

# Cybersecurity Challenges of Autonomous Systems

Mohammad Hamad\*, Christian Prehofer†, Mikael Asplund‡,  
Tobias Löhr§, Lucas Bublitz§, Alexander Zeh¶, Mridula Singh||, Sebastian Steinhorst\*

\*Technical University of Munich, Germany

†DENSO Automotive, Germany

‡Linköping University, Sweden

§P3 automotive GmbH, Germany

¶Infineon Technologies, Germany

||CISPA Helmholtz Center for Information Security, Germany

**Abstract**—With the recent dramatic increase in performance of artificial intelligence and related computing systems, together with advanced sensing, connectivity, and technological platforms, autonomous systems are poised to enter many application domains such as transportation and manufacturing. As autonomy increases, the risks of cybersecurity threats are equally rising, requiring the development of sophisticated methods on all layers of autonomous systems architectures. Therefore, this paper systematically introduces cybersecurity challenges ranging from the physical layer to the system of systems layer defining the collaboration of autonomous systems. Without loss of generality, autonomous vehicles are used to highlight current developments, illustrating which efforts are necessary to achieve secure and safe autonomous systems. Our discussions are comprehensively highlighting which research domains require further investigation and offer promising opportunities to contribute to mitigating cybersecurity challenges of autonomous systems.

**Index Terms**—Autonomous Systems, Autonomous Vehicles, Security.

## I. INTRODUCTION

Autonomous Systems are increasingly entering our everyday lives. While we are seeing a transition from Advanced Driver Assistance Systems (ADAS) towards autonomous driving in vehicles, we also witness autonomous functionality emerging in many other domains, from passenger trains and Unmanned Aerial Vehicles (AEVs) to production systems and robots in Industry 4.0 applications. The transition to autonomous systems is gaining speed due to the recent leap in Artificial Intelligence (AI) and Machine Learning (ML) capabilities.

What separates autonomous systems from conventional automated systems, which act within a predefined set of tasks, is their capability to independently make decisions and, therefore, dynamically adapt to unforeseen environmental changes. In the discussed domains, autonomous systems exist in a Cyber-Physical Systems (CPSs) context, interacting with the physical world. Compared to autonomous systems that may also purely reside in the cyber domain, such as trading of goods or in finance, the cyber-physical interaction of the autonomous systems in the focus of this paper can potentially pose physical safety risks to humans and infrastructure.

While developing safe autonomous systems is a challenge on its own, as there is no human operator to compensate for malfunction in real time, this also renders autonomous systems particularly critical from a cybersecurity perspective.

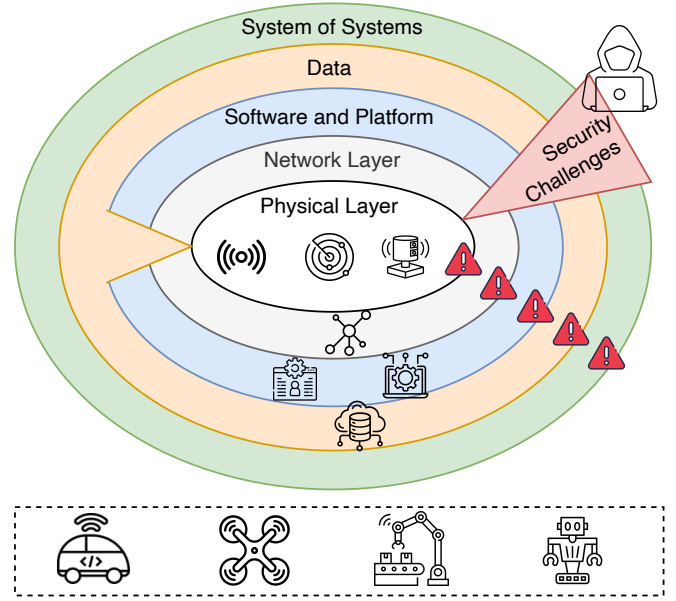


Fig. 1. Layered architecture of an autonomous system, showing the physical, network, software and platform, data, and system of systems layers.

Cybersecurity ensures that no unauthorized access to a system happens, which may otherwise lead to fatal outcomes in the case of unprevented malicious attacks.

In this paper, we will investigate the cybersecurity challenges of autonomous systems on several abstraction layers (see Fig. 1), choosing the autonomous vehicle domain as our target. In the vehicular domain, autonomy features are already in the market, and they are expected to develop quickly and continuously and will have a large market penetration. Illustrating such cybersecurity challenges spans from low-level physical layer features for secure in-vehicle and intra-vehicle communication to privacy, data integrity, and identity management. All such challenges equally exist in other application domains for autonomous systems. However, the autonomous vehicle domain serves as an ideal example for systems gradually entering the domain of autonomy, adding challenges from the integration of legacy technology with advanced paradigms required for achieving autonomy.

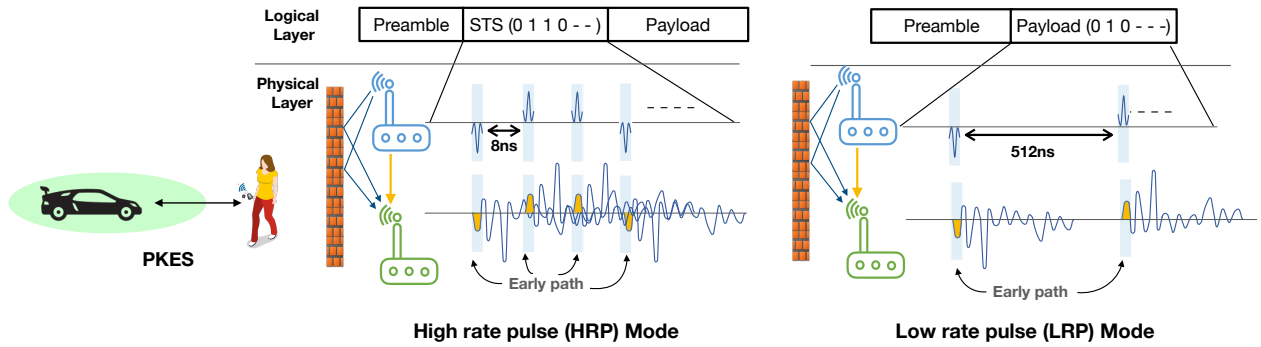


Fig. 2. UWB Ranging mode for the Passive Keyless Entry and Start System.

