessment, that are applicable across all phases of the vehicle lifecycle.

Zhang et al. conducted a case study focusing on threat analysis, test item determination, and vulnerability scoring, which are essential components of a comprehensive TARA procedure [110].

Dobaj et al. carried out a case study on risk-driven system design and the development of cybersecurity requirements [111]. This study complements the standard and offers engineers a practical guide for developing secure systems. Prior to initiating TARA, preliminary steps must be taken, including identifying system assets and associated risks through structured approaches.

A scenario-based TARA approach was also introduced [112], which was applied to Over-the-Air updates for CAVs to derive cybersecurity goals, which will then be translated into cybersecurity requirements.

Neither systematic risk assessment (typically used in model-based development projects) nor scenario-based risk assessment provides a complete solution for all automotive applications [31]). Depending on the safety criticality and complexity of the application, one of these methods might be chosen, or in some cases, a combined approach may be used, which could increase the costs of product development.

The Trusted Information Security Assessment Exchange (TISAX) certification, which is adapted from ISO 27001 [113], serves as a European automotive industry standard for "information security assessment" (ISA). It focuses on key aspects of information security, such as data protection and third-party connections [114]. The term TISAX did not appear in our bibliographic research because it is associated with "security" rather than "cybersecurity" within the automotive context. The implementation methods and benefits of TISAX were analyzed in [115]. A new version of TISAX is expected to be released in 2024.

3.3.4. Cybersecurity and Platooning Functions

Cybersecurity is crucial for platooning functions and connected vehicles [116]. Various studies have examined the impact of cybersecurity attacks on vehicle platoons [17,117–119]. Additionally, several cybersecurity solutions have been proposed for vehicle platoons, including an anomaly detection system [120] and a method for detecting false data injection attacks [121].

3.3.5. Secure Communication

Secure communication is an effective approach to enhancing the cybersecurity of vehicle systems. Since 2014, AUTOSAR has provided specifications for the Secure OnBoard Communication (SecOC) function [55], which can now be seamlessly integrated into ECU software by any supplier using AUTOSAR stacks and libraries.

To further bolster the cybersecurity of IVNs, various secure communication protocols have been proposed and validated, including TOUCAN and IDH-CAN [18,122–126]. TOUCAN (proTocol tO secUre Controller Area Network) was designed to secure CAN communication [122]. An improved version of TOUCAN, called CINNAMON (Confidential, INtegral aNd Authentic on board co-MunicatiON), was proposed to be compatible with AUTOSAR and addresses confidentiality issues that SecOC does not [127,128].

Identification Hopping CAN (IDH-CAN) is another hardware and software solution that ensures both communication security and real-time application constraints. It introduces a hardware firewall between the physical and data link layers. However, implementing IDH-CAN in existing vehicle architectures can be challenging, as it requires simultaneous updates to all hardware CAN drivers [124].

Palaniswamy et al. developed a new secure CAN protocol suite that includes a session key update protocol (NSKUP) to prevent key reuse [18,125]. While NSKUP requires significant computational resources and introduces time delays, Groza et al. introduced a lightweight broadcast authentication (LiBrA-CAN) protocol as a more resource-efficient alternative [129].

Additionally, the security of wireless communication between On-Board Units (OBUs) and Road Side Units (RSUs) has been examined, with recommendations for implementing lightweight cryptographic techniques for CAVs [126]. For vehicles in motion, rapid initialization of wireless communication between OBUs and RSUs is essential, as standard Wi-Fi authentication methods are too slow for Vehicle-to-Infrastructure (V2I) communication.

3.4. CS Testing and Validation

To enhance cyber defense activities, it is essential to advance validation and verification processes. This includes improving testbenches, CAN simulators, and Hardware-in-the-

Loop systems, developing new types of test cases, analyzing in-vehicle firewall properties, and exploring innovative cybersecurity solutions [130,131].

In support of the secure-by-design principle, methods adopted from other industries (black-box fuzz testing) has been developed to construct effective security tests. A case study with a CAN-fuzzer demonstrate the effectiveness of fuzz testing [132], while a security analysis and a reverse engineering case study applied for a instrument cluster ECU shown a way of using fuzz testing in later phases of product development [133]. Future research should focus on optimizing how useful metrics are gathered from fuzz testing.

Digital Twin-Based Security Testing is a new method proposed, which involves creating and executing cybersecurity test cases automatically in a black-box setting [134]. This approach demonstrates the feasibility of test automation by transferring attacks from a model (one system) to a SUT, through generalization using a domain-specific language. A case study using digital twin-based security method could not be identified in the literature.

In the past decade, model-based testing methods (whitebox testing) have become common in the automotive industry. These methods can also be applied to automotive security testing as a partial solution for detecting vulnerabilities [29–31].

Cui et al. [135] developed a simulation platform to s evaluate the performance of specific autonomous vehicle functions and conduct safety impact analyses under various cybersecurity attack scenarios.

Marksteiner et al. [136] conducted a case study that incorporates not only functional testing methods but also interface testing, static code analysis, penetration testing, vulnerability scanning, and fuzz testing. The proposed structured testing process is adaptable, allowing test engineers to use their preferred toolsets.

Standardizing automotive penetration testing from a black-box perspective is challenging. Zhang et al. developed a case study for a penetration testing framework called ICVTest, which guides inexperienced testers step-by-step through test case generation and execution [137].

Risk management during the development phase is handled similarly for safety and cybersecurity, using HARA (Hazard Analysis and Risk Assessment) for safety and TARA for cybersecurity [10]. Some studies suggest that integrating safety and security risk management, including shared processes and documentation, could provide a better overview of product risks and potentially reduce costs [52,84,112].

Model-based testing is not only applicable to functional safety requirements but can also partially support cybersecurity testing [28], helping to identify security issues earlier in the development process (as penetration testing typically occurs later).

Additionally, studies [138,139] propose sensor solutions for automobiles that enhance both safety (real-time and recovery requirements) and cybersecurity (attack detection) performance simultaneously.

To improve effectiveness and identify bugs earlier in the development process, Oka et al. suggest moving fuzz testing from the System and Acceptance Test phases to the Unit Test phase [140] This change would also facilitate easier automation and execution of fuzz tests.

