Intelligent Systems Engineering 2023/24

Literature survey: Cybersecurity in Autonomous On-Road Motor Vehicles focusing on connectivity and perception systems

Alberto Paganelli
alberto.paganelli3@studio.unibo.it

December 19, 2024

The rapid development of autonomous vehicles (AVs) introduces transformative potential for modern transportation systems, but it also raises critical concerns regarding cybersecurity. As AVs increasingly rely on complexity, the attack surface for potential threats expands, demanding robust and proactive security measures. This survey aims to provide an overview of current research on security challenges in autonomous vehicles, focusing on key cybersecurity threats, standards, and industry practices. Emphasizing the need for a multi-layered approach to cybersecurity in AVs, integrating secure software development, hardware resilience, and regulatory compliance is essential. Moreover, the survey explores future trends and emerging technologies that could enhance the security of autonomous vehicles helping the development of secure and reliable systems.

Contents

1 Methodology

1.1 Premises

In this review, I aim to provide a comprehensive overview of the research current state on security in autonomous vehicles, in particular autonomous cars. My focus is on the key cybersecurity threats, standards, and industry practices in the field, keeping in mind that the landscape is rapidly evolving. The goal is to identify the most critical challenges and opportunities for future research in this area and underline the importance of a multi-layered approach to cybersecurity in AVs, starting from the design phase. The ethical implications of the technology or the comparison between human-driven and autonomous vehicles in terms of accidents and fatalities will not be covered, also social implications will not be deepened.

1.2 Research Question

Starting from an introduction to the main threats in terms of cybersecurity regarding AV, the review will analyze the main actual opportunities to improve and regulate the security of these systems. After that, the review will focus on the industry standards concluding in the future trends and emerging technologies that could enhance and simplify the security process of AVs. This review address the following research questions:

1. *What are the most significant cybersecurity threats facing autonomous vehicles, and how these threats evolve with advancements in VANETs communications or with the evolution of the perception system of these vehicles?*

2. *What existing standards and regulatory frameworks address cybersecurity by design in autonomous vehicles, and are they enough to effectively tackle current and future security challenges?*

3. *What solutions and practices have been implemented by autonomous vehicle manufacturers, and how do they align with best practices in secure software development and system resilience?*

4. *What future trends and emerging technologies, such as artificial intelligence and blockchain, are being explored to enhance the cybersecurity of autonomous vehicles?*

1.3 Selection Criteria

The selection criteria for the literature review are as follows:

1. *Relevance:* The literature must be directly related to the topic of security in autonomous vehicles, focusing on cybersecurity threats, standards, and industry practices.

2. *Quality:* The literature should be published in reputable journals, conference proceedings, or books, ensuring high academic and technical standards.

3. *Recency:* The literature should be recent (published within the last five years) to reflect the latest developments in the field. Some references can be not recent enough to be included in the last five-year filter, but they are fundamental to understanding the historical context or some specific technology.

4. *Diversity:* The literature should cover a broad range of topics within the field of autonomous vehicle security, including but not limited to threat modeling, risk assessment, secure software development, and hardware security. At the same time, the literature should be representative and inherently connected to the cybersecurity topic.

5. *Accessibility:* The literature should be accessible online or through academic libraries to ensure that it can be reviewed and cited effectively.

1.4 Search Strategy

The search strategy for this review involved a systematic exploration of electronic databases, books, and relevant publications. The following databases were used to identify relevant literature:

1. Google Scholar
2. IEEE Xplore
3. WebOfScience
4. SpringerLink

Multiple searches were conducted, initially to discover in general the state of the art in the field of autonomous vehicles and then to focus on the security aspects. The search terms used included combinations of the following keywords: *autonomous vehicles*, *self-driving cars*, *cybersecurity*, *security threats*, *standards*, *industry practices*, *V2X communication*, *ISO/SAE 21434*, *UNECE WP.29 R155*, *secure software development*, *intrusion detection*, *over-the-air updates*, *artificial intelligence*, *digital twins*, *blockchain*.

Some principal queries were:

1. *autonomous vehicles cybersecurity threats*
2. *autonomous vehicles cybersecurity by design*
3. *autonomous vehicles cybersecurity standards*
4. *autonomous vehicles cybersecurity connectivity*
5. *autonomous vehicles cybersecurity perception sensors*
6. *autonomous vehicles cybersecurity architecture*
7. *autonomous vehicles cybersecurity accidents*

8. *autonomous vehicles cybersecurity V2V, V2I, V2X*
9. *autonomous vehicles cybersecurity future trends*
10. *secure software development lifecycle autonomous vehicle*
11. *autonomous vehicles secure over-the-air*
12. *autonomous vehicles cybersecurity future directions*
13. *autonomous vehicles cybersecurity privacy blockchain*
14. *autonomous vehicles cybersecurity artificial intelligence*

Moreover, some filter was applied to search only recent results, only peer-reviewed articles, and only articles in English. First, the search was conducted on Google Scholar and IEEE Xplore, used like entry points to the other databases. In other cases, instead, a direct search on institutional websites was conducted to find specific standards or reports (e.g. `https://www.sae.org/`, `https://unece.org/wp29-introduction`).

The search strategy aimed to identify a diverse range of sources, including academic papers, conference proceedings, books, and industry reports, to provide a comprehensive overview of research on security in autonomous vehicles. In certain cases, as already mentioned, the limit on the age of the publication was removed to include fundamental works that are not recent but representative of a specific technology or approach (e.g. CAN bus). Moreover, some references are relative to the automotive industry in general, but they are fundamental to understanding the context in which autonomous vehicles are developed.

1.4.1 Phases

The search of papers and documents was conducted in two phases:

1. *General Search:* The initial search aimed to identify the main topics and subtopics related to cybersecurity in autonomous vehicles, helping to understand the current state, main threats and some general aspects of the AVs.
2. *Specific Search:* The second search focused on specific aspects of cybersecurity in autonomous vehicles, such as specific threats, standards, industry practices, techniques, and then future trends.

Every search was conducted using the same base keywords and filters. To ensure consistency and comparability of results across different databases, in particular, the keywords *autonomous vehicles* and *cybersecurity* were always present in the search query to keep the focus on the main topic of the review. Only for the 8 section, a two-year filter was applied to ensure the most recent results but not excluding other works.

The number of citations was also considered but not like a primary filter, favoring instead the quality of the paper and the relevance in terms of cybersecurity of the content. Another important aspect is that social, ethical, and legal implications were not considered, so the papers focused on these aspects were excluded.

1.5 Quality Assessment

The quality assessment of the selected literature has been differentiated based on the type of citation. For books, the evaluation has been based on the reputation of the author and the publisher, considering both their academic credentials and contributions to the field. Additionally, like for the entire literature, the relevance of the book to the specific topics of cybersecurity and autonomous vehicles has been taken into account.

Given the interdisciplinary nature of this topic, many social sciences and related fields works are present but not considered if not for the brief historical and social implications' context. The grade of confidence for principal papers has been evaluated based on several factors: the demonstration of results, coherence of conclusions, and the methodology employed.

Articles that provide empirical data or case studies have been weighted more heavily, as they offer concrete evidence to support theoretical claims. The citation index and impact factor of journals have also been considered but not prioritized over the relevance and quality of the content.

This approach ensures a comprehensive understanding of the topic, acknowledging the complexity of cybersecurity challenges without losing the focus.

1.6 Data Extraction

The data extraction process involved identifying key information from the selected literature to address the research questions. The following data points were extracted from each source:

1. *Publication:* The title of the publication, including the journal, conference, or book where the work appeared.
2. *Year:* The publication year to determine the recency of the source.
3. *Research Focus:* A brief summary of the main research focus or objective of the publication.
4. *Key Findings:* The primary findings or results of the research, including any significant insights or conclusions.
5. *Methodology:* The research methodology employed in the study, such as case studies, surveys, experiments, theoretical analysis and proposals.
6. *Relevance:* The relevance of the publication to the research questions and the broader topic of cybersecurity in autonomous vehicles.

1.7 Limitations

The limitations of this review include the following:

1. *Scope:* The review focuses primarily on cybersecurity threats, standards, and industry practices in autonomous vehicles, excluding ethical, legal, and social implications. Moreover, the review focuses on the main threats, not considering all the possible attacks due to the complexity and always evolving nature of the field.

2. *Recency:* Due to the rapidly evolving nature of the field, some literature may not capture the most recent or current techniques in autonomous vehicle security (e.g. machine learning algorithms) but address the main common solutions.

3. *Accessibility:* The availability of certain publications may be limited, but access to academic databases and libraries minimized the issue.

4. *Interdisciplinary nature:* The interdisciplinary nature of the topic may present challenges in synthesizing findings from diverse fields, but efforts have been made to ensure a comprehensive and holistic review.

1.8 Motivation

Some historic major attacks highlighted the importance of security in AV systems. As a result, both manufacturers and researchers recognized the need to strengthen security measures. This realization led to an emphasis on improving security by design. Some proposal to hardening security in AVs will be analyzed; moreover, standards that are trying to regulate the security of these systems from the design to the deployment will be compared. The problem and the motivation are that the security of AVs is a complex issue to be solved by a single solution and without the collaboration of all the stakeholders Costantino et al. [2022a]. The goal is to provide a holistic vision of the main threats and the current solutions on which the researchers are focusing on the cybersecurity field analyzing main sensors composing the perception system and the VANETs communication system.

2 Introduction

The focus is on the security aspects of autonomous on-road motor vehicles, in particular the cybersecurity threats, standards, and industry practices used to secure these systems. The current state of the VANETs communication main technologies and sensors of the perception systems will be analyzed, exploring the attack surface, main vulnerabilities and possible mitigations.

2.1 Historical roots

The development of autonomous vehicles is a significant milestone in the evolution of intelligent transport systems. It is important to start with some historical context to understand the current state of autonomous vehicles and then, the security implications.