## II. PHYSICAL LAYER

The integration of sensors in modern autonomous systems is rapidly transforming the way we approach their safety and security. For example, in autonomous and smart vehicles, sensors are essential for many applications. From collision avoidance and lane departure warnings to driver monitoring and theft prevention, these systems help drivers stay safer and more aware of their surroundings. As sensor technology continues to evolve, we can expect even more sophisticated features to make driving more convenient and significantly reduce the risk of accidents and vehicle theft. However, when using insecure sensors, these systems inadvertently create new vulnerabilities. Many of these security vulnerabilities cannot be fixed at the data layer and require physical layer integrity checks to enable secure sensing. In the following section, we will use the Passive Keyless Entry and Start System (PKES) as an example to illustrate the importance of physical layer security and how the lessons learned from designing secure PKES can be applied to other sensors and communication systems.

### A. Passive Keyless Entry and Start System

Modern vehicles rely on PKES to unlock, lock, or start the car without user interaction, as long as the key fob is within close proximity. PKESs also enhance security in scenarios such as a user forgetting to manually lock the car or a jamming attack. However, the ease of manipulating PKES motivates the theft of vehicles.<sup>1</sup> The vulnerabilities in the PKES were revealed by researchers more than a decade ago [1]. However, designing a secure alternative is complicated as an attacker can exploit both data-layer and physical-layer weaknesses to manipulate the distance. Data-layer attacks can often be prevented by implementing strong cryptographic primitives. However, physical-layer attacks are of significant concern because they can be executed independently of any higher-layer cryptographic primitive [2].

Researchers, manufacturers, IEEE standards, FiRa Consortium, and the Car Connectivity Consortium collectively work to find a secure PKES that works under real-world scenarios. Two-way Time-of-flight measurement using Ultrawideband (UWB) signals has emerged as the secure solution. IEEE 802.15.4z

has defined two modes of operation, based on Low Rate Pulse (LRP) and High Rate Pulse (HRP), as shown in Figure 2 [3]. The HRP Mode uses pseudorandomly generated Secure Training Sequences (STS) for time-of-flight measurement. However, if cross-correlation is naively applied to compute the time-of-arrival on these STS sequences, it opens the door to distance manipulation attacks. Therefore, it is critical to implement integrity checks at the receiver to ensure the validity of the time-of-flight measurement [4]. On the other hand, LRP mode enables security by combining Distance Bounding at the logical layer, and distance commitment at the physical layer [5]. The LRP mode can enhance both performance and security by leveraging techniques such as pulse randomization and signal-level integrity checks [6], [7]. The HRP and LRP modes offer secure PKES solutions by applying cryptographic operations and integrity checks at the physical layer, underscoring the importance of securing physical layer designs [4], [6], [8].

### B. Collision Avoidance Systems

Collision avoidance systems rely on inputs from multiple sensors such as LiDAR, RADAR, cameras, and 5G's Positioning Reference Signal (PRS) to detect obstacles and take preventive actions, ensuring safer navigation and reducing accident risks. However, these sensors are vulnerable to spoofing attacks, which can either create false obstacles or obscure real ones, potentially leading to collisions with other vehicles or pedestrians [9]–[12]. To prevent such collisions with other vehicles, accurate, fast, and secure distance measurements using two-way ranging systems can be employed [13]. For this application, the physical layer must be resilient against both distance reduction (as in PKES) and distance enlargement attacks. The latter is particularly dangerous, as an attacker within the communication range can prevent detection of other vehicles by disrupting or distorting the legitimate signals, effectively preventing the receiver from correctly identifying them [14]. Recent research indicates that these systems can be safeguarded through integrity checks at the physical layer, using technologies like UWB and 5G, to ensure the accuracy and reliability of distance measurements even in the presence of adversarial interference [12], [13]. By implementing such measures, it is possible to build more secure collision avoidance

<sup>1</sup><http://www.bbc.com/news/uk-england-birmingham-42132689>

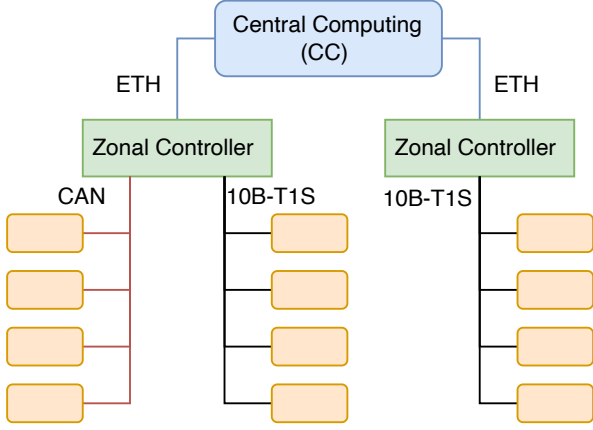


Fig. 3. Simplified IVN model for CAN and 10BASE-T1s (10B-T1s) endpoints.

systems that can withstand malicious attempts to manipulate sensor data and improve overall vehicle safety.

### III. NETWORK LAYER

Above the physical layer, the network layer plays a crucial role in connecting various components of an autonomous system, ensuring seamless data flow and communication between them. However, the network layer in autonomous systems is often heterogeneous and complex, making it a potential target for various types of cyberattacks. For example, Fig. 3 illustrates a simplified In-Vehicle Network (IVN) architecture. This architecture typically consists of a central computing unit, multiple zones, and several electronic control units (ECUs), also known as endpoints, which are connected within the zones. The zone controllers are connected to the central computing unit via point-to-point Ethernet, while the endpoints are connected either via Controller Area Network (CAN) or 10B-T1S (single-pair automotive Ethernet). Automotive Ethernet (AE) is a modified version of standard Ethernet to fulfill the automotive industry's requirements. Unlike traditional Ethernet, AE uses a single unshielded twisted pair (UTP) cable, allowing transmission and reception on the same pair to simplify wiring while ensuring high-speed, full-duplex data transfer. In addition to AE's bandwidth advantages, 10 BASE-T1S [15] can operate in multidrop mode, which decreases cabling weight. In addition to AE, CAN, CAN FD, or CAN XL (the latest version of CAN) are utilized. CAN XL is developed to be backward compatible to classic CAN [16] and CAN FD [17] in the sense that it can be used on the same bus in mixed applications, i.e., some nodes on the bus communicate CAN XL while some nodes still use Classic CAN or CAN FD.

A key vulnerability of the CAN bus is the lack of authentication, which allows attackers to impersonate safety-critical ECUs, such as the engine control unit, by using legitimate ECU identifiers. This can enable masquerade attacks, where attackers gain control of the vehicle's internal systems. In addition, the increasing use of wireless technologies like Bluetooth for communication with ECUs raises the risk of attacks, which could even lead to remote attacks [21]–[23].