4. Conclusions and Future Research

This paper provides a comprehensive review of the current state and challenges of [138] cybersecurity in the automotive industry. The bibliometric network analysis was based on the Web of Science Core Collection database and highlighted four clusters of cybersecurity-related themes: frameworks and technologies, standards and regulations, monitoring and vulnerability management, and testing and validation.

Frameworks and Technologies. Current automotive development frameworks are beginning to incorporate comprehensive cybersecurity processes required by new standards. There is a need to optimize these processes and improve their integration throughout the development cycle [15].

Recent studies recommend adopting a system-of-systems approach, which includes not only the vehicle and its components but also the cloud where vehicle data are stored, interactions with other vehicles, road infrastructure, and charging stations for electric vehicles [18].

The application of AI in vehicle security is promising, and the proposed solutions should undergo extensive testing [21,141]. Although AI concepts and algorithms were proposed as solutions for security challenges during the last years, their practical implementation has been limited.

The integration of AI in the automotive industry has led to a need for innovative methods to validate self-learning systems. By integrating the advantages of scenario-based testing with metamorphic relations—particularly for generating test inputs and creating test oracles—it becomes possible to mitigate both functional and security risks [51].

Standards and Regulations. The R155 and ISO 21434 regulations mark a significant milestone in establishing clear requirements for the scope, performance, and auditing of cybersecurity, covering the entire product lifecycle [136]. A second release of ISO/SAE 21434 is currently in development, aiming to address gaps in the existing version [125]. Simultaneously, researchers and practitioners must develop specific technologies and methods, such as cybersecurity testing, to help OEMs and suppliers meet the standards' requirements.

Enhancements are also needed in the relationships between OEMs, suppliers, and third-party providers, as recent cybersecurity incidents have highlighted vulnerabilities originating from ECU supplier software [130]. The first edition of ISO/SAE 21434 provides a good framework for dividing responsibilities in security incidents, but agreements between OEMs and suppliers, or between suppliers and third parties, lack standardization.

Monitoring and vulnerability management. While many IDS solutions have been proposed, OEMs have been reluctant to adopt them, primarily due to implementation costs and real-time performance issues [142]. There is a need to extend the validation of proposed IDSs across different vehicle configurations and architectures. Many existing IDS solutions are designed for CAN networks, and significant changes may be required for CAN-FD. Future research should also focus on recovery strategies for IVNs, after a security breach is detected [101].

The theoretical frameworks for cybersecurity risk assessment (TARA) need also refinement to develop practical models and methods. Future research should aim to enhance risk assessment indicators [107] and create a generic security-driven development lifecycle model [111].

CAVs face multiple conflicts, such as balancing safety with security and cost with usability. These conflicts should be identified in the early design phases to mitigate their impact [112]. The effects of cyberattacks in mixed traffic scenarios involving CAVs and human-driven vehicles need further analysis [52].

Previous studies focused on improving communication security while minimizing the impact on real-time automotive processes [128]. Lightweight secure communication can be a solution to this challenge [129]. Additionally, researchers are exploring hardware solutions to enhance the temporal performance of secure communication.

Testing and Validation. The addition of new cybersecurity features has increased the complexity of testing, particularly in simulation tools and test execution [134]. Some proposed testing solutions have only been validated in small-scale setups with limited ECUs [131]. A significant research gap remains in the development of effective metrics for fuzz testing [132].

Cybersecurity testing often emphasizes automated test case generation to meet requirements. However, penetration testing remains a manual method, and adapting fuzz testing from IT to the automotive sector has potential for improvement, especially in testing efficiency.