Vehicle automation has roots with General Motors showcasing the first concept of an automated vehicle in 1939. Initial R&D efforts were led by General Motors and the Radio Corporation of America Sarnoff Laboratory in the 1950s. From 1964 to 2003, various government and academic initiatives in the US, Europe, and Japan focused on automated buses, truck platoons, and advanced driving systems Pendleton [2017], Shladover [2017]. A significant boost came from DARPA's Grand Challenges Program in the 2000s Defense Advanced Research Projects Agency (DARPA) [2007], where AVs first navigated desert terrains in 2005 and urban roads in 2007 Pendleton [2017], Shladover [2017].

Since then, researchers have rapidly progressed in academia and industry. Volvo, Tesla, Audi, BMW, Mercedes-Benz and Nissan are some of the major car manufacturers that have invested in AV technology Faisal et al. [2019].

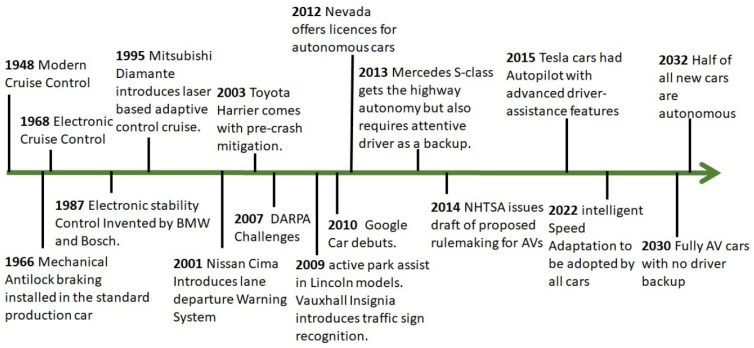

Figure 1: Historical timeline of autonomous vehicles.
From Hafeez [2021]

2.2 Autonomous Vehicles

The introduction on the market of autonomous vehicle brings to a revolutionary change in the automotive sector. It is important to understand the impact that these vehicles can have on the society and the economy, influencing not only the automotive sector.

This type of vehicle can bring us to a new era of mobility, where transportation systems become intelligent, keeping in mind that connected components can be dangerous if not specially designed or well maintained Schneier [2014]

This major challenge, as often happens during times of innovation, has brought both advantages and drawbacks in terms of security. What is intended is that the real driving force behind this innovation has been the convenience and socially beneficial aspects that have led to the rapid evolution of the sector. However, as is often the case in such situations, some fundamental details get overlooked—it's a natural consequence. In this instance, the principle of cybersecurity by design was overlooked Chattopadhyay et al. [2021], and similar to the early development of the web, efforts are now underway to rectify this.

A lot of innovations also in terms of communication have been made since the introduction of these vehicles. To improve functionalities, infotainment, safety, comfort and a lot of other aspects, vehicles require a lot of communication between them and the infrastructure like manufacturers backends or smart cities' services. The shift from isolated and static systems to dynamic and interconnected systems increases the attack surfaces, particularly in terms of adaptability, dynamism, and awareness Yu et al. [2023], Bouchouia et al. [2023].

For instance, vehicles relying on open software protocols and connecting with in-vehicle electric infrastructures play a vital role in strengthening their security framework. With the need and integration of complex systems like the perception one, these vehicles essentially evolve into a highly sophisticated set of technologies influencing each other Chattopadhyay et al. [2021].

2.2.1 Levels of Automation

The level of driving automation is determined by the specific roles assigned to both the driving automation system feature and the human user in performing the dynamic driving task (DDT) and DDT fallback SAE International [2021]. The manufacturer of the automation system defines the requirements, operational design domain (ODD), and operating characteristics of the feature, including its level of automation. Additionally, the manufacturer outlines how the feature should be properly used, ensuring that its capabilities and limitations are clearly understood and followed during operation. The Society of Automotive Engineers (SAE) has defined six levels of driving automation, ranging from no automation (Level 0) to full automation (Level 5) SAE International [2021].

1. **Level 0 (No Automation):** The human driver is responsible for all aspects of the dynamic driving task.

2. **Level 1 (Driver Assistance):** The vehicle helps the driver with specific tasks, such as steering or acceleration (e.g. lane keeping assist, adaptive cruise control).

3. **Level 2 (Partial Automation):** The vehicle can control both steering and acceleration/deceleration simultaneously under certain conditions, but the driver must

remain engaged and monitor the environment (e.g. combined LKA and ADC in traffic conditions).

4. **Level 3 (Conditional Automation):** The vehicle can perform all aspects of the DDT under certain conditions like in traffic jams or highway driving, but the driver must be ready to take over when prompted.

5. **Level 4 (High Automation):** The user (become passenger) does not need to supervise the Automated driving system (ADS) or be receptive to a request to intervene while the ADS is engaged, restricted to some conditions (e.g., Google's Self-Driving Car Teoh and Kidd [2017]).

6. **Level 5 (Full Automation):** The vehicle can perform all aspects of the DDT under all conditions without human intervention.

Levels 0–2 are generally classified as driver-assisted systems, while Levels 3 and 4 are considered semi-automated, and Level 5 represents full autonomy.

Acronym	**Definition**
ADS	Automated Driving System
DDT	Dynamic Driving Task
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response

Table 1: Definitions of Key Acronyms in Automated Driving

2.3 Overview of AVs Architecture

This section provides a high-level overview of the autonomous vehicles (AVs) architecture and the key parts that enable their operation. Moreover, an alternative architecture proposed in Hafeez [2021] will be briefly discussed. The architecture of AVs is designed to integrate various hardware and software components that work together to perceive the environment, make decisions, and control the vehicle Payton [1986].

The overall architecture presented in 2 is composed of layers of hardware and software that interact to enable the vehicle to operate autonomously. In its simplest and first form, the architecture consists of four main layers: perception, decision and planning, control and reflexive. Each layer is responsible for a specific aspect of the AV's operation, from sensing the environment to executing driving maneuvers reflexively Payton [1986].

1. **Perception**: This stage involves sensing the AV's surroundings using sensors. As expected, data processing is a fundamental step to exploit the correct information by other modules, such as adaptive detection and recognition frameworks, control systems, lane departure warning systems, traffic sign recognition, obstacle recognition, and vehicle positioning modules. The processed data is then sent to the decision and planning stage. It is important to note that performance in processing the data is fundamentals.

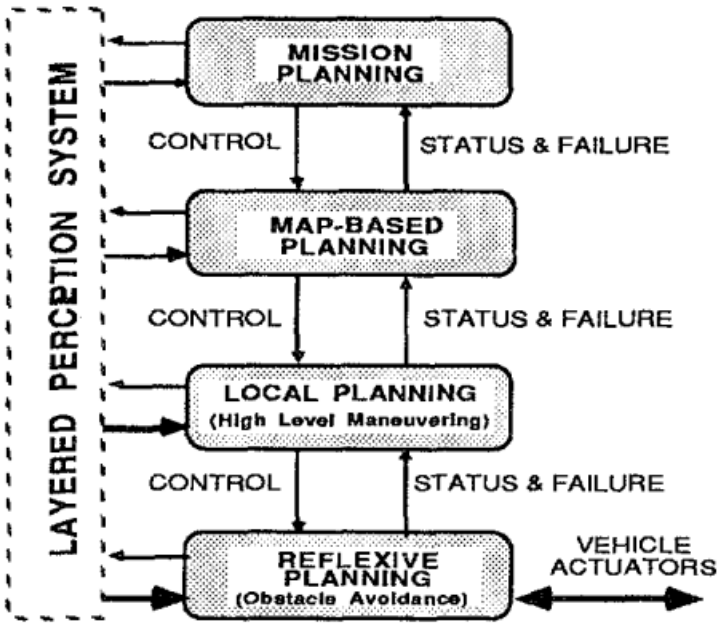

Figure 2: Hierarchical architecture of autonomous vehicles control.
From Payton [1986]

2. **Decision and Planning**: Using the data from the perception stage, this stage plans and controls the AV's motion and behavior. It handles tasks like path planning, action prediction, and obstacle avoidance based on real-time maps, traffic data, user inputs, and past information. It may also include a data log module for error tracking and future reference.

3. **Control**: The control module receives instructions from the decision and planning stage and manages the physical functions of the AV, such as steering, braking, and acceleration.

4. **Reflexive**: This final stage interfaces with the mechanical components like the motors for the accelerator, brake, steering wheel, and gear. These components are controlled by the signals from the control module to execute the AV's movements.

The proposed and secured architecture extends this architecture providing four new layers: monitoring, analysis, decision-making, and visualization. Any services, processes, and communication are monitored by the agents and analyzed by the process controllers. A set of decision controllers act on the information from the process controllers. The decisions are archived in a black box, while the analysis, reporting, and visualization layers are accessible both within the vehicle and through an external Virtual Security Operations Center (VSOC), allowing the user to consult them as needed Adu-Kyere et al. [2023].

What can be easily noted is the need to monitor and analyze the data that are exchanged between the different components of the AVs. Also, the data that are exchanged between the vehicle and the infrastructure should be monitored and analyzed to prevent and in case recover from possible attacks. Some possible research directions could be the development of a secure and efficient monitoring system that can analyze the data in real-time and take action in case of attacks 7.2.

2.4 Social implications

This section aims to provide a little insight into the social implications of autonomous vehicles. The introduction of autonomous vehicles (AVs) is expected to have a profound impact on society Thomas et al. [2020], transforming transportation systems Christian Creß [2023], urban planning Thompson et al. [2018], and the economy Boruń et al. [2020]. Some potential pros and cons of AVs are summarized in Table 2.

Pros	**Cons**
Number of accidents reduced	Definition of legal responsibilities
Time saved	Job losses
Comfort	Price

Table 2: Some pros and cons from Hafeez [2021]

The consideration of time saved is related to the trust that the user has in the vehicle and how effectively the cities in which the vehicles are used are designed and smart enough. Some references to explore in depth the social implications are left above.