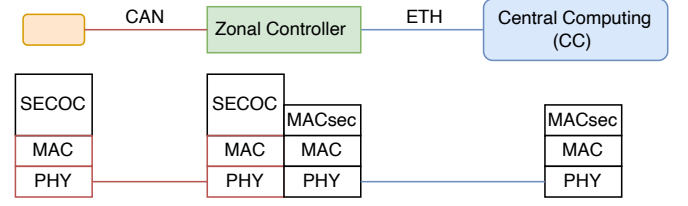


Fig. 4. Scenario S1: AUTOSAR's SECOC and MACsec. Solid lines illustrate a physical connection, while dashed lines show logical ones.

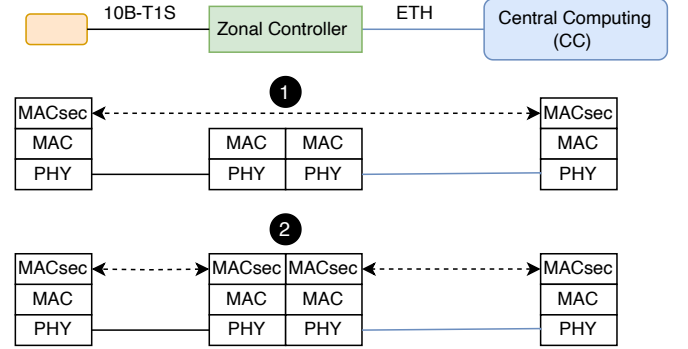


Fig. 5. Scenario S2: IEEE802.1AE MACsec deployed in end-to-end ❶ or point-to-point ❷.

#### A. Challenges for Security Protocol Stacks of IVN

As presented in Table I, various security protocols can be employed to secure different types of links within the IVN. For instance, the Ethernet connection between the zone controller and the central computing unit can be secured using multiple protocols, including IEEE 802.1AE MACsec [20]. Controller Area Network Security (CANsec) is a working draft proposed by CiA [19], inspired by MACsec for Ethernet [20], and is designed to enhance the security of CAN communication by providing message authenticity and confidentiality. Additionally, AUTOSAR's Secure Onboard Communication (SECOC) [18] offers a standardized approach to securing communication over both CAN and Ethernet networks.

The various communication scenarios involving different ECUs across different zones or with the central computing unit introduce unique combinations of security protocol stacks, leading to various challenges. For the *first scenario (S1)*, shown in Fig. 4, an ECU communicates via CAN with the zone controller and the central computing unit. The security pro-

TABLE I  
EXISTING SECURITY PROTOCOLS FOR IN-VEHICLE COMMUNICATION.

ISO-OSI	Ethernet	CAN XL
7 - Application	SECOC [18]	SECOC [18]
4 - Transport	(D)TLS	
3 - Network	IPsec	CANsec [19]
2 - Data Link	MACsec [20]	

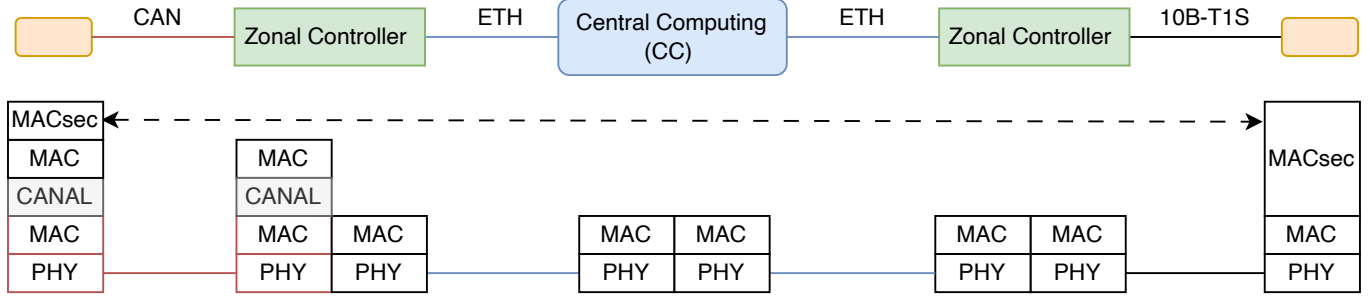


Fig. 6. Scenario S3: CAN Adaption Layer (CANAL) using MACsec end-to-end.

protocol stack includes AUTOSAR's SECOC [18], which secures communication between the ECU and the zone controller, and MACsec, which secures the link between the zone controller and the central computing unit. The key disadvantages of S1 include the software load imposed by the relatively "heavy" AUTOSAR stack, its authentication-only security capabilities, and the requirement for (session) key storage within the zone controller.

The *second scenario*, shown in Fig. 5, is a homogeneous Ethernet-only network, where MACsec [20] can be deployed end-to-end ① or point-to-point ②. For both variants, the availability of MACsec's existing hardware support is advantageous. Deploying MACsec end-to-end avoids key storage in the intermediate zone controller and security processing. However, communication mechanisms restrict the modification of header information.

Inspired by the ATM Adaptation Layer (AAL) [24], the CAN Adaption Layer (CANAL), illustrated in the *third scenario* (S3) shown in Fig. 6, enables the deployment of higher-layer Ethernet protocols and MACsec on CAN nodes. CANAL supports end-to-end deployment but is not limited to it. Ideally, this allows the usage of IEEE802.1AE MACsec [20] and MACsec Key Agreement (MKA) [25], as well as alternative key agreement protocols, including security associations between CAN and 10B-T1S endpoints.

#### IV. SOFTWARE AND PLATFORM LAYER

Software plays a crucial role in autonomous systems, with many functionalities being implemented through software. In autonomous vehicles, the trend is toward Software-Defined Vehicles (SDVs), where most functions are realized via software [26]. The traditional way of automotive architecture was that software was specifically tailored for specific hardware in a vehicle in order to optimize hardware demands. For instance, the software to manage the engine would work only on specific hardware for engine control, which has suitable computing hardware and interfaces. While this provided hardware-oriented modularity of a system, it led to a large number of computing devices, in some cases more than one hundred. In contrast to that, the SDV aims to ensure that the software can be replaced, updated, or reconfigured after production and features an agnostic hardware platform that can run different software.

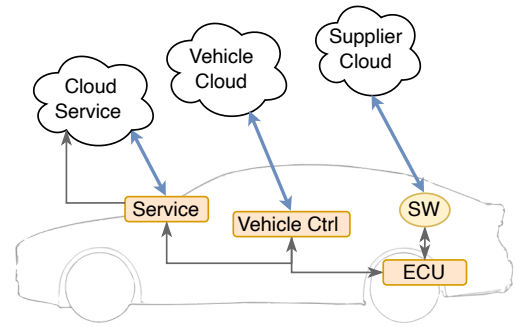


Fig. 7. Software-defined vehicle with cloud connections and trust relations.