Despite significant progress, there remains a limited number of studies addressing cybersecurity throughout the entire automotive lifecycle. Future research is essential given the growing complexity of cyber-physical systems, the expanding attack surfaces, the

increasing demand for data protection, the integration of AI in autonomous vehicles, and the critical importance of supply chain security and regulatory compliance.

Author Contributions: Conceptualization, C.V.K. and A.P.; methodology, A.P.; validation, C.V.K.; formal analysis, C.V.K.; investigation, A.P.; resources, C.V.K.; data curation, A.P.; writing—original draft preparation, C.V.K. and A.P.; writing—review and editing, C.V.K. and A.P.; visualization, A.P.; supervision, C.V.K.; project administration, C.V.K.; funding acquisition, C.V.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Lucian Blaga University of Sibiu research grant LBUS-IRG-2022-08.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: This research was supported by the Lucian Blaga University of Sibiu through the research grant LBUS-IRG-2022-08.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Bandur, V.; Selim, G.; Pantelic, V.; Lawford, M. Making the Case for Centralized Automotive E/E Architectures. *IEEE Trans. Veh. Technol.* **2021**, *70*, 1230–1245. [CrossRef]
2. Reinhardt, D.; Kaule, D.; Kucera, M. Achieving a Scalable E/E-Architecture Using AUTOSAR and Virtualization. *SAE Int. J. Passeng. Cars—Electron. Electr. Syst.* **2013**, *6*, 489–497. [CrossRef]
3. Verstegen, A.; Verdult, R.; Bokslag, W. Hitag 2 Hell—Brutally Optimizing Guess-and-Determine Attacks. In Proceedings of the 12th USENIX Workshop on Offensive Technologies, WOOT 2018, Baltimore, MD, USA, 13–14 August 2018.
4. Verdult, R.; Garcia, F.D.; Balasch, J. Gone in 360 Seconds: Hijacking with Hitag2. In Proceedings of the 21st USENIX Security Symposium, Bellevue, WA, USA, 8–10 August 2012.
5. Chen, H.; Liu, J.; Yang, C.F. Design of Intelligent Locks Based on the Triple KeeLoq Algorithm. *Adv. Mech. Eng.* **2016**, *8*. [CrossRef]
6. Miller, C.; Valasek, C. Remote Exploitation of an Unaltered Passenger Vehicle. *Defcon 23* **2015**, *9*, 1–91.
7. Oka, D. *Building Secure Cars: Assuring the Software Development Lifecycle*; John Wiley & Sons: Hoboken, NJ, USA, 2021; ISBN 9781119710745/9781119710783.
8. *SAE J3061*; Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International: Warrendale, PA, USA, 2016.
9. UN-ECE R155—Cyber Security and Cyber Security Management System. Available online: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:L:2021:082:TOC (accessed on 19 September 2024).
10. *ISO/SAE 21434:2021*; Road Vehicles—Cybersecurity Engineering. ISO: Geneva, Switzerland, 2021.
11. *ISO 26262-1:2018*; Road Vehicles—Functional Safety. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/68383.html (accessed on 19 September 2024).
12. Khatun, M.; Wagner, F.; Jung, R.; Glass, M. An Approach of a Safety Management System for Highly Automated Driving System. In Proceedings of the 2021 5th International Conference on System Reliability and Safety (ICSRS 2021), Palermo, Italy, 24–26 November 2021; IEEE: New York, NY, USA, 2021; pp. 222–229.
13. *ISO 21448:2022*; Road Vehicles—Safety of the Intended Functionality. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/77490.html (accessed on 19 September 2024).
14. Macher, G.; Schmittner, C.; Veledar, O.; Brenner, E. ISO/SAE DIS 21434 Automotive Cybersecurity Standard—In a Nutshell. In *Computer Safety, Reliability, and Security. SAFECOMP 2020 Workshops, Proceedings of the International Conference on Computer Safety, Reliability, and Security, Lisbon, Portugal, 15–18 September 2020*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020.
15. Luo, F.; Jiang, Y.; Wang, J.; Li, Z.; Zhang, X. A Framework for Cybersecurity Requirements Management in the Automotive Domain. *Sensors* **2023**, *23*, 4979. [CrossRef] [PubMed]
16. *VOXViewer*; Leiden University: Leiden, The Netherlands, 2024; Available online: https://www.vosviewer.com/ (accessed on 19 September 2024).
17. Wang, P.; Wu, X.; He, X. Modeling and Analyzing Cyberattack Effects on Connected Automated Vehicular Platoons. *Transp. Res. Part C-Emerging Technol.* **2020**, *115*, 102625. [CrossRef]
18. Palaniswamy, B.; Camtepe, S.; Foo, E.; Pieprzyk, J. An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3107–3122. [CrossRef]
19. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity Challenges in Vehicular Communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]