2.5 Cyber-insecurity consequences

Before introducing new threats of new autonomous vehicle technologies, it is important to understand some historical key attacks. In the past, researchers have demonstrated various attacks on AVs, including remote hijacking, sensor spoofing, and data breaches. The attack surface of AVs is expanding due to the increasing complexity of these systems, which rely on a combination of hardware, software, and communication technologies Kukkala et al. [2022]. This expansion is due to the aggressive attempts of manufacturers to make vehicles fully autonomous in a short period of time and without considering the cybersecurity implications. Focussing always on the functionalities offered to the driver in terms of comfort, the security of the vehicle has been considered as a secondary aspect, leading to a lot of vulnerabilities that can be exploited by attackers.

Some famous attacks that bring the attention to the cybersecurity of AVs are:

1. The Jeep Cherokee hack in 2015: researchers remotely hijacked a Jeep Cherokee through its infotainment system, demonstrating the risks of cyber-attacks on connected vehicles Miller and Valasek [2015].

2. The Tesla Model S hack in 2016: researchers exploited vulnerabilities in the vehicle's software to take control of the car's brakes, door locks, and other critical

systems Francillon et al. [2011].

3. The Nissan Leaf hack in 2016: researchers demonstrated how an attacker could remotely control the vehicle's heating and air conditioning systems, drain the battery, and access the driver's personal information.

4. The VW group hacked in 2016: researchers discovered vulnerabilities in the keyless entry systems of several VW group vehicles, allowing attackers to unlock the doors and start the engine without the key fob Garcia et al. [2016].

5. The Tesla cybertruck: it continues to be exploited by attackers to gain access to the vehicle's systems and control its functions remotely.

These are only some examples of the risks associated with AVs and the need for robust cybersecurity measures to protect against cyber-attacks.

3 Communication

Communication as mentioned before is a key part of AVs. A *Vehicular ad hoc network* (or VANET) is a proposed type of *mobile ad hoc network* (called also MANET) involving road vehicles. This type of network permits vehicles to communicate with roadside equipment, such as traffic lights, and with each other Sheikh and Liang [2019]. The main purpose of such technology is to generate security on the roads, in this case security in terms of passengers and pedestrian safety. The main components of VANET technology are: *On-board unit (OBU)*, *Road-side unit (RSU)*, *Trusted Authority (TA)*. The Trusted Authority acts as a key part in the VANET architecture, as it is responsible for managing the security of the network and ensuring that all vehicles are authenticated and authorized to communicate.

Communications are crucial for Autonomous Vehicles (AVs) to interact with other vehicles, infrastructure, and the cloud. There may be many ways to categorize communications in AV devices. One approach is based on the range of communication, so a categorization that focus on the different distances covered by it. Another approach can be based on the kind of subject involved in the communication, so a categorization that focus on the type of interaction and the entities involved in the communication itself. Classification of AVs communications by range:

1. **Short-range communication**

2. **Medium-range communication**

3. **Long-range communication**

Or by the kind of subject involved in the communication:

1. **Vehicle-to-Vehicle (V2V)**

2. **Vehicle-to-Infrastructure (V2I)**

3. **Vehicle-to-Everything (V2X)**

In the following sections, more details for the different type of communication will be provided.

3.1 Vehicle-to-Vehicle (V2V)

When speaking about Vehicle-to-Vehicle (V2V), the focus is on communications that happen between vehicles. It obviously involves wireless communications between motor vehicles, aiming primarily to prevent accidents by exchanging data such as position and speed. This communication happens within an ad-hoc mesh network, which can either be fully connected or partially connected. In both cases, messages can be relayed directly or through multiple paths, ensuring robust communication even if some nodes fail. While wired mesh networks were once expensive and challenging to implement, wireless technologies, such as WPANs, have made them possible today Arena and Pau [2019].

The advantages in terms of new functionalities and comfort offered to the drivers are clearly various. Some examples of security-improving features created by exploiting V2V are the Blind Spot Detection (BSD) that warns the drivers about other vehicles of any type located out of sight, the Forward Collision Warning System (FCWS), automatic emergency braking (AEB) and the Lane departure warning system (LDWS) Arena and Pau [2019].

In terms of design, the USDOT (Department of Transportation of the United States of America) has documented the security requirements of systems and in particular, the need to define security network requirements for V2V and its supporting systems.

3.2 Vehicle to Infrastructure (V2I)

Vehicle to Infrastructure is another type of communication in Intelligent Transportation System (ITS) that enables vehicles to communicate with roadside infrastructure, such as traffic lights, signs, and road sensors.

In this case, communication can vary greatly depending on the type of infrastructure with which you want to communicate. It can be exploited to provide real-time traffic information, road condition updates, and other services to drivers, representing the next evolution and a significant step towards the development of smart cities Department of Transportation of the United States of America [2024].

State and local agencies are expected to install V2I systems either alongside or integrated with existing ITS equipment. As a result, many V2I deployments could be eligible for similar federal-aid programs as ITS, provided the deploying agency meets certain requirements Department of Transportation of the United States of America [2024].

3.3 Vehicle to Everything (V2X)

Vehicle-to-Everything (V2X) is a general communication model that generalizes Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) systems, incorporating interactions between vehicles and other entities, such as pedestrians (V2P) Tahmasbi-Sarvestani et al. [2017], roadside equipment (V2R) Wu et al. [2018], and devices (V2D). V2X, like V2V and V2I, aims to enhance road safety, focussing on vulnerable road users.

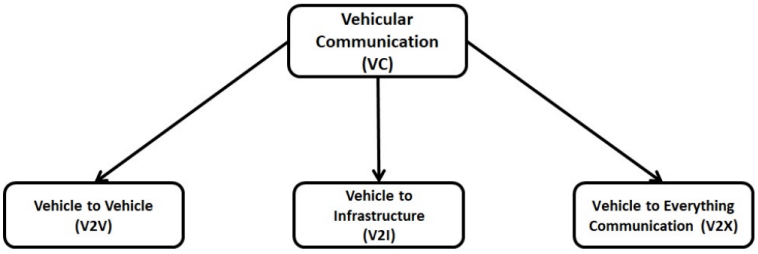

Figure 3: VANETs

3.4 Controller Area Network bus

Internal communications are managed by the Controller Area Network (CAN) bus. CAN is the most common network topology used for controlling industrial machinery and widely used in the automotive industry also due to its cheapness and reliability. It is a communication network that offers rapid communication among microcontroller devices. Each component in the network is connected to the bus and called node. CAN permits these nodes to use a message-based protocol designed to let all nodes receive and send messages on the network Kiencke et al. [1986]. The CAN bus is a broadcast network, meaning that all nodes on the network receive the message and require no authentication to receive the message, that is hazardous in terms of security. Due to its unsecure nature, the CAN bus is vulnerable to cyber-attacks and is the standard interface that attackers use to inject attack messages into the communication network. It is required for a malicious attacker to have physical access to the vehicle to perform the attack, constraining the attacker to be near the target vehicle. The exploitation in this case is only physical and not through the network; in that case, the attacker can be located anywhere in the world. Researchers tried to evaluate some new technologies to detect the malicious code and mitigate the attacks Aldhyani and Alkahtani [2022] 8.1 using deep learning algorithms to detect the malicious code on the CAN bus. The proposed systems have demonstrated effective detection of abnormal packets to safeguard the CAN bus. Additionally, they can be adapted to other security system designs within the complex infrastructures of autonomous vehicle networks, ensuring more secure data processing.

4 Perception

It is fundamental in AVs to perceive the environment and understand the context in which the vehicle is operating for obvious reasons. The perception system is responsible for collecting data from various sensors, such as cameras, LiDAR, radar, and ultrasonic sensors, to create a detailed representation of the vehicle's surroundings. In this case, it is important to consider the possible tampering that can be done on these sensors to alterate the perception of the vehicle, leading to dangerous situations Kim et al. [2020], Girdhar et al. [2023], Shahida Malik [2020], El-Rewini et al. [2020].

4.1 Main sensors

1. **Cameras**: Cameras are used to capture visual data, such as images and videos, of the vehicle's surroundings.
2. **LiDAR (Light Detection and Ranging)**: LiDAR sensors use laser light to measure distances and create detailed 3D maps of the environment.
3. **Radar (Radio Detection and Ranging)**: Radar sensors use radio waves to detect objects and measure their distance, speed, and direction.
4. **Ultrasonic Sensors**: Ultrasonic sensors use sound waves to detect objects and measure their distance.
5. **GPS (Global Positioning System)**: GPS sensors use satellite signals to determine the vehicle's location and navigate to a destination.
6. **IMU (Inertial Measurement Unit)**: IMU sensors measure the vehicle's acceleration, orientation, and angular velocity.

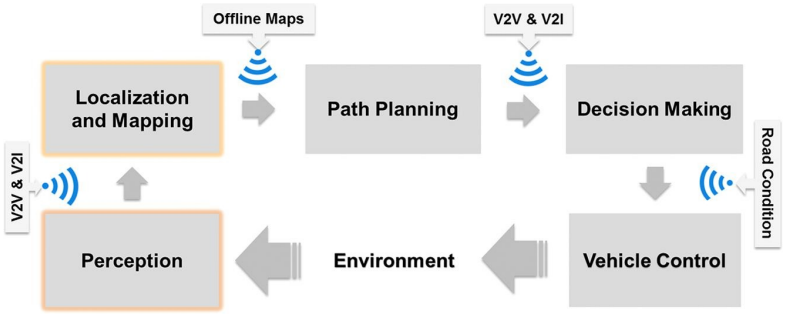

Figure 4: Overview

As understood, these sensors provide the critical data needed for navigation, obstacle detection, and decision-making processes and are essential for ensuring safety Penumarthy et al. [2020], Kukkala et al. [2022].

In the next sections 5 there will be a deep dive into the main sensors used in AVs and their vulnerabilities.