This flexibility leads to several new challenges, e.g. [27], and in particular regarding security [26], [28].

One of the critical requirements in SDVs is to ensure that trust relationships are more flexible and dynamic [29]. This includes hardware, in-vehicle software components, as well as cloud software or other locally connected (V2X) devices. These trust relationships include the following:

- System integrity for reconfiguration: ensuring that only trusted software and firmware can run on the vehicle's systems is essential to prevent malware and unauthorized modifications.
- Data security and authentication: protecting sensitive data transmitted between the vehicle and external systems is critical to prevent unauthorized access and data breaches.
- Interoperable services and multiple trust anchors exist due to different stakeholders of software, hardware, and cloud components.

Self-sovereign identity (SSI) [30] provides a new approach for identities and digitally signed documents based on asynchronous encryption. In simple terms, this can be seen as asynchronous cryptography with different trust anchors stored in an immutable, publicly available storage. This is important as setting up a distributed, interoperable public key infrastructure is challenging. One example of such an infrastructure is the authentication of web services with TLS certificates [31], which can be issued by different trust anchors. In fact, SSI can use this infrastructure using one instance of SSI technology, called

did:web<sup>2</sup>. In the following, we highlight three use cases and argue that SSI technology is a very suitable solution.

#### A. Component Reconfiguration and Trust Setup

A main feature of SDVs is the flexibility of software placement and updates. Due to reliability and safety requirements, it must be ensured that the hardware fits the current software and also that the software is approved for it. This can be achieved by mutual authentication to avoid compatibility issues and potential attacks in the reconfiguration process. This follows the zero-trust security approach [29]. For instance, if some control unit fails, software may have to be placed on other components, and it needs to be ensured that the software and new hardware are fully compatible. Similarly, in the case of software updates or hardware replacements, authentication is essential.

This is illustrated in Fig. 7, which shows communications and example trust relationships. Note that ECU stands for electronic control unit, and SW and Service are considered software components. The main point here is that hardware, vehicle software, and cloud components often originate from different companies that may want to check the authenticity of a piece of software by themselves. This creates the need for a distributed authentication and certification infrastructure with multiple trust anchors, hence leading to an SSI solution.

#### B. Data Integrity and Protection

Following the above use case, an ensuing problem is to authenticate data. A simple example are crash reports, logs, or scenario data, which are needed to analyze errors or unexpected behaviors. This gets increasingly complex as some functions, like assisted driving, are difficult to specify precisely for all possible scenarios. As such solutions are typically composed of hardware and software components of different vendors, it is important to ensure the authenticity of such data. Similarly, data protection is important as vehicles host an abundance of privacy-sensitive data like driving records or user settings, plus sensitive data like service credentials, as in the use case below. For all of these cases, it is necessary to protect data, both by encryption and by digital signatures, for authentication. In complex scenarios, such signed documents need to be linked, e.g., to describe a complex scenario with different hardware and software components. The same problem occurs when communicating with cloud services. Here, security becomes even more important as the attack surface increases significantly when communicating with multiple entities over communication infrastructure. The same is true for connected services, as discussed in the section below.

#### C. Distributed Charging Services

Another interesting use case is the charging of electric vehicles, ideally by plug-and-charge, where the vehicle negotiates a charging contract when the charging cable is plugged in [32]. The challenge here is that we have many charging station operators, different vehicle types, and many possible charging service providers. There are dedicated protocols like

OCPI and ISO-15118 to facilitate this process [32], [33]. In these protocols, we need authentication between the vehicle and its charging contact provider with the charging station operator, which is like roaming in mobile networks if both are not the same company. While these existing protocols, like ISO-15118, build up a complex public key infrastructure, it was shown in [32] that this can also be done by using SSI technology. The main advantage is that SSI is a use-case-independent technology that can be extended or used similarly for many other use cases. For instance, other services like parking or highway fees have similar interoperability issues due to many players in the market. For these, SSI could build a common basis, as investigated in the MoveID Project<sup>3</sup>. Another advantage of SSI solutions is the support for offline scenarios when the Internet is unavailable or disturbed, as investigated in [34].

### V. DATA LAYER

In the last days of 2024, a major data breach affecting mostly electric vehicles from the Volkswagen group was announced by German news outlet Der Spiegel [35] and the ethical hacking group Chaos Computer Club. The data breach, which affects around 800,000 customers across the world, includes personal information and detailed geolocation data. Apart from the significant privacy violations, the breach also has clear national security implications as the data includes information about cars driven by persons likely associated with intelligence services.

In this section, we take a closer look at this incident and discuss the potential implications and lessons learned we can draw for automotive security at large. At first glance, a data breach (which should only affect confidentiality) might be dismissed as less relevant to the security of autonomous systems, where we are primarily concerned with safety-related security violations. However, we argue that this and other similar incidents must be taken seriously and that the current approach to automotive security is not sufficient to meet future security challenges.

#### A. Brief Summary of the Incident

The German automotive maker Volkswagen, with brands that include VW, Skoda, Audi, and Seat, announced a new strategy in 2021 named "New Auto". The focus of this strategy was to transform Volkswagen into a software-driven mobility provider. At the heart of this transformation lies the subsidiary CARIAD, which was created to drive the development of new data-driven business models, new mobility services, and automated driving. This is also the company responsible for the telemetry data breach discussed here. Figure 8 shows a slightly simplified illustration of the potential attack kill chain, which is based on the presentation given at the 2024 Chaos Communication Congress [36].

The data affected by the breach was stored in an Amazon cloud service controlled and operated by CARIAD. Information about the possible vulnerability was revealed by an unnamed whistleblower to Der Spiegel and the ethical hacking group Chaos Computer Club. We refer to the people who investigated

<sup>2</sup><https://w3c-ccg.github.io/did-method-web/>

<sup>3</sup><https://moveid.org/>



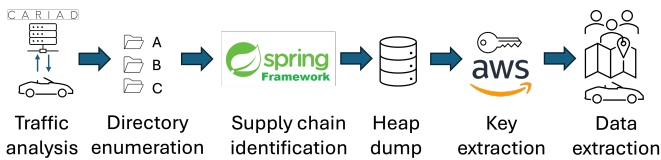


Fig. 8. CARIAD data extraction kill chain.

this breach as analysts. The first indication of a potential problem was the web API of the telemetry interface that allowed a directory enumeration attack (performed with the tool gobuster). Having access to the directory structure of the web service, the analysts were able to determine that the web framework Spring was being used.