20. Kukkala, V.K.; Thiruloga, S.V.; Pasricha, S. Roadmap for Cybersecurity in Autonomous Vehicles. *IEEE Consum. Electron. Mag.* **2022**, *11*, 13–23. [CrossRef]
21. Abu Elkhail, A.; Refat, R.U.D.; Habre, R.; Hafeez, A.; Bacha, A.; Malik, H. Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses. *IEEE Access* **2021**, *9*, 162401–162437. [CrossRef]
22. Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, I.A. Facts Approach to Address Cybersecurity Issues in Electric Vehicle Battery Systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 11–14 June 2019; IEEE: New York, NY, USA, 2019.
23. Khalid Khan, S.; Shiwakoti, N.; Stasinopoulos, P. A Conceptual System Dynamics Model for Cybersecurity Assessment of Connected and Autonomous Vehicles. *Accid. Anal. Prev.* **2022**, *165*, 106515. [CrossRef] [PubMed]
24. Aldhyani, T.H.H.; Alkahtani, H. Attacks to Automatous Vehicles: A Deep Learning Algorithm for Cybersecurity. *Sensors* **2022**, *22*, 360. [CrossRef] [PubMed]
25. Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of Onboard Charging Systems for Electric Vehicles-Review, Challenges and Countermeasures. *IEEE Access* **2020**, *8*, 226982–226998. [CrossRef]
26. Hafeez, A.; Topolovec, K.; Awad, S. ECU Fingerprinting through Parametric Signal Modeling and Artificial Neural Networks for In-Vehicle Security against Spoofing Attacks. In Proceedings of the 2019 15th International Computer Engineering Conference (ICENCO 2019), Cairo, Egypt, 29–30 December 2019; IEEE: New York, NY, USA, 2019; pp. 29–38.
27. Sabaliauskaite, G.; Bryans, J.; Jadidbonab, H.; Ahmad, F.; Shaikh, S.; Wooderson, P. TOMSAC—Methodology for Trade-off Management between Automotive Safety and Cyber Security. *Comput. Secur.* **2024**, *140*, 103798. [CrossRef]
28. Lo Bello, L.; Mariani, R.; Mubeen, S.; Saponara, S. Recent Advances and Trends in On-Board Embedded and Networked Automotive Systems. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1038–1051. [CrossRef]
29. Sommer, F.; Kriesten, R.; Kargl, F. Survey of Model-Based Security Testing Approaches in the Automotive Domain. *IEEE Access* **2023**, *11*, 55474–55514. [CrossRef]
30. Mahmood, S.; Fouillade, A.; Nguyen, H.N.; Shaikh, S.A. A Model-Based Security Testing Approach for Automotive Over-the-Air Updates. In Proceedings of the 2020 IEEE 13th International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Porto, Portugal, 24–28 October 2020; IEEE: New York, NY, USA, 2020; pp. 6–13.
31. Mahmood, S.; Nguyen, H.N.; Shaikh, S.A. Systematic Threat Assessment and Security Testing of Automotive Over-the-Air (OTA) Updates. *Veh. Commun.* **2022**, *35*, 100468. [CrossRef]
32. Kirk, R.; Nguyen, H.N.; Bryans, J.; Shaikh, S.; Evans, D.; Price, D. Formalising UPTANE in CSP for Security Testing. In Proceedings of the 2021 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C 2021), Hainan, China, 6–10 December 2021; IEEE Computer Soc: Los Alamitos, CA, USA, 2021; pp. 816–824.
33. Kirk, R.; Nguyen, H.N.; Bryans, J.; Shaikh, S.A.; Wartnaby, C. A Formal Framework for Security Testing of Automotive Over-the-Air Update Systems. *J. Log. Algebr. Methods Program.* **2023**, *130*, 100812. [CrossRef]
34. Li, Z.; Jiang, W.; Liu, X.; Tan, K.; Jin, X.; Yang, M. GAN Model Using Field Fuzz Mutation for In-Vehicle CAN Bus Intrusion Detection. *Math. Biosci. Eng.* **2022**, *19*, 6996–7018. [CrossRef]
35. Yang, Y.; Xie, G.; Wang, J.; Zhou, J.; Xia, Z.; Li, R. Intrusion Detection for In-Vehicle Network by Using Single GAN in Connected Vehicles. *J. Circuits Syst. Comput.* **2021**, *30*, 2150007. [CrossRef]
36. Alfardus, A.; Rawat, D.B. Intrusion Detection System for CAN Bus In-Vehicle Network Based on Machine Learning Algorithms. In Proceedings of the 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 1–4 December 2021; Paul, R., Ed.; IEEE: New York, NY, USA, 2021; pp. 944–949.
37. Fraga-Lamas, P.; Fernandez-Carames, T.M. A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry. *IEEE Access* **2019**, *7*, 17578–17598. [CrossRef]
38. Dibaei, M.; Zheng, X.; Xia, Y.; Xu, X.; Jolfaei, A.; Bashir, A.K.; Tariq, U.; Yu, D.; Vasilakos, A. V Investigating the Prospect of Leveraging Blockchain and Machine Learning to Secure Vehicular Networks: A Survey. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 683–700. [CrossRef]
39. Di Francesco Maesa, D.; Mori, P.; Ricci, L. A Blockchain Based Approach for the Definition of Auditable Access Control Systems. *Comput. Secur.* **2019**, *84*, 93–119. [CrossRef]
40. Jiang, T.; Fang, H.; Wang, H. Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis. *IEEE Internet Things J.* **2019**, *6*, 4640–4649. [CrossRef]
41. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
42. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, H.A.; Di, J.; Li, Q.; Lee, Y. An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. *IEEE J. Emerg. Sel. Top. POWER Electron.* **2022**, *10*, 1270–1281. [CrossRef]
43. Salek, M.S.; Khan, S.M.; Rahman, M.; Deng, H.-W.; Islam, M.; Khan, Z.; Chowdhury, M.; Shue, M. A Review on Cybersecurity of Cloud Computing for Supporting Connected Vehicle Applications. *IEEE Internet Things J.* **2022**, *9*, 8250–8268. [CrossRef]
44. Xu, X.J.; Tatge, L.; Xu, X.L.; Liu, Y. Blockchain Applications in the Supply Chain Management in German Automotive Industry. *Prod. Plan. Control* **2024**, *35*, 917–931. [CrossRef]
45. Yassin, A.M.; Aslan, H.K.; Halim, I.T.A. Smart Automotive Diagnostic and Performance Analysis Using Blockchain Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 32. [CrossRef]