5 Cybersecurity Threats

In this section, the goal is to discuss potential threats about the two macro-areas covered by this report: communication (specifically VANETs) and the perception system, giving a comprehensive overview of the potential threats and the countermeasures that can be adopted to mitigate them, focussing on remote attacks. The multitude of technologies involved in these two areas makes the AVs vulnerable to a wide range of attacks, decreasing the threshold of security. With the threshold, it is meant the acceptable level of security that is needed to protect the system from attacks. If not only the safety of the system but also the safety of other potential road users is taken into consideration, the threshold must be extremely high. Attackers can exploit vulnerabilities to compromise the safety and functionality of AVs, posing significant risks to passengers, pedestrians, and other road users. Since now cars are connected to the internet, there is no need to be physically close to the car to exploit these vulnerabilities and this expands the attack surface drastically. In the past decade (2010 onward), nearly 79.6% of all automotive attacks have been remote attacks Kukkala et al. [2022].

5.1 General

This section highlights various attacks, possible tempering and threats that affect the security services in general regarding the CIA triad. It is important to mention that the CIA triad is a model designed to guide policies for information security, and in the list below, some techniques cannot be present.

Attack on Confidentiality

1. **Eavesdropping**: Intercepts confidential information, such as user identity and location.
2. **Traffic Analysis**: Analyzes message transmission patterns to extract sensitive information.
3. **Man-in-the-Middle**: Intercepts and alters messages between communicating vehicles.
4. **Social Engineering**: Distracts and exploits drivers to gain access to confidential information.
5. **Sybil Attack**: Uses multiple fake identities to mislead vehicles and compromise confidentiality.
6. **GPS Spoofing**: Creates false GPS information, compromising location confidentiality.

Attack on Data Integrity

1. **Masquerading**: Uses valid credentials to broadcast false messages.
2. **Replay**: Repeats or delays transmissions, complicating emergency responses.
3. **Message Tampering**: Modifies messages to influence driving behavior.
4. **Illusion**: Generates misleading traffic warnings based on malicious data.
5. **Node Impersonation**: Uses a valid user ID to impersonate another user, compromising the integrity of communications.
6. **Key/Certificate Replication**: Uses duplicates to create confusion, affecting data authenticity and integrity.

Attack on Availability

1. **Denial-of-Service**: Blocks vehicle communication, disrupting operations; can occur as distributed denial of service (DDoS) Sontakke and Chopade [2022].
2. **Jamming**: Uses strong signals to disrupt communication channels, critical for safety applications.
3. **Malware**: Penetrates OBUs, RSUs or other system component leading to system malfunctions.
4. **Broadcast Tampering**: Untrustworthy vehicles alter or replicate messages, hiding critical safety information.
5. **Black-hole**: Malicious nodes receive but do not forward packets, obstructing communication. Another version is the *Gray-hole* that selectively drops only some packets.

To deepen the knowledge about other specific techniques for attacking and potential countermeasures, a specific evaluation can be found in Iqbal et al. [2022], Sheikh and Liang [2019], Macena et al. [2023].

A = Availability, AU = Authentication, C = Confidentiality, I = Integrity from Sheikh and Liang [2019].

5.2 VANETs

In this section, the focus is on the communication system, specifically on the VANETs. Some countermeasures are presented to mitigate the threats that affect the security services in VANETs, in particular the location privacy and related info. Some of the main countermeasures, with benefits and limitations, are presented and discussed.

Attack	Compromised	Countermeasures
DOS	A	Signature-based authentication technique 7.2
Jamming	A	Direct-sequence spread spectrum (DSSS Wang et al. [2022])
Malware	A	Reliable hardware and digital signature of software
Broadcast tampering	I, A	Non-repudiation mechanism may exist
Black-hole, gray-hole	A	Reliable hardware and digital signature of software
Greedy behavior	A	Use intrusion detection systems (IDSs)
Spamming	C, A	Reliable hardware and digital signature of software
Eavesdropping	C, I	Exploit physical layer security protocols
Traffic analysis	C	Encryption techniques
Man-in-the-middle	C, I, A	Robust authentication technique (E.g. CA)

5.2.1 Pseudonym Change and Silent Periods

Dividing road networks into observed and unobserved zones allow vehicles to change pseudonyms and behavior, such as altering speeds and directions in unobserved zones. This, combined with random silent periods in vehicle-to-vehicle (V2V) communication, reduces the risk of tracking and identity linking. However, this technique can lead to privacy loss and computational strain for certain vehicles, particularly in V2I (vehicle-to-infrastructure) interactions, where more complex tasks are required.

1. **Key Features**:
   a) Road networks divided into observed/unobserved zones.
   b) Vehicles in unobserved zones change pseudonyms, directions, and speeds.
   c) Random silent periods in V2V communications to unlink identities.
2. **Limitations**: Navigation group leaders privacy and computational overhead in V2I applications.

5.2.2 Cryptographic MIX-Zone (CMIX)

RSUs (Roadside Units) provide cryptographic keys to vehicles, enabling secure pseudonym exchanges in encrypted zones. This method strengthens privacy, but the high costs of the required hardware and the complexity of managing pseudonym certification represent significant hurdles, particularly when applied on a larger scale.

1. **Key Features**:
   a) RSUs provide vehicles with cryptographic keys.
   b) Pseudonym exchange in encrypted mixing zones.
   c) Possible pseudonym certification through authorities.
   d) Optional use of hardware security modules (HSMs).
2. **Challenges**: High hardware costs and managing pseudonym certification.

5.2.3 K-Anonymity

A trusted server anonymizes data, and location information is shared only if enough vehicles are present nearby, making individual tracking more difficult. This technique is scalable and can be adjusted based on vehicle density, making it well-suited for dynamic traffic conditions.

1. **Key Features**:
    a) Trusted server anonymizes data via cloaking.
    b) Location shared only if K vehicles are nearby.
2. **Advantages**: Scalable and customizable based on vehicle density.

5.2.4 Dynamically Changing MAC/PHY

Periodic swapping of these addresses complicates tracking efforts. Cryptographic key exchanges ensure that address changes are secure, although this approach requires careful management of the cryptographic process to maintain seamless communication.

1. **Key Features**:
    a) Periodic MAC/PHY address swapping.
    b) Cryptographic key exchange during address changes.
2. **Advantages**: Makes vehicle tracking harder.

5.2.5 Density-Based Location Privacy (DLP)

Offers protection by changing pseudonyms based on the number of surrounding vehicles. In high-traffic areas, this method enhances privacy, but determining the optimal conditions for triggering pseudonym changes can be a challenge, particularly in environments with rapidly shifting traffic densities.

1. **Key Features**:
    a) Pseudonym change occurs with k neighboring nodes.
    b) Improved privacy in high-traffic areas.
2. **Challenges**: Dynamic pseudonym change thresholds.

The integration of pseudonyms, cryptographic techniques, dynamic address changes, and density-based strategies offers a comprehensive framework for improving location privacy, however, practical implementation requires careful consideration of the associated costs and complexities Macena et al. [2023].

5.3 Perception System

The perception system in AVs is responsible for collecting and processing data from various sensors to understand the vehicle's surroundings. The data collected by the perception system is crucial for making informed decisions and coordinating the vehicle's actuators in a safe and efficient manner. However, since it is composed by a multitude of sensors, the perception system is a subsystem where the attack surface is huge 5. In this section, some main issues about the perception system will be presented and discussed, focusing on the potential threats and the countermeasures that can be adopted to mitigate them El-Rewini et al. [2020].

As mentioned, some sensors are *LiDAR*, *radar*, *cameras*, and *ultrasonic sensors*, to perceive and interpret their surroundings accurately. For their nature, it is challenging preventing from common attacks like spoofing and jamming. Sensor spoofing involves introducing false data into the sensor systems, while jamming overwhelms the sensors with noise, disrupting their normal functioning.

Through such manipulation, attackers can deceive the vehicle's control systems, causing misinterpretations of the environment. For example, projecting fake obstacles might cause unnecessary breaking, while concealing real obstacles could lead to collisions. These manipulations result in erratic driving behavior. In cases of jamming, AVs may become *careless* to their surroundings, resulting in dangerous situations due to the absence of reliable sensor input Durlik et al. [2022].

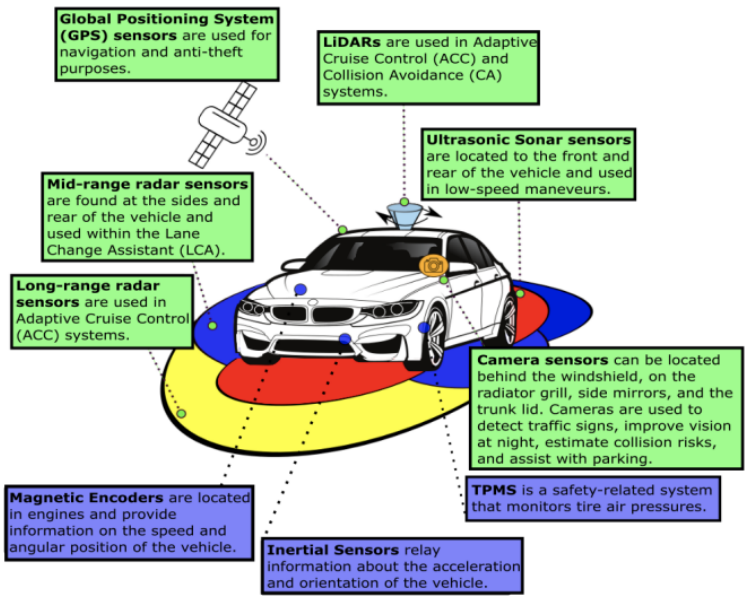

Figure 5: Main sensors used in AVs from El-Rewini et al. [2020]

What emerges from the literature is that the perception system is a critical component of AVs, mainly every sensor can be a potential target for cyber-attacks using the tech-

niques mentioned above. From LiDAR, Ultrasonic Sensor, Camera, Radar, GPS, that are the most common sensors used is AVs, to the Tire Pressure sensors are all potential targets El-Rewini et al. [2020].