Spring has a debugging feature called Heap Dump that essentially allows a complete memory dump of the JVM application at some checkpoint. Such data should obviously not remain in a production system, but unfortunately, this is exactly what happened in the case of the CARIAD telemetry application. Even worse, the memory dump (which can be easily analyzed with tools made for debugging) revealed cryptographic keys to access additional AWS services. In particular, having access to these master keys, the system provided an API to generate access keys for any user in the system.

The analysts could now access 9.5 terabytes of vehicle telemetry data, which includes personal information (name, email), information about the vehicle, and most problematic geolocation data going back several months in time.

### B. Takeaways for Automotive Security

This data breach is not unique and not too surprising. Both Toyota<sup>4</sup> and Volvo<sup>5</sup> experienced recent data breaches and a 2023 report from the Mozilla foundation rated the privacy policies of 25 automakers as "terrible" [37]. Still, there are some lessons we can learn from this incident for automotive cybersecurity at large.

1) *Lack of incidents is not an indication of security:* First, the discovery of this particular problem was due to luck and a single individual who decided to make this information public. If this had not happened, it might never have become publicly known. At the same time, we do not know who else has had knowledge of this data. We have seen many cases of public data breaches where hackers threaten to make information public and, in some cases, go through with the threat [38]. However, depending on the motivations of the attackers, it might be beneficial to never reveal themselves at all or to keep hidden until some point when they strike with maximum impact. Therefore, we should assume that there are a number of compromised systems out there that we do not know about.

<sup>4</sup><https://www.bleepingcomputer.com/news/security/toyota-car-location-data-of-2-million-customers-exposed-for-ten-years/>

<sup>5</sup><https://www.media.volvocars.com/global/en-gb/media/pressreleases/292817/notice-of-cyber-security-breach-by-third-party-1>

2) *Correlation between security measures and security:* A second takeaway from this incident is that security is hard. This might seem like a trivial observation, and it is generally well-known that this is the case [39]. However, as we are now creating more and more capable and complex systems, such as autonomous systems, this is worth reiterating. So, what does it mean to say that security is hard in this case? When reading about the incident, there are details in the kill chain that are surprising. Making a complete memory dump accessible by a simple HTTP GET request is one such example.

However, there is nothing to indicate that CARIAD paid any less attention to cybersecurity than other actors. Maybe future investigations will reveal internal issues with the management of cybersecurity, but as far as we know, they are no worse at this than many other similar software development companies. The company stated as early as 2021 that "security is our top priority"<sup>6</sup>. In March 2023, the security company SecurityCompass released a case study<sup>7</sup> where they had collaborated with CARIAD to ensure that the developer organization had proper cybersecurity training and awareness.

So, how can a company that seems to care about cybersecurity make such a seemingly trivial mistake? The issue is that it is only trivial once you know about it. In fact, you can employ a number of security measures without necessarily finding this particular problem.

3) *Increasing attack surfaces:* Finally, it is clear that attack surfaces for automotive systems are increasing as more and more vehicles are being connected to various cloud services. Some of these services might seem spurious and created just to collect more data about customers, whereas others provide clear customer benefits. In either case, the fact that most new vehicles are now essentially connected to the Internet means that we have to assume that they will also be the target of cyberattacks.

Telemetry applications have been widely deployed by automotive companies, and it is likely that we will see an expansion in the use cases and uptake of this technology. Electric vehicles, in particular, seem to be associated with new software stacks and increased connectivity. Similar to the security issues we have seen for telemetry, electric vehicle charging infrastructure brings its own security problems [40], [41].

### C. Call for a Rethinking of Design Philosophy

To wrap up this section, we turn back to autonomous vehicles and what we need to do to ensure their cybersecurity properties. Clearly, the automotive domain will be no more protected from attacks than other domains, such as the electric grid, telecommunication, and aviation, which have all been subject to severe attacks in the last few years. So far, we have been lucky in the sense that incidents have been mostly related to privacy, but we should not count on this being true in the future.

So, what can we learn from past incidents when it comes to increasing the security of these emerging systems? The answer

<sup>6</sup><https://cariad.technology/de/en/news/stories/automotive-cybersecurity.html>

<sup>7</sup><https://www.securitycompass.com/case-studies/cariad-inc-partners-with-security-compass/>

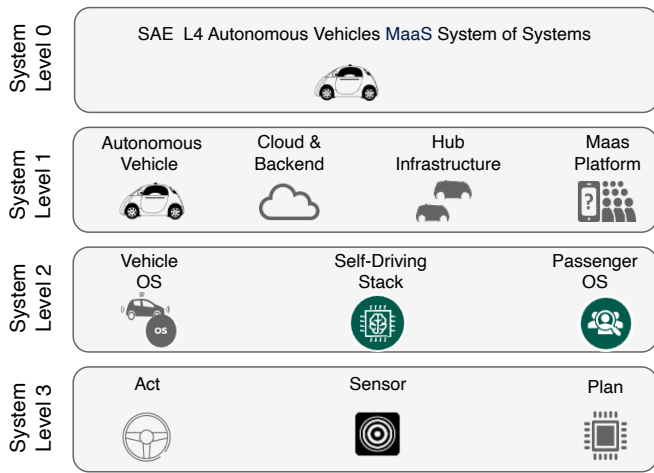


Fig. 9. Autonomous Vehicles System of Systems for Mobility as a Service.

is to *reduce attack surfaces*. That is, instead of creating more and more complexity and then adding increasingly complex defense mechanisms, we need to start aiming for simple designs. By taking away features and options that are not strictly needed, we enable a better understanding of possible misuse and even the ability to reason formally about security properties.

## VI. SYSTEM OF SYSTEMS LAYER

The deployment of SAE Level 4 (L4) autonomous Vehicles for Mobility as a Service (MaaS) ride-hailing services in the US, Europe, and China has underscored the significant technological advancements achieved in autonomous driving over the past few years. Unlike traditional automotive solutions, these systems feature a complex architecture comprising a retrofitted vehicle operating system, a self-driving stack, and a passenger operating system, which acts as the gateway to the MaaS platform and manages passenger interactions within the car. This leads to an interconnected, interdependent, and multimodal architecture; however, it also engenders new challenges in ensuring cybersecurity due to an expanded lifecycle perspective that extends from the development phase through the operational phase to the end of service for autonomous vehicles.

The AD MaaS ecosystem consists of multiple layers, lacking a direct relationship between clients and original equipment manufacturers (OEMs) and having no clear responsibility for the technology. The AD MaaS stakeholders, critical for deploying autonomous vehicles, have increased and now include hub operators, Mobility as a Service platform operators, backend system operators, vehicle manufacturers, and others [42].