46. Rajapaksha, S.; Kalutarage, H.; Al-Kadri, M.O.; Petrovski, A.; Madzudzo, G.; Cheah, M. AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Comput. Surv.* **2023**, *55*, 237. [CrossRef]
47. Zang, M.; Yan, Y. Machine Learning-Based Intrusion Detection System for Big Data Analytics in Vanet. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-SPRING), Virtual Event, 25 April–19 May 2021; IEEE: New York, NY, USA, 2021.
48. Bari, B.S.; Yelamarthi, K.; Ghafoor, S. Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study. *Sensors* **2023**, *23*, 3610. [CrossRef] [PubMed]
49. Suwwan, R.; Alkafri, S.; Elsadek, L.; Afifi, K.; Zualkernan, I.; Aloul, F. Intrusion Detection for CAN Using Deep Learning Techniques. In Proceedings of the International Conference on Applied Cyber Security (ACS) 2021, Dubai, United Arab Emirates, 13–14 November 2021; Hassen, H.R., Batatia, H., Eds.; Springer International Publishing AG: Cham, Switzerland, 2022; Volume 378, pp. 13–19.
50. Al-Jarrah, O.Y.; El Haloui, K.; Dianati, M.; Maple, C. A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks. *IEEE Open J. Veh. Technol.* **2023**, *4*, 271–280. [CrossRef]
51. Stang, M.; Sommer, M.; Kraus, D.; Sax, E.; Machinery, A.C. Improving the Validation of Automotive Self-Learning Systems through the Synergy of Scenario-Based Testing and Metamorphic Relations. In Proceedings of the IEEE/ACM 10th International Conference on BIG DATA Computing, Applications and Technologies BDCAT, Messina, Italy, 4–7 December 2023.
52. Lee, C.W.; Madnick, S. Cybersafety Approach to Cybersecurity Analysis and Mitigation for Mobility-as-a-Service and Internet of Vehicles. *Electronics* **2021**, *10*, 1220. [CrossRef]
53. Viadero-Monasterio, F.; Nguyen, A.T.; Lauber, J.; Boada, M.J.L.; Boada, B.L. Event-Triggered Robust Path Tracking Control Considering Roll Stability Under Network-Induced Delays for Autonomous Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 14743–14756. [CrossRef]
54. AUTOSAR. AUTomotive Open System ARchitecture (AUTOSAR). Available online: https://www.autosar.org/ (accessed on 19 September 2024).
55. AUTOSAR. Specification of Secure Onboard Communication—CP Release 22-11. Available online: https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_SWS_SecureOnboardCommunication.pdf (accessed on 6 July 2023).
56. AUTOSAR. Specification of Secure Diagnostic. Available online: https://www.autosar.org/fileadmin/standards/R23-11/AP/AUTOSAR_AP_SWS_Diagnostics.pdf (accessed on 1 July 2024).
57. AUTOSAR. Specification of Intrusion Detection System Manager. Available online: https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_SWS_IntrusionDetectionSystemManager.pdf (accessed on 6 July 2023).
58. El-Rewini, Z.; Sadatsharan, K.; Sugunaraj, N.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity Attacks in Vehicular Sensors. *IEEE Sens. J.* **2020**, *20*, 13752–13767. [CrossRef]
59. Prantl, T.; Iffländer, L.; Herrnleben, S.; Engel, S.; Kounev, S.; Krupitzer, C. ACM Performance Impact Analysis of Securing MQTT Using TLS. In Proceedings of the ACM/SPEC International Conference on Performance Engineering (ICPE '21), Virtual Event, 19–23 April 2021; pp. 241–248.
60. Shin, Y.; Jeon, S. MQTree: Secure OTA Protocol Using MQTT and MerkleTree. *Sensors* **2024**, *24*, 1447. [CrossRef]
61. Rodriguez, E.; Otero, B.; Canal, R. A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things. *Sensors* **2023**, *23*, 1252. [CrossRef]
62. Elsisi, M.; Tran, M.-Q. Development of an IoT Architecture Based on a Deep Neural Network against Cyber Attacks for Automated Guided Vehicles. *Sensors* **2021**, *21*, 8467. [CrossRef]
63. *IEEE 802.3bw-2015*; IEEE Standard for Ethernet Amendment 1: Physical Layer Specifications and Management Parameters for 100 Mb/s Operation over a Single Balanced Twisted Pair Cable (100BASE-T1). IEEE Standards Association: Piscataway, NJ, USA, 2016. Available online: https://standards.ieee.org/ieee/802.3bw/5969/ (accessed on 1 July 2024).
64. De Vincenzi, M.; Costantino, G.; Matteucci, I.; Fenzl, F.; Plappert, C.; Rieke, R.; Zelle, D. A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet. *ACM Comput. Surv.* **2024**, *56*, 135. [CrossRef]
65. De Vincenzi, M.; Bodei, C.; Matteucci, I. Securing Automotive Ethernet: Design and Implementation of Security Data Link Solutions. In Proceedings of the 2023 20th ACS/IEEE International Conference on Computer Systems and Applications AICCSA, Giza, Egypt, 4–7 December 2023; IEEE: Piscataway, NJ, USA, 2023.
66. Lo Bello, L.; Patti, G.; Leonardi, L. A Perspective on Ethernet in Automotive Communications—Current Status and Future Trends. *Appl. Sci.* **2023**, *13*, 1278. [CrossRef]
67. Benyahya, M.; Collen, A.; Kechagia, S.; Nijdam, N.A. Automated City Shuttles: Mapping the Key Challenges in Cybersecurity, Privacy and Standards to Future Developments. *Comput. Secur.* **2022**, *122*, 102904. [CrossRef]
68. Wan, Z.; Zhou, Y.; Ren, K. Zk-AuthFeed: Protecting Data Feed to Smart Contracts with Authenticated Zero Knowledge Proof. *IEEE Trans. Dependable Secur. Comput.* **2023**, *20*, 1335–1347. [CrossRef]
69. Pape, S.; Syed-Winkler, S.; Garcia, A.M.; Chah, B.; Bkakria, A.; Hiller, M.; Walcher, T.; Lombard, A.; Abbas-Turki, A.; Yaich, R. A Systematic Approach for Automotive Privacy Management. In Proceedings of the 7th ACM Computer Science in Cars Symposium CSCS, Darmstadt, Germany, 5 December 2023.
70. Kong, Q.L.; Lu, R.X.; Yin, F.; Cui, S.G. Blockchain-Based Privacy-Preserving Driver Monitoring for MaaS in the Vehicular IoT. *IEEE Trans. Veh. Technol.* **2021**, *70*, 3788–3799. [CrossRef]