Countermeasures Given the complexity of autonomous vehicle perception systems, they can easily become a target for attacks. The current approach acknowledges this vulnerability, which is challenging to fully eliminate. Instead, the focus is shifting towards recognizing the stimuli detected by these systems and determining whether they are legitimate or not. As highlighted in the machine learning/AI section 8.1, machine learning algorithms—particularly those for anomaly detection—are being employed to identify and respond to irregularities in sensor data. Another possible countermeasure is sensor fusion, which involves cross-referencing data from multiple sensors. This technique helps to provide more accurate measurements and enables more stable decision-making and reactions.

However, while machine learning offers new avenues for detecting and mitigating these attacks, it introduces new challenges in terms of legal and ethical considerations. Since the focus is not on these aspects but in the technical ones, it is essential to consider the forensic implications of these algorithms Durlik et al. [2022], Prinkle Sharma [2022] and possible research for the future to eliminate these vulnerabilities.

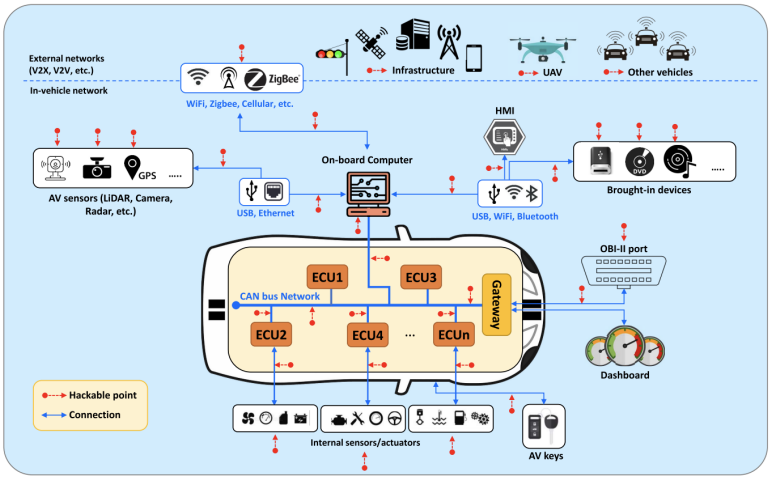

Figure 6: Main attack vectors from Bendiab et al. [2023]

6 Cybersecurity-by-design standards

6.1 ISO/SAE 21434: Overview

Released in August 2021, the ISO/SAE 21434 standard is a joint standard developed by the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) to address the cybersecurity of road vehicles.

The standard is designed to provide a framework for the development of secure vehicles and their components, covering the entire lifecycle of a vehicle, from design and development to production and operation. It provides guidelines for identifying and assessing cybersecurity risks, as well as for implementing security measures to mitigate those risks. The standard also includes requirements for monitoring and responding to cybersecurity incidents, as well as for managing the security of vehicle components and systems.

It establishes guidelines for original equipment manufacturers (OEMs) and suppliers to manage cybersecurity risks introducing the concept of Cybersecurity Assurance Levels, which categorize the severity of cybersecurity threats and the corresponding measures to mitigate them Moukahal et al. [2021], Costantino et al. [2022b].

Here's an overview, including key points, limitations, and guidelines.

6.1.1 Key Points

1. **Cybersecurity Culture**: Organizations should promote a strong cybersecurity culture within them, emphasizing safety and security in all engineering processes, starting from the design phase.

2. **Risk Management**: Some risk management plan guidelines for identifying and managing cybersecurity risks, including threat analysis, impact assessment, and risk mitigation strategies.

3. **Documentation Requirements**: Technical Documentation to establish a series of required work products, including asset identification, threat scenarios, and a cybersecurity incident response plan.

4. **Lifecycle Integration**: Lifecycle management to cover cybersecurity aspects from the initial design phase to decommissioning, ensuring that security measures are integrated throughout the vehicle's lifecycle.

5. **Collaboration with Other Standards**: It enables the integration of the standards with existing standards, particularly ISO 26262 (which focuses on functional safety), ensuring that both safety and security are taken into account during vehicle development.

6. **Continuous Monitoring and Improvement**: It encourages continuous cybersecurity assessment and updates to address evolving threats and vulnerabilities.

6.1.2 Limitations

1. **Lack of Specific Technical Solutions**: The standard does not prescribe specific technologies or methods for implementing cybersecurity measures, potentially leading to varied interpretations and implementations among manufacturers.

2. **Potential for Fragmentation**: Without defined methods, companies may adopt proprietary solutions that could create compatibility issues within a highly connected automotive environment.

3. **No Mandatory Compliance**: ISO/SAE 21434 is a guideline rather than a regulation, meaning compliance is not enforced by law, which could lead to inconsistent application across the industry.

4. **Limited Focus on Cybersecurity Techniques**: While the standard outlines processes and documentation, it does not provide detailed methodologies for specific cybersecurity assessments or techniques to evaluate vulnerabilities effectively.

6.1.3 Guidelines

1. **Threat Analysis and Risk Assessment**: The standard emphasizes conducting thorough threat assessments to identify potential vulnerabilities in vehicle systems and the likelihood of cyberattacks.

2. **Incident Response**: Requires the establishment of a cybersecurity incident response plan to ensure quick and effective actions are taken in the event of a security breach.

3. **Continuous Improvement**: Advocates for regular updates and improvements to cybersecurity practices to adapt to new and emerging threats in the automotive landscape.

6.2 UNECE WP.29 R155: Overview

The United Nations Economic Commission for Europe (UNECE) oversees regulations concerning cybersecurity and software updates for road vehicles, specifically through the UNECE WP.29 section. Regulation 155 (R155) was established in March 2021 to address cybersecurity threats in vehicles and ensure user safety. It outlines requirements for original equipment manufacturers (OEMs) and tier suppliers to implement cybersecurity measures in new vehicles, with compliance becoming mandatory for all vehicles by July 2024. Since there are currently no uniform evaluation criteria at the product level, the question arises as to which development artifacts could serve as indicators to determine the effectiveness of mitigation strategies. In response to this challenge, SAE analyzes existing security concepts in the ISO/SAE 21434 standard, providing an overview of the-state-of-the-art in security evaluation methods. The general goal is to derive applicable evaluation criteria and recommendations for an R155 approval, taking into account relevant security properties that help decide the sufficiency of security measures Hellstern et al. [2024].

As for the ISO/SAE 21434 standard, key points, correlations, threats, and mitigations in UNECE WP.29 R155 are discussed below.

6.2.1 Key Points

1. **Cybersecurity Regulations (R155)**: Crucial regulations for OEMs and tier suppliers in UNECE member countries. Mandatory compliance for new vehicle types since July 2022 and for all vehicles from July 2024. Compliance is mandatory.

2. **Cybersecurity Management System (CSMS)**: Organizations must implement CSMS to manage cyber risks across the vehicle lifecycle. This systematic approach involves defining processes, responsibilities, and governance to protect vehicles from cyber threats.

3. **Certification**: OEMs must apply for a Certificate of Compliance for their CSMS, which is valid for three years, subject to renewal. The approval process involves assessments and validation by technical services and Approval Authorities.

6.2.2 Structure

1. **Part A**: Identifies 32 potential threats related to various attack surfaces. Each threat includes examples of vulnerabilities affecting CIA triad of vehicle systems.

2. **Part B**: Outlines high-level mitigation actions specifically for vehicle-related threats.

3. **Part C**: Addresses threats from external entities.

6.2.3 Limitations

1. **Focus on Conventional Vehicles**: R155 was developed with traditional vehicles in mind and may not fully address the unique complexities of autonomous vehicles (AVs) with their advanced software, sensors, and connectivity.

2. **Lack of Adaptability**: The regulation does not provide specific guidance on securing AI models, machine learning algorithms, or V2X communication, which are crucial for AVs.

3. **Lack of Flexibility**: R155 emphasizes managing known risks but lacks the flexibility to proactively address evolving cybersecurity threats, which are rapidly changing in the AV domain.

4. **Insufficient Supply Chain Risk Management**: The regulation lacks in addressing cybersecurity risks across complex AV supply chains, like third-party software.

5. **Critical Assessment**: As mentioned, it is challenging for AV manufacturers to demonstrate compliance due to a lack of standardized product-level evaluation criteria.

6. **Need for Continuous Monitoring**: R155 does not emphasize the need for continuous threat monitoring.

7. **Gap and lag for New Threats**: It is impossible to think that a regulation can be updated as fast as the threats evolve.

6.3 Comparative Analysis

	UNECE R155	ISO 21434
Document Type	regulation	standard
Application	mandatory	optional
First Release Date	March 2021	August 2021
Application Phase	Homologation	Life-cycle Product
Approach	Risk-based	Security by design
Glossary	13 terms	40 terms

Figure 7: Comparison of ISO/SAE 21434 and UNECE WP.29 R155
From Costantino et al. [2022a]

The development of UNECE R155 and ISO/SAE 21434 arose from the need to enhance cybersecurity in road vehicles to ensure user safety and protect personal data. Although UNECE R155 was released in March 2021 and ISO/SAE 21434 followed in August 2021, the two documents serve different purposes within the automotive cybersecurity landscape. Here's a detailed analysis of their similarities, differences, and limitations.

6.3.1 Correlations

Overall, the UNECE regulations emphasize a comprehensive and systematic approach to cybersecurity in the automotive sector, requiring OEMs to be proactive in identifying risks and implementing suitable mitigations. ISO 26262 emphasizes the relationship between safety and cybersecurity, ensuring that both aspects are addressed in vehicle design. UNECE WP.29 R155, instead, provides a legal framework for cybersecurity in vehicles, complementing ISO/SAE 21434 by outlining regulatory requirements and compliance timelines.