In contrast to passenger car manufacturers, AD MaaS vehicles operate under a distributed, shared hierarchy of responsibility, lacking clear roles, unified integration, and release processes, which results in a more network-oriented architecture. Due to the relevance of safety and security in achieving safe and secure operations, ensuring product compliance with current and upcoming regulations, and mitigating product liability, new

paradigms are required for managing this partnership-oriented platform approach [43].

### A. Autonomous Vehicle MaaS System of Systems

As shown in Fig. 9, the layers of the system-of-systems architecture for the autonomous mobility platform are schematically derived across multiple levels. At *system level 0*, the entire platform is considered as a single entity. Moving to *system level 1*, the architecture consists of distinct components, including autonomous vehicles, backend infrastructure, hub and fleet management, and the mobility service platform. At *system level 2*, the approach further extends to the internal subsystems of the vehicle. For autonomous vehicles, the system-of-systems framework at level 2 characterizes key internal subsystems, including the vehicle operating system, which handles safety-critical functions such as steering, braking, and lighting, as well as comfort functions like climate control and seating, which are considered the *system level 3*. Additionally, the passenger operating system provides interfaces to the mobility platform and facilitates passenger monitoring. Finally, the self-driving system encompasses perception, planning, and control modules.

### B. Cybersecurity System of Systems Challenges

One of the critical challenges of such an AD MaaS system of systems lies in establishing a unified communication, functional, and security framework across these isolated subsystems, which often include non-standardized vehicle interfaces. Despite their distinct functionalities, these subsystems are built on shared onboard computing hardware and a standardized software architecture, all of which rely on backend connectivity through various telematics gateways. From a security perspective, this system-of-systems architecture introduces a broad attack surface due to multiple physical and digital entry points, including sensor interfaces, in-vehicle functions, and telematics connections [44].

Another challenge is addressing critical requirements related to safety and efficiency. The heterogeneous nature of underlying technologies, combined with unsynchronized development and integration processes, introduces substantial vulnerabilities. Increasing regulatory demands further complicate the landscape, revealing additional cybersecurity gaps [45]. The disjointed development and validation processes present several challenges. Many autonomous vehicle MaaS platforms retrofit legacy vehicles—such as in partnerships between Waymo and Chrysler—rather than developing integrated systems from scratch. As a result, development milestones for a cohesive solution become fragmented, leading to inconsistent validation efforts. Furthermore, ambiguous roles and responsibilities within large-scale value networks hinder comprehensive risk assessments, robust threat analyses, and effective traceability of cybersecurity requirements throughout the system lifecycle.

Furthermore, the integration of multiple protocols and technologies introduces additional vulnerabilities. A security breach in one subsystem can trigger a cascade of risks, potentially compromising the entire system of systems. Real-time data, which is crucial for autonomous vehicle operations, is highly susceptible to spoofing and denial-of-service (DoS) attacks,

potentially affecting decision-making, jeopardizing safety, and even causing system failures or accidents.

Also, the involvement of third-party software and hardware integrations further complicates cybersecurity efforts. Many of these components come with inherent risks, including both known and unknown vulnerabilities that could compromise critical functions. Additionally, legacy infrastructure—while still essential to many systems—often lacks modern security features, leaving it vulnerable to exploitation.

Finally, the reliance on AI and ML systems introduces additional risks [46], making them susceptible to adversarial attacks. These attacks can manipulate decision-making algorithms, potentially leading to unsafe behaviors or even catastrophic failures.

## VII. COLLABORATION LAYER

As discussed in the previous section, autonomous systems are typically part of a larger ecosystem where multiple autonomous entities coexist, interact, and exchange information. For example, sensor data (e.g., from cameras and LiDAR) collected by one autonomous vehicle can be shared with other autonomous vehicles to achieve collaborative perception [47], enhancing overall efficiency and safety. However, such collaboration introduces significant conceptual and security concerns that must be carefully addressed.

### A. Competing Collaborative Systems

As different autonomous systems share the same environment, they will also share the same resources (e.g., roads for autonomous vehicles). Assuming these systems will “honestly” collaborate is overly simplistic. For example, autonomous vehicles need to and will have a level of self-interest; otherwise, they may end up in deadlock situations (e.g., different cars stuck at an intersection, each waiting for the other to proceed). Consequently, while these systems may collaborate, they will also compete for resources, as each system is programmed to optimize resource usage and maximize efficiency. This can result in behaviors that, although legal, may seem unethical from a human driver’s perspective (e.g., trying to get through traffic jams as quickly as possible or blocking other vehicles to reach a destination in a shorter time). Considering this, an optimization battle could arise among different agents or software providers, each aiming to implement such “intelligence” in their algorithms to ensure safe but efficient collaboration while simultaneously competing for resources. Such a situation would require strict national and international legislation to ensure that competing collaborative systems adhere to common directives.

### B. Secure and Trustworthy Collaborative Systems

Many security issues can arise when autonomous systems collaborate and share sensor information. The first challenge arises from *external malicious attackers* who could intercept collaborative communications and inject false or harmful information. Although addressing this issue might seem straightforward by implementing secure communication protocols between autonomous systems, the interoperability and compatibility of various security standards and requirements across different nodes pose significant challenges.

However, even if secure communication is achieved, a more complex and difficult challenge arises when an autonomous system itself acts maliciously by injecting false or harmful data (i.e., *an internal attacker*) [48]. In such cases, secure communication alone is insufficient, as the malicious node may possess legitimate credentials. Addressing this threat requires more comprehensive intrusion detection methods, which rely on redundant sources of information to validate received data. Unfortunately, such redundancy may not always be available, making detection and mitigation even more challenging.

## VIII. REMARKS ON SECURING AUTONOMOUS SYSTEMS

The complex nature of autonomous systems, such as autonomous vehicles, requires a comprehensive security solution. These systems can be seen as a single entity made up of multiple interconnected subsystems, each with its own functional layers. Additionally, they operate within a larger ecosystem, which itself functions as a higher-level system of systems. This intricate and layered structure demands a security approach that is both holistic and multi-layered. Such a solution must ensure the ability to detect attacks at their earliest stages and respond effectively across the multiple levels of the system of systems, as well as within the layers of each individual system. It is critical to recognize that security measures implemented at different layers will not be effective unless they are designed to work in synergy with one another. Each layer may require a distinct security solution tailored to its specific needs.