71. *ISO 26262-1:2011*; Road Vehicles—Functional Safety. ISO: Geneva, Switzerland, 2018. Available online: https://www.iso.org/standard/43464.html (accessed on 1 July 2024).
72. AUTOSAR Overview of Functional Safety Measures in AUTOSAR. Available online: https://www.autosar.org/fileadmin/standards/R22-11/CP/AUTOSAR_EXP_FunctionalSafetyMeasures.pdf (accessed on 1 July 2024).
73. VDA QMC Working Group 13/Automotive SIG. Automotive SPICE 3.1 The Process Reference and Assessment Model. Available online: http://vda-qmc.de/wp-content/uploads/2023/02/Automotive_SPICE_PAM_31_EN.pdf (accessed on 1 July 2024).
74. Manufacturing Standards Committee. *TR 68: Autonomous Vehicles—Part 1: Basic Behaviour*, 1st ed.; Enterprise: Singapore, 2019; ISBN 978-981-48-3558-9.
75. *ISO/TR 4804:2020*; Road Vehicles—Safety and Cybersecurity for Automated Driving Systems—Design, Verification and Validation. ISO: Geneva, Switzerland, 2020. Available online: https://www.iso.org/standard/80363.html (accessed on 1 July 2024).
76. SAE International Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. *SAE Int. J. Connect. Autom. Veh.* **2021**, 129. [CrossRef]
77. VDA QMC Project Group 13 Automotive SPICE Process Reference and Assessment Model for Cybersecurity Engineering. Available online: http://vda-qmc.de/wp-content/uploads/2023/02/Automotive_SPICE_for_Cybersecurity_EN.pdf (accessed on 1 July 2024).
78. UN-ECE UN Regulation No. 156—Software Update and Software Update Management System. Available online: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update (accessed on 1 July 2024).
79. UNECE UN Regulation No. 157—Automated Lane Keeping Systems (ALKS). Available online: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks (accessed on 1 July 2024).
80. AUTOSAR AUTOSAR Explanation of Security Overview. Available online: https://www.autosar.org/fileadmin/standards/R22-11/FO/AUTOSAR_EXP_SecurityOverview.pdf (accessed on 1 July 2024).
81. *ISO/PAS 5112:2022*; Road Vehicles—Guidelines for Auditing Cybersecurity Engineering. ISO: Geneva, Switzerland, 2022. Available online: https://www.iso.org/standard/80840.html (accessed on 1 July 2024).
82. *ISO 24089:2023*; Road Vehicles—Software Update Engineering. ISO: Geneva, Switzerland, 2023. Available online: https://www.iso.org/standard/77796.html (accessed on 1 July 2024).
83. Skoglund, M.; Warg, F.; Sangchoolie, B. In Search of Synergies in a Multi-Concern Development Lifecycle: Safety and Cybersecurity. In Proceedings of the Computer Safety, Reliability, and Security, Safecomp, Vasteras, Sweden, 19–21 September 2018; Gallina, B., Skavhaug, A., Schoitsch, E., Bitsch, F., Eds.; SPRINGER International Publishing AG: Cham, Switzerland, 2018; Volume 11094, pp. 302–313.
84. Skoglund, M.; Warg, F.; Hansson, H.; Punnekkat, S. Synchronisation of an Automotive Multi-Concern Development Process. In Proceedings of the Computer Safety, Reliability, and Security (SAFECOMP 2021), York, UK, 7 September 2021; Habli, I., Sujan, M., Gerasimou, S., Schoitsch, E., Bitsch, F., Eds.; Springer International Publishing AG: Cham, Switzerland, 2021; Volume 12853, pp. 63–75.
85. Schwarzl, C.; Marko, N.; Martin, H.; Expósito Jiménez, V.; Castella Triginer, J.; Winkler, B.; Bramberger, R. Safety and Security Co-Engineering for Highly Automated Vehicles. *Elektrotech. Inf.* **2021**, *138*, 469–479. [CrossRef]
86. Schmittner, C.; Macher, G.; Shaaban, A.; Stolfa, S.; Stolfa, J.; Plucar, J.; Spanyik, M.; Salamun, A.; Messnarz, R.; Ekert, D.; et al. Automotive Cybersecurity Standards—Relation and Overview. In Proceedings of the Communications in Computer and Information Science, Turku, Finland, 10 September 2019.
87. Cheng, B.H.C.; Doherty, B.; Polanco, N.; Pasco, M. Security Patterns for Automotive Systems. In Proceedings of the 2019 ACM/IEEE 22ND International Conference on Model Driven Engineering Languages and Systems Companion (Models-C 2019), Munich, Germany, 15–20 September 2019; Burgueno, L., Pretschner, A., Voss, S., Chaudron, M., Kienzle, J., Volter, M., Gerard, S., Zahedi, M., Rensink, A., Polack, F., et al., Eds.; IEEE: Los Alamitos, CA, USA, 2019; pp. 54–63.
88. Dobaj, J.; Macher, G.; Ekert, D.; Riel, A.; Messnarz, R. Towards a Security-Driven Automotive Development Lifecycle. *J. Softw. Evol. Process* **2021**, *35*, e2407. [CrossRef]
89. Schober, T.; Griessnig, G. Cybersecurity Regulations and Standards in the Automotive Domain. In *Systems, Software and Services Process Improvement, Proceedings of the 29th European Conference, EuroSPI 2022, Salzburg, Austria, 31 August–2 September 2022*; Springer: Cham, Switzerland, 2022; Volume 1646, CCIS; pp. 530–539.
90. Lee, T.-Y.; Lin, I.-A.; Liao, R.-H. Design of a FlexRay/Ethernet Gateway and Security Mechanism for In-Vehicle Networks. *Sensors* **2020**, *20*, 641. [CrossRef]
91. Jo, W.; Kim, S.; Kim, H.; Shin, Y.; Shon, T. Automatic Whitelist Generation System for Ethernet Based In-Vehicle Network. *Comput. Ind.* **2022**, *142*, 103735. [CrossRef]
92. Shrivastwa, R.-R.; Bouakka, Z.; Perianin, T.; Dislaire, F.; Gaudron, T.; Souissi, Y.; Karray, K.; Guilley, S. An Embedded AI-Based Smart Intrusion Detection System for Edge-to-Cloud Systems. In Proceedings of the Cryptography, Codes and Cyber Security, First Proceedings of the International Conference, I4CS 2022, Casablanca, Morocco, 27–28 October 2022; Nitaj, A., Zkik, K., Eds.; Springer International Publishing AG: Cham, Switzerland, 2022; Volume 1747, pp. 20–39.
93. Casino, M.; Coppola, S.; De Santo, M.; Pascale, F.; Santonicola, E. Embedded Intrusion Detection System for Detecting Attacks over CAN-BUS. In Proceedings of the 2019 4th International Conference on System Reliability and Safety (ICSRS 2019), Rome, Italy, 20–22 November 2022; IEEE: New York, NY, USA, 2019; pp. 136–141.