6.3.2 Similarities

1. **Objectives**: Both UNECE R155 and ISO/SAE 21434 aim to improve cybersecurity throughout the product lifecycle of road vehicles.
2. **High-Level Solutions**: Both documents propose high-level solutions and do not prescribe specific implementations, allowing manufacturer flexibility to adopt suitable measures for their contexts.
3. **Threat Identification**: UNECE R155 identifies possible threats while ISO/SAE 21434 cites similar scenarios requiring analysis and mitigation.

4. **Structured Organization**: Both documents require a structured approach to managing cybersecurity, including
5. **CSMS**: Cybersecurity Management Systems and risk identification.
6. **Risk Mitigation**: Both emphasize risk mitigation processes, where UNECE R155 focuses on risk management and ISO/SAE 21434 outline specific risk treatment options.
7. **Documentation for Compliance**: Documentation required for ISO/SAE 21434 can support compliance with UNECE R155, facilitating a cohesive approach.
8. **Continuous Review**: Both standards require continuous monitoring and improvement of cybersecurity measures to address evolving threats.
9. **Cost Considerations**: Both UNECE R155 and ISO/SAE 21434 acknowledge the need for cybersecurity compliance that balances implementation costs with operational feasibility.

6.3.3 Differences

1. **Type**:
   a) **UNECE R155**: A legally binding regulation that mandates compliance for all UNECE member countries.
   b) **ISO/SAE 21434**: A non-mandatory standard expected to be widely accepted within the automotive industry.
2. **Timeline**:
   a) **UNECE R155**: Compliance from July 2022 and for all vehicles by July 2024.
   b) **ISO/SAE 21434**: Became applicable from August 2021.
3. **Application Phases**:
   a) **UNECE R155**: Focused primarily on the homogenization process of new vehicles.
   b) **ISO/SAE 21434**: Product lifecycle, requiring ongoing documentation for annual audits, from design to decommissioning.
4. **Threat and Mitigation**:
   a) **UNECE R155**: Provides tables outlining specific threats and recommended mitigations.
   b) **ISO/SAE 21434**: Does not directly address attacks but emphasizes vulnerability analysis and risk assessments.
5. **Compliance Requirements**:

a) **UNECE R155**: Offers a less detailed list of compliance documentation compared to ISO/SAE 21434.

b) **ISO/SAE 21434**: Details the attack feasibility ratings and their implications.

6. **Regulatory Authority**:

a) **UNECE R155**: Enforced by regulatory authorities in UNECE member states, with compliance being mandatory.

b) **ISO/SAE 21434**: Lacks mandatory enforcement, relying on industry acceptance and best practices.

6.3.4 Conclusion

In conclusion, while UNECE R155 and ISO/SAE 21434 share common goals of enhancing cybersecurity in the automotive industry, they differ significantly in their nature, application, and requirements. UNECE R155 is a binding regulation focused on approval, while ISO/SAE 21434 serves as a comprehensive standard for the entire vehicle lifecycle. Their complementary nature allows manufacturers to leverage the documentation and processes of one to meet the requirements of the other, fostering a more robust approach to cybersecurity in road vehicles Costantino et al. [2022a]. The problem remains that the lack of mandatory enforcement in ISO/SAE 21434 could lead to inconsistent implementation across the industry and hinder the standard's effectiveness.

7 Actual Solutions

7.1 Secure Software Development Life-Cycle

Cybersecurity in autonomous vehicles (AVs) is a critical concern that requires a comprehensive and multi-faceted approach. One of the key strategies for enhancing AV security is the implementation of secure software development practices. The secure software development life cycle (SDLC) is a systematic and structured approach to developing software that prioritizes security at every stage of the development process. By integrating security considerations into the software development process from the outset, developers can identify and mitigate security vulnerabilities early, reducing the vulnerability time window. A specific way to update will be analyzed in section 7.2.1.

The major challenges in implementing a secure software development life-cycle are:

1. **Complexity of AV Systems**: AV systems are complex and interconnected, containing a huge number of LOC that can easily introduce vulnerabilities.

2. **Various Technologies**: AV systems are composed of various technologies, including sensors, actuators, and communication systems, each of which presents unique security challenges in terms of code vulnerabilities and attack surfaces.

3. **Outsourcing**: Many AV manufacturers outsource software development to third-party vendors, introducing possible supply chain vulnerabilities.

4. **Open-source Code**: Can be seen as a double-edged sword, but if not properly managed, it can introduce security vulnerabilities.

5. **Security Decays Over Time**: As software ages, vulnerabilities may be discovered, and security patches may be required.

To address these challenges, AV manufacturers must adopt a security-first mindset and integrate security into every phase of the software development life cycle Moukahal et al. [2021]. The main phases of the secure software development life cycle include:

1. **Requirement Analysis:** Consider the complexity of automotive systems that require special security consideration to manage it properly.

2. **Design:** Examine the system architecture thoroughly to construct proper measures limiting system weaknesses.

3. **Assurance Planning:** Guarantees that manufacturers are ready to take proper and prompt actions to mitigate cyber incidents, starting after the cybersecurity design phase to ensure incident response planning abides by the system design.

4. **Implementation:** Involves security engineers monitoring the development of automotive components to confirm compliance with secure coding practices.

5. **Component Testing:** Part of the security verification phases dedicated to ensuring the integrity of individual components.

6. **Integration Testing:** Evaluates the interactions between integrated components to identify potential vulnerabilities.

7. **Resilience Verification:** Assesses the overall resilience of the system against cyber threats.

The cybersecurity challenge requires a comprehensive and multi-faceted approach, and the secure software development life cycle is a key strategy for enhancing AV security. In this case, only main challenges are presented, but there are many more that can be found in the literature Moukahal et al. [2021] and others.

7.2 Intrusion Detection and Prevention Systems

IDPS are essential parts of a comprehensive cybersecurity strategy for AVs, they allow for real-time monitoring and detection of potential cyber threats, enabling rapid response and mitigation of security incidents. As mentioned in Kim et al. [2020] the need of an intrusion detection system is not something new, research papers have been published since 2009, and the need for a proper system is still present.

Before the emergence of connected vehicles, the primary emphasis was on detecting malicious software within the vehicle itself. However, the focus has now expanded to include a broader range of threats beyond just in-vehicle malware detection. This type of systems helps to detect and prevent unauthorized access to the vehicle's network, monitor the behavior of connected devices, and identify anomalous activities that may indicate a cyberattack. New approaches make large use of machine learning algorithms to detect anomalies in the vehicle's network traffic, and to identify patterns that may indicate a potential security threat Nagarajan et al. [2023].

7.2.1 Secure Over-the-Air (OTA) Updates

One of the key challenges in maintaining the security of AVs is the need to update software and firmware over-the-air (OTA) to address security vulnerabilities and bugs when they are discovered. OTA updates are crucial for maintaining both the security and functionality of autonomous vehicle (AV) systems, Durlik et al. [2022], Hafeez [2021] but the need to ensure that these updates are secure and tamper-proof is essential. Secure OTA mechanisms ensure that software updates are properly authenticated and delivered without the risk of tampering.

An immediate advantage of OTA updates is the ability to quickly deploy security patches and updates to all vehicles in a fleet, reducing the risk of exploitation of known vulnerabilities. However, in terms of security, OTA updates pose significant challenges due to their complexity, multiple attack surfaces, and reliance on outdated techniques.

Some main functionalities of OTA updates are:

1. **Addressing Vulnerabilities**: Rapid hot-fix security of flaws reducing the risk of exploitation.
2. **Enhancing Security Features**: Patching intrusion detection and authentication protocols.
3. **Bug Fixes**: Resolving software bugs that may cause malfunctions or security risks.
4. **Adapting to Emerging Threats**: Updating software to counter new and evolving cybersecurity threats.
5. **Minimizing Downtime**: Ensuring updates occur with minimal disruption to vehicle operation.
6. **Maintaining Compliance**: Keeping the vehicle up to date with regulatory security standards.

Best practices:

1. **Secure Update Mechanism**: Ensures the integrity and confidentiality of the update process through authentication and encryption.

2. **Testing and Validation**: Rigorous testing to prevent new vulnerabilities and maintain functionality.

3. **User Notification and Consent**: Informing users about updates and getting consent when necessary.

4. **Regular Update Schedule**: Consistent schedule to ensure timely updates.

A proposal for a secure OTA software update scheme designed for cloud-based deployment is STRIDE, a resistant to malicious attacks and scalable to accommodate concurrent updates across many vehicles. It enables scalable, fast and secure distribution of update packages from software providers to vehicles, ensuring end-to-end security through ciphertext-policy attribute-based encryption. Extensive experimental evaluations show that STRIDE effectively reduces overhead without increasing network load or software update retrieval time compared to the best-performing the newest schemes Ghosal et al. [2020].

8 Future Directions

In this section, a brief overview of the future directions in cybersecurity for autonomous vehicles is provided exploring the potential of emerging technologies and trends to enhance the security of AVs.

8.1 Artificial Intelligence

Artificial Intelligence (AI) and Machine Learning (ML) are becoming increasingly important parts of cybersecurity in AVs. Given the amount of data generated by AVs, many AI and ML applications can be useful not only to perceive the environment but also to enhance path-following algorithms, environmental sensing, and improve driver convenience and safety Giannaros et al. [2023].

In the context of cybersecurity, AI is used to recognize threats, deploy adaptive security systems, mitigate risks, identify anomalies, and, in some instances, automatically isolate potentially compromised components or reroute communication paths to counterthreats Durlik et al. [2022].

8.2 Blockchain

Blockchain technology and infrastructure can enhance the security of autonomous vehicles in several ways exploiting its main features.

1. **Secure Communication**: Blockchain can be employed to secure vehicle-to-everything (V2X) communication, ensuring that the data exchanged between AVs, infrastructure, and other entities is tamper-proof and authenticated. This prevents unauthorized access and data manipulation.