For instance, at the physical and sensor layer, specialized solutions are needed to address the unique characteristics of various smart sensors, such as cameras [49], LiDAR [50], and other sensing technologies. These solutions should account for their specific vulnerabilities and requirements. At the network layer, implementing robust security protocols like MACsec or IPsec is essential. However, additional defensive measures, such as intrusion detection systems that monitor network activity or ensure the integrity of components across different platforms, may also be necessary [51]–[53]. Moreover, the widespread distribution of data within such systems necessitates controlled access mechanisms that allow data owners to retain the rights to grant or restrict access [54]. Achieving such access control is particularly challenging in ecosystems involving multiple owners and stakeholders [55]. Finally, the high connectivity and interdependency of these systems require them to be self-resilient and capable of proactive measures to prevent attacks [56], including coordinated attacks at a larger scale.

## IX. CONCLUSION

The introduction of autonomous systems, such as autonomous vehicles, is gaining momentum. At the same time, their increasing adoption raises critical security challenges that must be identified and addressed, as potential attacks could have drastic impacts. This paper systematically discusses relevant security challenges in such autonomous systems by examining their key layers: the physical, network, software and platform, and data layers. Additionally, viewing these systems as part of a larger, interconnected system introduces further security challenges discussed in our paper. Eventually, the goal of



enabling different autonomous systems to collaborate opens the door to security challenges stemming from the emergence of several interacting autonomous systems. Our presentation of these challenges aims not only to highlight the complexity of securing autonomous systems but also to stimulate new directions for research and development.

#### ACKNOWLEDGEMENTS

This paper is supported in part by the Federal Ministry for Economic Affairs and Climate Action (BMWK) as part of the MoveID project on the basis of a decision by the German Bundestag. In addition, this work is supported by the European Union-funded project CyberSecDome (Agreement No.: 101120779).

#### REFERENCES

- [1] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," *IACR Cryptol. ePrint Arch.*, vol. 2010, p. 332, 2010.
- [2] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.
- [3] "802.15.4z - standard for low-rate wireless networks amendment: Enhanced high rate pulse (hrp) and low rate pulse (lrp) ultra wide-band (uwb) physical layers (phys) and associated ranging techniques," <https://standards.ieee.org/develop/project/802.15.4z.html>. [Online; Accessed 7. August 2018].
- [4] X. Luo, C. Kalkanli, H. Zhou, P. Zhan, and M. Cohen, "Secure ranging with ieee 802.15.4z hrp uwb," in *2024 IEEE Symposium on Security and Privacy (SP)*, p. 2794–2811, IEEE, May 2024.
- [5] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "Uwb rapid-bit-exchange system for distance bounding," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '15, pp. 2:1–2:12, ACM, 2015.
- [6] M. Singh, P. Leu, and S. Capkun, "UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks," in *NDSS*, 2019.
- [7] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Čapkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," in *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 500–516, 2020.
- [8] M. Singh, M. Roeschlin, E. Zalzala, P. Leu, and S. Čapkun, "Security analysis of ieee 802.15.4z/hrp uwb time-of-flight distance measurement," in *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, (New York, NY, USA), pp. 227–237, Association for Computing Machinery, 2021.
- [9] R. R. Vennam, I. K. Jain, K. Bansal, J. Orozco, P. Shukla, A. Ranganathan, and D. Bharadia, "mmspoof: Resilient spoofing of automotive millimeter-wave radars using reflect array," in *2023 IEEE Symposium on Security and Privacy (SP)*, pp. 1807–1821, IEEE, 2023.
- [10] R. S. Hallyburton, Y. Liu, Y. Cao, Z. M. Mao, and M. Pajic, "Security analysis of Camera-LiDAR fusion against Black-Box attacks on autonomous vehicles," in *31st USENIX Security Symposium (USENIX Security 22)*, (Boston, MA), pp. 1903–1920, USENIX Association, Aug. 2022.
- [11] Y. Cao, S. H. Bhupathiraju, P. Naghavi, T. Sugawara, Z. M. Mao, and S. Rampazzi, "You can't see me: Physical removal attacks on lidar-based autonomous vehicles driving frameworks," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023.
- [12] M. Singh, M. Roeschlin, A. Ranganathan, and S. Capkun, "V-Range: Enabling Secure Ranging in 5G Wireless Networks," in *Network and Distributed System Security Symposium (NDSS)*, 2022.
- [13] M. Singh, P. Leu, A. Abdou, and S. Capkun, "UWB-ED: Distance enlargement attack detection in Ultra-Wideband," in *28th USENIX Security Symposium (USENIX Security 19)*, (Santa Clara, CA), pp. 73–88, USENIX Association, Aug. 2019.
- [14] N. O. Tippenhauer, K. B. Rasmussen, and S. Čapkun, "Physical-layer Integrity for Wireless Messages," *Computer Networks*, vol. 109, no. P1, pp. 31–38, 2016.
- [15] IEEE, "IEEE Standard for Ethernet - Amendment 5: Physical Layer Specifications and Management Parameters for 10 Mb/s Operation and Associated Power Delivery over a Single Balanced Pair of Conductors," *IEEE Std 802.3cg-2019*, Feb. 2020.
- [16] Specification, "CAN Specification 2.0 (1991, 1997)," *Robert Bosch GmbH*, 1991.
- [17] Specification, "Bosch CAN FD Specification Version 1.0 (2012)," *Robert Bosch GmbH*, 2012.
- [18] AUTOSAR, "Specification of Secure Onboard Communication Protocol."
- [19] CiA, "CAN XL Add-on Services - Part 2: Security," Tech. Rep. CiA 613-2 Version 0.0.7, CAN in Automation, 2022.
- [20] IEEE, "IEEE Standard for Local and Metropolitan Area Networks-Media Access Control (MAC) Security," *IEEE Std 802.1AE-2018*, Dec. 2018. Conference Name: IEEE Std 802.1AE-2018 (Revision of IEEE Std 802.1AE-2006).
- [21] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," SEC'11, (USA), USENIX Association, 2011.
- [22] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, no. S 91, 2015.
- [23] R. Baker and I. Martinovic, "Losing the car keys: Wireless {PHY-Layer} insecurity in {EV} charging," in *28th USENIX Security Symposium (USENIX Security 19)*, pp. 407–424, 2019.
- [24] T. Suzuki, "ATM Adaptation Layer Protocol," *IEEE Communications Magazine*, vol. 32, pp. 80–83, Apr. 1994. Conference Name: IEEE Communications Magazine.
- [25] IEEE, "IEEE Standard for Local and Metropolitan Area Networks-Port-Based Network Access Control," *IEEE Std 802.1X-2020*, Feb. 2020. Conference Name: IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018).
- [26] D. Püllen, *Holistic Security Engineering for Software-Defined Vehicles*. PhD thesis, Universität Passau, 2024.
- [27] Z. Liu, W. Zhang, and F. Zhao, "Impact, challenges and prospect of software-defined vehicles," *Automotive Innovation*, vol. 5, no. 2, pp. 180–194, 2022.
- [28] M. De Vincenzi, M. D. Pesé, C. Bodei, I. Matteucci, R. R. Brooks, M. Hasan, A. Saracino, M. Hamad, and S. Steinhart, "Contextualizing security and privacy of software-defined vehicles: State of the art and industry perspectives," *arXiv preprint arXiv:2411.10612*, 2024.
- [29] M. E. Shipman, N. Millwater, K. Owens, and S. Smith, "A zero trust architecture for automotive networks," tech. rep., SAE Technical Paper, 2024.
- [30] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, M. Sabadello, and J. Holt, "Decentralized identifiers (dids) v1. 0," *Draft Community Group Report*, 2020.
- [31] E. Rescorla and T. Dierks, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug. 2008.
- [32] A. Kailus, D. Kern, and C. Krauß, "Self-sovereign identity for electric vehicle charging," in *International Conference on Applied Cryptography and Network Security*, pp. 137–162, Springer, 2024.
- [33] D. Richter and J. Anke, "Exploring potential impacts of self-sovereign identity on smart service systems: an analysis of electric vehicle charging services," in *Business Information Systems*, pp. 105–116, 2021.
- [34] S. Chenna and C. Prehofer, "Combining verifiable credentials and blockchain tokens for traceable and offline token operations," in *2023 IEEE 9th World Forum on Internet of Things (WF-IoT)*, pp. 1–6, IEEE, 2023.
- [35] D. Spiegel, "Volkswagen-konzern datenleck: Wir wissen, wo dein auto steht," January 2024. Accessed: 2025-01-27.
- [36] M. Kreil and Flüpke, "Wir wissen wo dein auto steht: Volksdaten von volkswagen." Presentation at the 38th Chaos Communication Congress 27–30 December, CCH, Hamburg, <https://media.ccc.de/v/38c3-wir-wissen-wo-dein-auto-steht-volksdaten-von-volkswagen>.
- [37] J. Caltrider, M. Rykov, and Z. MacDonald, "It's official: Cars are the worst product category we have ever reviewed for privacy," September 2023. Accessed: 2025-01-27.
- [38] H. R. Nikkhah and V. Grover, "An empirical investigation of company response to data breaches," *MIS Quarterly*, vol. 46, no. 4, 2022.
- [39] R. Anderson, "Why information security is hard - an economic perspective," in *Seventeenth Annual Computer Security Applications Conference*, pp. 358–365, 2001.