94. Aliwa, E.; Rana, O.; Perera, C.; Burnap, P. Cyberattacks and Countermeasures for In-Vehicle Networks. *ACM Comput. Surv.* **2021**, *54*, 21. [CrossRef]
95. Bhatia, R.; Kumar, V.; Serag, K.; Celik, Z.B.; Payer, M.; Xu, D. Evading Voltage-Based Intrusion Detection on Automotive CAN. In Proceedings of the Network and Distributed System Security (NDSS) Symposium, Virtual Event, 21–25 February 2021.
96. Cheng, P.; Han, M.; Li, A.; Zhang, F. STC-IDS: Spatial–Temporal Correlation Feature Analyzing Based Intrusion Detection System for Intelligent Connected Vehicles. *Int. J. Intell. Syst.* **2022**, *37*, 953–9561. [CrossRef]
97. Vitale, C.; Piperigkos, N.; Laoudias, C.; Ellinas, G.; Casademont, J.; Escrig, J.; Kloukiniotis, A.; Lalos, A.S.; Moustakas, K.; Diaz Rodriguez, R.; et al. CARAMEL: Results on a Secure Architecture for Connected and Autonomous Vehicles Detecting GPS Spoofing Attacks. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 115. [CrossRef]
98. Wu, W.; Li, R.; Xie, G.; An, J.; Bai, Y.; Zhou, J.; Li, K. A Survey of Intrusion Detection for In-Vehicle Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 919–933. [CrossRef]
99. Sharma, S.; Kaul, A. A Survey on Intrusion Detection Systems and Honeypot Based Proactive Security Mechanisms in VANETs and VANET Cloud. *Veh. Commun.* **2018**, *12*, 138–164. [CrossRef]
100. Al-Jarrah, O.Y.; Maple, C.; Dianati, M.; Oxtoby, D.; Mouzakitis, A. Intrusion Detection Systems for Intra-Vehicle Networks: A Review. *IEEE Access* **2019**, *7*, 21266–21289. [CrossRef]
101. Olufowobi, H.; Young, C.; Zambreno, J.; Bloom, G. SAIDuCANT: Specification-Based Automotive Intrusion Detection Using Controller Area Network (CAN) Timing. *IEEE Trans. Veh. Technol.* **2020**, *69*, 1484–1494. [CrossRef]
102. Mansourian, P.; Zhang, N.; Jaekel, A.; Kneppers, M. Deep Learning-Based Anomaly Detection for Connected Autonomous Vehicles Using Spatiotemporal Information. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 16006–16017. [CrossRef]
103. Ed Huang, S.; Feng, Y.; Liu, H.X. A Data-Driven Method for Falsified Vehicle Trajectory Identification by Anomaly Detection. *Transp. Res. Part C-Emerging Technol.* **2021**, *128*, 103196. [CrossRef]
104. Park, S.; Choi, J.-Y. Malware Detection in Self-Driving Vehicles Using Machine Learning Algorithms. *J. Adv. Transp.* **2020**, *1*, 3035741. [CrossRef]
105. Rumez, M.; Grimm, D.; Kriesten, R.; Sax, E. An Overview of Automotive Service-Oriented Architectures and Implications for Security Countermeasures. *IEEE Access* **2020**, *8*, 221852–221870. [CrossRef]
106. Hofbauer, J.; Gomez, K.; Hof, H.-J. From SOC to VSOC: Transferring Key Requirements for Efficient Vehicle Security Operations In Proceedings of 21th escar Europe: The World's Leading Automotive Cyber Security, Hamburg, Germany, 15–16 November 2023.
107. Fenzl, F.; Plappert, C.; Rieke, R.; Zelle, D.; Costantino, G.; De Vincenzi, M.; Matteucci, I. Collaborative Security Patterns for Automotive Electrical/Electronic Architectures. In *Advanced Sciences and Technologies for Security Applications*; Springer International Publishing: Cham, Switzerland, 2023.
108. Barletta, V.S.; Caivano, D.; Catalano, C.; De Vincentiis, M.; Machinery, A.C. Quantum-Based Automotive Threat Intelligence and Countermeasures. In Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering EASE, Salerno, Italy, 18–21 June 2024; pp. 548–554.
109. Wang, Y.; Wang, Y.; Qin, H.; Ji, H.; Zhang, Y.; Wang, J. A Systematic Risk Assessment Framework of Automotive Cybersecurity. *Automot. Innov.* **2021**, *4*, 253–261. [CrossRef]
110. Zhang, Y.; Shi, P.; Dong, C.; Liu, Y.; Shao, X.; Ma, C. Test and Evaluation System For Automotive Cybersecurity. In Proceedings of the 2018 21st IEEE International Conference on Computational Science and Engineering (CSE 2018), Bucharest, Romania, 29–91 October 2018; Pop, F., Negru, C., GonzalezVelez, H., Rak, J., Eds.; IEEE: New York, NY, USA, 2018; pp. 201–207.
111. Dobaj, J.; Ekert, D.; Stolfa, J.; Stolfa, S.; Macher, G.; Messnarz, R. Cybersecurity Threat Analysis, Risk Assessment and Design Patterns for Automotive Networked Embedded Systems: A Case Study. *J. Univers. Comput. Sci.* **2021**, *27*, 830–849. [CrossRef]
112. Khatun, M.; Glass, M.; Jung, R. An Approach of Scenario-Based Threat Analysis and Risk Assessment Over-the-Air Updates for an Autonomous Vehicle. In Proceedings of the 2021 7th International Conference on Automation, Robotics and Applications (ICARA 2021), Virtual Event, 4–6 February 2021; IEEE: New York, NY, USA, 2021; pp. 122–127.
113. ISO/IEC JTC 1/SC 27 ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. Available online: https://www.iso.org/standard/27001 (accessed on 1 July 2024).
114. ENX Association Trusted Information Security Assessment Exchange. Available online: https://enx.com/en-us/tisax/ (accessed on 1 July 2024).
115. Królikowski, T.; Ubowska, A. TISAX—Optimization of IT Risk Management in the Automotive Industry. *Procedia Comput. Sci.* **2021**, *192*, 4259–4268. [CrossRef]
116. Taylor, S.J.; Ahmad, F.; Nguyen, H.N.; Shaikh, S.A.; Evans, D.; Price, D. Vehicular Platoon Communication: Cybersecurity Threats and Open Challenges. In Proceedings of the 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-W 2021), Taipei, Taiwan, 21–24 June 2021; IEEE Computer Society: Los Alamitos, CA, USA, 2021; pp. 19–26.
117. Viadero-Monasterio, F.; Meléendez-Useros, M.; Jiméenez-Salas, M.; Boada, B.L.; Boada, M.J.L. What Are the Most Influential Factors in a Vehicle Platoon? In Proceedings of the IEEE Conference on Evolving and Adaptative Intelligent Systems, Madrid, Spain, 23–24 May 2024; pp. 375–381.