2. **Data Integrity**: The immutable nature of blockchain's ledger ensures that all recorded data is verifiable and cannot be altered retroactively. This is particularly beneficial for maintaining the integrity of sensor data, driving logs, and software updates, thereby enhancing trust in the system.

3. **Identity Management**: Blockchain can provide a decentralized framework for identity management, ensuring that only authenticated and authorized entities can access AV systems. This reduces the risk of identity spoofing and unauthorized access.

These are not the only applications of blockchain in AV cybersecurity that can also support **transparent and secure storage of data**, **reputation and trust management**, and **forensics applications**. However, challenges remain in areas such as scalability, latency, energy consumption, and privacy concerns associated with both permission-less and permissioned blockchains Bendiab et al. [2023], Giannaros et al. [2023], Khan et al. [2020], Admass et al. [2023], Ahmad et al. [2023].

8.3 Quantum Computing

The rise of quantum computers presents a challenge to current cryptographic systems. To defend against quantum-based attacks, quantum-resistant cryptography is essential. Future research should prioritize developing quantum-resistant algorithms to safeguard sensitive cryptographic data and ensure long-term security Ahmad et al. [2023], Admass et al. [2023].

1. **Quantum-Resistant Cryptography**: Adopt post-quantum cryptographic algorithms (e.g., lattice-based, code-based) designed to withstand quantum attacks.

2. **Quantum Key Distribution (QKD)**: Utilize quantum mechanics for secure key distribution, ensuring protection from quantum attacks in the V2X ecosystem.
   a) Implement standardized components like quantum random number generators (QRNG).
   b) Use post-quantum encryption algorithms and reconfigurable hardware like FPGA.

3. **Hybrid Cryptography**: Combine classical and quantum-resistant techniques to enhance security, using a hybrid approach for data encryption and key exchange.

4. **Quantum-Safe TLS**: Develop or adopt quantum-resistant TLS protocols that use quantum-safe key exchanges and digital signatures for secure communication.

5. **Quantum Blockchain Technology**: Use blockchain with quantum-resistant algorithms to secure transactions, ensuring data integrity and transparency.

6. **Continuous Monitoring and Update**: Regularly assess and update security measures in CAV systems to stay ahead of quantum advancements.

One interesting future direction is the integration of QC with explainable AI and blockchain for secure AVs Bendiab et al. [2023].

8.4 Digital Twins

Digital Twins can serve as a tool for enhancing cybersecurity measures in electric and autonomous vehicles. By creating a virtual model that mirrors the vehicle's operations and interactions, cybersecurity professionals can simulate attacks and assess vulnerabilities in a controlled environment. This proactive approach allows for the identification and mitigation of security risks before they impact the physical vehicle Ali et al. [2023].

Simulating environments, connections, and attacks can help to understand the vulnerabilities of the system, test the effectiveness of the implemented security measures and develop new strategies to enhance the security of AVs. The advantage is that this testing can be done in a controlled environment, without the risk of damaging the physical vehicle. Yigit et al. [2024]

Proposal for digital twins not only for AVs but also for RSUs in VANETs environment, focussing on a robust real-time vehicular network framework integrating cyber twins with advanced AI models, addressing the complexities of vehicle-to-infrastructure communications Yigit et al. [2024].

9 Discussion

9.1 Research Questions

In this section, a brief answer to the research questions is provided. For each question, one or more sections are referred to where the answer is discussed in a more detailed way.

9.1.1 Question 1

What are the most significant cybersecurity threats facing autonomous vehicles, and how these threats evolve with advancements in communications and other emerging technologies? The most significant cybersecurity threats facing autonomous vehicles include sensor spoofing, remote hijacking, data breaches, and denial of service (DoS) attacks, a more detailed answer can be found in section 5. These threats evolve with advancements in vehicle-to-everything (V2X) communication and other emerging technologies, as discussed in section 8. What can be understood is that the more the technology evolves, the more the threats evolve, and there is not enough pressure on the security by design principles. The definition of a rigorous security-by-design framework, encapsulating current standards and best practices, is essential to address these threats in new technologies. Moreover, new technologies like AI and blockchain are being explored to enhance the security of AVs, but they also pose challenges in real-world applications and in case of effectiveness, they need to be regulated. Another important aspect is that the security of AVs is not only a technical issue, but also a sociotechnical one, requiring collaboration

among manufacturers, regulators, and other stakeholders to ensure comprehensive and effective security measures.

9.1.2 Question 2

What existing standards and regulatory frameworks govern cybersecurity by design in autonomous vehicles, and how effectively do they address current and future security challenges? There are standards developed by organizations such as ISO/SAE and UN-ECE WP.29 that provide guidelines for cybersecurity by design in autonomous vehicles, as discussed in section 6. These standards aim to address current and future security challenges by establishing requirements for secure software development, risk assessment, and incident response. However, there are gaps in the existing standards, such as the lack of specific guidance on emerging technologies like AI and blockchain, and the need for more comprehensive coverage of security across the entire AV lifecycle. To effectively address current and future security challenges, it is essential to continuously update and expand existing standards to keep pace with technological advancements and evolving threats.

9.1.3 Question 3

What cybersecurity solutions and practices have been implemented by autonomous vehicle manufacturers, and how do they align with best practices in secure software development and system resilience? Autonomous vehicle manufacturers have implemented various cybersecurity solutions and practices, such as intrusion detection systems, secure over-the-air updates, and encryption, as discussed in section 7. These practices align with best practices in secure software development and system resilience by integrating security measures into the software development lifecycle, monitoring for potential threats, and ensuring the integrity and confidentiality of data. However, there are challenges in implementing these practices, such as the complexity of AV systems, the use of various technologies, and the need for continuous monitoring and updates to address new vulnerabilities. The heterogeneity of AV systems and the interconnected nature of their components require a multi-faceted approach to security that combines technical solutions with organizational processes and policies. Collaboration among manufacturers to determine the best practices for secure software development and system resilience is essential to address these challenges, and heterogeneous systems need to be standardized. A common ground is essential for securing also the supply chain, which is a critical aspect of AV cybersecurity that requires close collaboration among manufacturers, suppliers, and other stakeholders to ensure the integrity and security of components and software.

9.1.4 Question 4

What future trends and emerging technologies, such as artificial intelligence and blockchain, are being explored to enhance the cybersecurity of autonomous vehicles, and what challenges do they pose in real-world applications? Future trends and emerging technologies,

such as artificial intelligence and blockchain, are being explored to enhance the cybersecurity of autonomous vehicles, as discussed in section 8. Artificial intelligence is used mainly for threat detection, adaptive security systems, and anomaly identification, while blockchain is employed maily for secure communication, data integrity, and identity management. These technologies offer promising solutions to enhance the security of AVs, but they also pose challenges in real-world applications, such as scalability, latency, energy consumption, and privacy concerns. To address these challenges, further research is needed to develop quantum-resistant cryptography, hybrid encryption techniques, and secure communication protocols that can withstand emerging threats.

10 Conclusions

This review emphasizes the critical role of cybersecurity in autonomous vehicles, which are vulnerable to a range of cyber threats. While existing defenses like intrusion detection systems, regular updates, and current standards offer some protection, they are insufficient to fully safeguard AVs from evolving threats.

Key challenges include the lack of unified security standards, latency, scalability, and resource limitations, alongside a need for robust security-by-design principles and increased collaboration among manufacturers. Persistent attacks can erode public confidence, slowing the adoption of AV technology.

To secure AVs, it's crucial to ensure data integrity, establish secure communication standards, and bolster sensor data resilience. Knowledge sharing, standardizing protocols, and joint research are essential strategies to tackle emerging vulnerabilities effectively.

Looking ahead, AV cybersecurity will likely focus on adaptive, resilient systems that can withstand attacks. Artificial intelligence, machine learning, and digital twins will be pivotal in developing real-time threat detection and automated response capabilities, while blockchain technology will enhance data integrity and secure communications. This comprehensive approach is vital to maintaining the safety, reliability, and public trust in autonomous vehicle systems also if it needs to be correctly regulated.

11 Bibliography

References

Wasyihun Sema Admass, Yirga Yayeh Munaye, and Abebe Abeshu Diro. Cyber security: State of the art, challenges and future directions. *Cybersecurity Analytics*, 3:100031, 2023. doi: 10.1016/j.csa.2023.100031. URL https://doi.org/10.1016/j.csa.2023.100031.

Akwasi Adu-Kyere, Ethiopia Nigussie, and Jouni Isoaho. Self-aware cybersecurity architecture for autonomous vehicles: Security through system-level accountability. *Sensors*, 23(21):8817, 2023. doi: 10.3390/s23218817. URL https://doi.org/10.3390/s23218817.

Jameel Ahmad, Muhammad Umer Zia, Ijaz Haider Naqvi, Jawwad Nasar Chattha, Faran Awais Butt, Tao Huang, and Wei Xiang. Machine learning and blockchain technologies for cybersecurity in connected vehicles. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2023. doi: 10.1002/widm.1515. URL https://doi.org/10.1002/widm.1515.

Theyazn H. H. Aldhyani and Hasan Alkahtani. Attacks to autonomous vehicles: A deep learning algorithm for cybersecurity. *Sensors*, 22(1):360, 2022. doi: 10.3390/s22010360. URL https://doi.org/10.3390/s22010360.

Wasim A. Ali, Maria Pia Fanti, Michele Roccotelli, and Luigi Ranieri. A review of digital twin technology for electric and autonomous vehicles. *Applied Sciences*, 13(10):5871, 2023. doi: 10.3390/app13105871. URL https://doi.org/10.3390/app13105871.

Fabio Arena and Giovanni Pau. An overview of vehicular communications. *Future Internet*, 11(2):27, 2019. doi: 10.3390/fi11020027. URL https://doi.org/10.3390/fi11020027.