- [40] R. Plaka, M. Asplund, and S. Nadjm-Tehrani, "Vulnerability analysis of an electric vehicle charging ecosystem," in *Critical Information Infrastructures Security* (S. Pickl, B. Hämmerli, P. Mattila, and A. Sevilano, eds.), (Cham), pp. 155–173, Springer Nature Switzerland, 2024.
- [41] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Chargeprint: A framework for internet-scale discovery and security analysis of ev charging management systems," in *Network and Distributed System Security (NDSS)*, 2023.
- [42] M. G. Augusto, J. Maas, M. Kosch, M. Henke, T. Küster, F. Straube, and S. Albayrak, "Autonomous van and robot last-mile logistics platform: A reference architecture and proof of concept implementation," *Logistics*, vol. 9, no. 1, pp. 1–15, 2025.
- [43] I. Durlík, T. Müller, E. Kostecka, Z. Zwierzewicz, and A. Łobodzińska, "Cybersecurity in autonomous vehicles—are we ready for the challenge?," *Electronics*, vol. 13, no. 13, p. 2654, 2024.
- [44] B. A. Tanaji and S. Roychowdhury, "A survey of cybersecurity challenges and mitigation techniques for connected and autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, 2024.
- [45] M. Girdhar, J. Hong, and J. Moore, "Cybersecurity of autonomous vehicles: A systematic literature review of adversarial attacks and defense models," *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 417–437, 2023.
- [46] M. Hamad and S. Steinhorst, "Security challenges in autonomous systems design," *arXiv preprint arXiv:2312.00018*, 2023.
- [47] Y. Han, H. Zhang, H. Li, Y. Jin, C. Lang, and Y. Li, "Collaborative perception in autonomous driving: Methods, datasets, and challenges," *IEEE Intelligent Transportation Systems Magazine*, vol. 15, no. 6, pp. 131–151, 2023.
- [48] Q. Zhang, S. Jin, R. Zhu, J. Sun, X. Zhang, Q. A. Chen, and Z. M. Mao, "On data fabrication in collaborative vehicular perception: Attacks and countermeasures," in *33rd USENIX Security Symposium (USENIX Security 24)*, pp. 6309–6326, 2024.
- [49] M. Kühn, M. Hamad, P. MohajerAnsari, M. D. Pesé, and S. Steinhorst, "Sok: Security of the image processing pipeline in autonomous vehicles," *arXiv preprint arXiv:2409.01234*, 2024.
- [50] R. Changalvala and H. Malik, "Lidar data integrity verification for autonomous vehicle," *IEEE Access*, vol. 7, pp. 138018–138031, 2019.
- [51] S. K. Valappil, L. Vogel, M. Hamad, and S. Steinhorst, "Advanced idps architecture for connected and autonomous vehicles," in *2024 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1779–1785, IEEE, 2024.
- [52] M. Kneib, O. Schell, and C. Huth, "EASI: Edge-Based Sender Identification on Resource-Constrained Platforms for Automotive Networks," in *NDSS*, 2020.
- [53] A. Finkenzeller, O. Butowski, E. Regnath, M. Hamad, and S. Steinhorst, "Ptpsec: Securing the precision time protocol against time delay attacks using cyclic path asymmetry analysis," in *IEEE INFOCOM 2024 - IEEE Conference on Computer Communications*, pp. 461–470, 2024.
- [54] M. Hamad, A. Finkenzeller, H. Liu, J. Lauinger, V. Prevelakis, and S. Steinhorst, "Seemqtt: secure end-to-end mqtt-based communication for mobile iot systems using secret sharing and trust delegation," *IEEE Internet of Things Journal*, vol. 10, no. 4, pp. 3384–3406, 2022.
- [55] M. Annabi, A. Zeroual, and N. Messai, "Towards zero trust security in connected vehicles: A comprehensive survey," *Computers & Security*, p. 104018, 2024.
- [56] M. Hamad, A. Finkenzeller, M. Kühn, A. Roberts, O. Maennel, V. Prevelakis, and S. Steinhorst, "React: Autonomous intrusion response system for intelligent vehicles," *Computers & Security*, vol. 145, p. 104008, 2024.