118. Khattak, Z.H.; Smith, B.L.; Fontaine, M.D. Impact of Cyberattacks on Safety and Stability of Connected and Automated Vehicle Platoons under Lane Changes. *Accid. Anal. Prev.* **2021**, *150*, 105861. [CrossRef]
119. Malik, S.; Bandi, P.; Sun, W. An Experimental Study of Denial of Service Attack Against Platoon of Smart Vehicles. In Proceedings of the 2021 Fourth International Conference on Connected and Autonomous Driving (METROCAD 2021), Detroit, MI, USA, 28–29 April 2021; IEEE Computer Soc: Los Alamitos, CA, USA, 2021.
120. Wang, Y.; Zhang, R.; Masoud, N.; Liu, H.X. Anomaly Detection and String Stability Analysis in Connected Automated Vehicular Platoons. *Transp. Res. Part C-Emerging Technol.* **2023**, *151*, 104114. [CrossRef]
121. Zhao, C.; Gill, J.S.; Pisu, P.; Comert, G. Detection of False Data Injection Attack in Connected and Automated Vehicles via Cloud-Based Sandboxing. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 9078–9088. [CrossRef]
122. Bella, G.; Biondi, P.; Costantino, G.; Matteucci, I. TOUCAN A ProTocol tO SecUre Controller Area Network. In Proceedings of the ACM Workshop on Automotive Cybersecurity (AUTOSEC'19), Richardson, TX, USA, 27 March 2019; Assoc Computing Machinery: New York, NY, USA, 2019; pp. 3–8.
123. Biondi, P.; Bella, G.; Costantino, G.; Matteucci, I. Demo: Implementing CAN Bus Security by TOUCAN. In Proceedings of the 2019 the Twentieth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC'19), Catania, Italy, 2–5 July 2019; ASSOC Computing Machinery: NEW YORK, NY, USA, 2019; pp. 399–400.
124. Wu, W.; Kurachi, R.; Zeng, G.; Matsubara, Y.; Takada, H.; Li, R.; Li, K. IDH-CAN: A Hardware-Based ID Hopping CAN Mechanism with Enhanced Security for Automotive Real-Time Applications. *IEEE Access* **2018**, *6*, 54607–54623. [CrossRef]
125. Palaniswamy, B.; Ansari, K.; Reddy, A.G.; Das, A.K.; Shetty, S. Robust Certificateless Authentication Protocol for the SAE J1939 Commercial Vehicles Bus. *IEEE Trans. Veh. Technol.* **2023**, *72*, 4493–4509. [CrossRef]
126. Jadoon, A.K.; Wang, L.; Li, T.; Zia, M.A. Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wirel. Commun. Mob. Comput.* **2018**, *1*, 1640167. [CrossRef]
127. Bella, G.; Biondi, P.; Costantino, G.; Matteucci, I. CINNAMON: A Module for AUTOSAR Secure Onboard Communication. In Proceedings of the 2020 16th European Dependable Computing Conference (EDCC 2020), Munich, Germany, 7–10 September 2020; IEEE Computer Soc: Los Alamitos, CA, USA, 2020; pp. 103–110.
128. Bella, G.; Biondi, P.; Costantino, G.; Matteucci, I. Designing and Implementing an AUTOSAR-Based Basic Software Module for Enhanced Security. *Comput. Netw.* **2022**, *218*, 109377. [CrossRef]
129. Groza, B.; Murvay, S.; Van Herrewege, A.; Verbauwhede, I. LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks. *ACM Trans. Embed. Comput. Syst.* **2017**, *16*, 90. [CrossRef]
130. Fowler, D.S.; Cheah, M.; Shaikh, S.A.; Bryans, J. Towards A Testbed for Automotive Cybersecurity. In Proceedings of the 2017 10th IEEE International Conference on Software Testing, Verification and Validation (ICST), Tokyo, Japan, 19–17 March 2017; IEEE: New York, NY, USA, 2017; pp. 540–541.
131. Oruganti, P.S.; Appel, M.; Ahmed, Q. Hardware-in-Loop Based Automotive Embedded Systems Cybersecurity Evaluation Testbed. In Proceedings of the ACM Workshop on Automotive Cybersecurity (AUTOSEC'19), Richardson, TX, USA, 27 March 2019; Assoc Computing Machinery: New York, NY, USA, 2019; pp. 41–44.
132. Fowler, D.S.; Bryans, J.; Cheah, M.; Wooderson, P.; Shaikh, S.A. A Method for Constructing Automotive Cybersecurity Tests, a CAN Fuzz Testing Example. In Proceedings of the 2019 Companion of the 19th IEEE International Conference on Software Quality, Reliability and Security (QRS-C 2019), Sofia, Bulgaria, 22–26 July 2019; IEEE Computer Soc: Los Alamitos, CA, USA, 2019; pp. 1–8.
133. Anistoroaei, A.; Groza, B.; Murvay, P.-S.; Gurban, H. Security Analysis of Vehicle Instrument Clusters by Automatic Fuzzing and Image Acquisition. In Proceedings of the 2022 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR 2022), Cluj-Napoca, Romania, 19–21 May 2022; IEEE: New York, NY, USA, 2022; pp. 13–18.
134. Marksteiner, S.; Bronfman, S.; Wolf, M.; Lazebnik, E. Using Cyber Digital Twins for Automated Automotive Cybersecurity Testing. In Proceedings of the 2021 IEEE European Symposium on Security and Privacy Workshops (EUROS\&PW 2021), Vienna, Austria, 6–10 September 2021; IEEE: New York, NY, USA, 2021; pp. 123–128.
135. Cui, L.; Hu, J.; Park, B.B.; Bujanovic, P. Development of a Simulation Platform for Safety Impact Analysis Considering Vehicle Dynamics, Sensor Errors, and Communication Latencies: Assessing Cooperative Adaptive Cruise Control under Cyber Attack. *Transp. Res. Part C-Emerging Technol.* **2018**, *97*, 1–22. [CrossRef]
136. Marksteiner, S.; Marko, N.; Smulders, A.; Karagiannis, S.; Stahl, F.; Hamazaryan, H.; Schlick, R.; Kraxberger, S.; Vasenev, A. A Process to Facilitate Automated Automotive Cybersecurity Testing. In Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-SPRING), Virtual Event, 25–28 April 2021; IEEE: New York, NY, USA, 2021.
137. Zhang, H.C.; Wang, J.; Wang, Y.J.; Li, M.F.; Song, J.H.; Liu, Z.L. ICVTest: A Practical Black-Box Penetration Testing Framework for Evaluating Cybersecurity of Intelligent Connected Vehicles. *Appl. Sci.* **2024**, *14*, 204. [CrossRef]
138. Wang, Y.; Masoud, N.; Khojandi, A. Real-Time Sensor Anomaly Detection and Recovery in Connected Automated Vehicle Sensors. *IEEE Trans. Intell. Transp. Syst.* **2021**, *22*, 1411–1421. [CrossRef]
139. Toker, O.; Alsweiss, S. Design of a Cyberattack Resilient 77 GHz Automotive Radar Sensor. *Electronics* **2020**, *9*, 573. [CrossRef]
140. Kengo Oka, D. *Building Secure Cars*; John Wiley & Sons: Hoboken, NJ, USA, 2021.

141. Kamal, M.; Kyrkou, C.; Piperigkos, N.; Papandreou, A.; Kloukiniotis, A.; Casademont, J.; Porras Mateu, N.; Baos Castillo, D.; Diaz Rodriguez, R.; Gregorio Durante, N.; et al. A Comprehensive Solution for Securing Connected and Autonomous Vehicles. In Proceedings of the 2022 Design, Automation & Test in Europe Conference & Exhibition (DATE 2022), Antwerp, Belgium, 14–23 March 2022; Bolchini, C., Verbauwhede, I., Vatajelu, I., Eds.; IEEE: New York, NY, USA, 2022; pp. 790–795.
142. Baldini, G. On the Application of Entropy Measures with Sliding Window for Intrusion Detection in Automotive In-Vehicle Networks. *Entropy* **2020**, *22*, 1044. [CrossRef]