Gueltoum Bendiab, Amina Hameurlaine, Georgios Germanos, Nicholas Kolokotronis, and Stavros Shiaeles. Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. *IEEE Transactions on Intelligent Transportation Systems*, 2023. doi: 10.1109/TITS.2023.3236274. URL https://doi.org/10.1109/TITS.2023.3236274.

Władysław Boruń, Marianna Jacyna, Mariusz Izdebski, and Emil Szczepański. Economic aspects of driving various types of vehicles in intelligent urban transport systems, including car-sharing services and autonomous vehicles. *Applied Sciences*, 10(16):5580, 2020. doi: 10.3390/app10165580. URL https://doi.org/10.3390/app10165580.

Mohammed Lamine Bouchouia, Houda Labiod, Ons Jelassi, Jean-Philippe Monteuuis, Wafa Ben Jaballah, Jonathan Petit, and Zonghua Zhang. A survey on misbehavior

detection for connected and autonomous vehicles. *Vehicular Communications*, 39: 100586, 2023. doi: 10.1016/j.vehcom.2023.100586. URL https://doi.org/10.1016/j.vehcom.2023.100586.

Anupam Chattopadhyay, Kwok-Yan Lam, and Yaswanth Tavva. Autonomous vehicle: Security by design. *IEEE Transactions on Intelligent Transportation Systems*, 22 (11):7015–7029, 2021. doi: 10.1109/TITS.2020.3000797. URL https://doi.org/10.1109/tits.2020.3000797.

Alois C. Knoll Christian Creß, Zhenshan Bing. Intelligent transportation systems using roadside infrastructure: A literature survey. *IEEE Transactions on Intelligent Transportation Systems*, 2023. doi: 10.1109/TITS.2023.3343434. URL https://doi.org/10.1109/tits.2023.3343434.

Gianpiero Costantino, Marco De Vincenzi, and Ilaria Matteucci. A comparative analysis of unece wp.29 r155 and iso/sae 21434. In *2022 IEEE European Symposium on Security and Privacy Workshops*, pages 340–347, 2022a. doi: 10.1109/EuroSPW55150.2022.00041. URL https://doi.org/10.1109/EuroSPW55150.2022.00041.

Gianpiero Costantino, Marco De Vincenzi, and Ilaria Matteucci. In-depth exploration of iso/sae 21434 and its correlations with existing standards. *IEEE Communications Standards Magazine*, 6(1):84–92, 2022b. doi: 10.1109/MCOMSTD.0001.2100080. URL https://doi.org/10.1109/MCOMSTD.0001.2100080.

Defense Advanced Research Projects Agency (DARPA). *DARPA's Grand Challenges Program: A Historical Perspective*. DARPA Publications, 2007. ISBN 978-3-540-73428-4.

Department of Transportation of the United States of America. Vehicle-to-vehicle (v2v) communications for safety, 2021. URL https://www.its.dot.gov/research_archives/safety/v2v_comm_plan.htm. Accessed: 2024-10-10.

Department of Transportation of the United States of America. Vehicle-to-infrastructure (v2i) resources, 2024. URL https://www.its.dot.gov/v2i/index.htm. Accessed: 2024-10-10.

Irmina Durlik, Tymoteusz Miller, Ewelina Kostecka, Zenon Zwierzewicz, and Adrianna Łobodzińska. Cybersecurity in autonomous vehicles—are we ready for the challenge? *Electronics*, 13(13):2654, 2022. doi: 10.3390/electronics13132654. URL https://doi.org/10.3390/electronics13132654.

Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity attacks in vehicular sensors. *IEEE Sensors Journal*, 20(22):13752–13767, 2020. doi: 10.1109/JSEN.2020.3004275. URL https://doi.org/10.1109/JSEN.2020.3004275.

Asif Faisal, Md Kamruzzaman, Tan Yigitcanlar, and Graham Currie. Understanding autonomous vehicles. *Journal of Transport and Land Use*, 12(1):45–72, 2019. doi: 10.5198/jtlu.2019.1405. URL https://doi.org/10.5198/jtlu.2019.1405.

Aurélien Francillon, Boris Danev, and Srdjan Capkun. Fast, furious and insecure: Passive keyless entry and start systems in modern supercars. In *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*, pages 997–1008. ACM, 2011. doi: 10.13154/tches.v2019.i3.66-85. URL https://doi.org/10.13154/tches.v2019.i3.66-85.

Flavio D. Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. Lock it and still lose it—on the (in)security of automotive remote keyless entry systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*, pages 1601–1612. ACM, 2016. ISBN 978-1-931971-32-4. URL https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_garcia.pdf.

Amrita Ghosal, Subir Halder, and Mauro Conti. Stride: Scalable and secure over-the-air software update scheme for autonomous vehicles. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pages 1–6, 2020. doi: 10.1109/ICC40277.2020.9148649. URL https://doi.org/10.1109/ICC40277.2020.9148649.

Anastasios Giannaros, Aristeidis Karras, Leonidas Theodorakopoulos, Christos Karras, Panagiotis Kranias, Nikolaos Schizas, Gerasimos Kalogeratos, and Dimitrios Tsolis. Autonomous vehicles: Sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. *Journal of Cybersecurity and Privacy*, 3(3):433–463, 2023. doi: 10.3390/jcp3030025. URL https://doi.org/10.3390/jcp3030025.

Mansi Girdhar, Junho Hong, and John Moore. Cybersecurity of autonomous vehicles: A systematic literature review of adversarial attacks and defense models. *IEEE Open Journal of Vehicular Technology*, 4:417–437, 2023. doi: 10.1109/OJVT.2023.3265363. URL https://doi.org/10.1109/OJVT.2023.3265363.

M. Nadeem Ahangar; Qasim Z. Ahmed; Fahd A. Khan; Maryam Hafeez. A survey of autonomous vehicles: Enabling communication technologies and challenges. *Sensors*, 21 (1):123, 2021. doi: 10.3390/s21030706. URL https://doi.org/10.3390/s21030706.

Mona Hellstern, Stefan Langhanki, Florian Grün, Reiner Kriesten, and Eric Sax. Cybersecurity approval criteria: Application of un r155. In *SAE Technical Paper 2024-01-2983*, pages 1–9. SAE International, 2024. doi: 10.4271/2024-01-2983. URL https://doi.org/10.4271/2024-01-2983.

Safras Iqbal, Peter Ball, Muhammad H Kamarudin, and Andrew Bradley. Simulating malicious attacks on vanets for connected and autonomous vehicle cybersecurity: A machine learning dataset. In *2022 13th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pages 332–337,

2022. doi: 10.1109/CSNDSP54353.2022.9908023. URL https://doi.org/10.1109/CSNDSP54353.2022.9908023.

Shah Khalid Khan, Nirajan Shiwakoti, Peter Stasinopoulos, and Yilun Chen. Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness, and future directions. *Accident Analysis & Prevention*, 144:105837, 2020. doi: 10.1016/j.aap.2020.105837. URL https://doi.org/10.1016/j.aap.2020.105837.

U. Kiencke, S. Dais, and M. Litschel. Automotive serial controller area network. Technical Report 860391, SAE Technical Paper, 1986. URL https://doi.org/10.4271/860391.

Kyounggon Kim, Jun Seok Kim, Seonghoon Jeong, Jo-Hee Park, and Huy Kang Kim. Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, 102:102150, 2020. doi: 10.1016/j.cose.2020.102150. URL https://doi.org/10.1016/j.cose.2020.102150.

Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, and Sudeep Pasricha. Roadmap for cybersecurity in autonomous vehicles. *IEEE Consumer Electronics Magazine*, 11 (6):13–23, 2022. doi: 10.1109/MCE.2022.3154346. URL https://doi.org/10.1109/MCE.2022.3154346.

Bruno Macena, Celio Albuquerque, and Raphael Machado. Cybersecurity and privacy protection in vehicular networks (vanets). *Advances in Internet of Things*, 13(4):49–58, 2023. doi: 10.4236/ait.2023.134006. URL https://doi.org/10.4236/ait.2023.134006.

Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. Technical report, IOActive, 2015. URL https://illmatics.com/Remote%20Car%20Hacking.pdf.

Lama J. Moukahal, Mohammad Zulkernine, and Martin Soukup. Towards a secure software lifecycle for autonomous vehicles. In *2021 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*, pages 1–6. IEEE, 2021. doi: 10.1109/ISSREW53611.2021.00104. URL https://doi.org/10.1109/ISSREW53611.2021.00104.

Jay Nagarajan, Pegah Mansourian, Muhammad Anwar Shahid, Arunita Jaekel, Ikjot Saini, Ning Zhang, and Marc Kneppers. Machine learning based intrusion detection systems for connected autonomous vehicles: A survey. *Journal of Network and Systems Management*, 31:1–32, 2023. doi: 10.1007/s12083-023-01508-7. URL https://doi.org/10.1007/s12083-023-01508-7.

D. Payton. An architecture for reflexive autonomous vehicle control. In *Proceedings. 1986 IEEE International Conference on Robotics and Automation*, volume 3, pages 1838–1845, 1986. doi: 10.1109/ROBOT.1986.1087458. URL https://doi.org/10.1109/ROBOT.1986.1087458.

Scott Drew Pendleton. Perception, planning, control, and coordination for autonomous vehicles. *Machines*, 5(1):6, 2017. doi: 10.3390/machines5010006. URL https://doi.org/10.3390/machines5010006.

Sai Sreekar Penumarthy, Yulong Fei, Hong Yu, and Zonghua Zhang. A connected and autonomous vehicle reference architecture for attack surface analysis. *Applied Sciences*, 9(23):5101, 2020. doi: 10.3390/app9235101. URL https://doi.org/10.3390/app9235101.

James Gillanders Prinkle Sharma. Cybersecurity and forensics in connected autonomous vehicles: A review of the state-of-the-art. *IEEE Access*, 10:110255–110270, 2022. doi: 10.1109/ACCESS.2022.3213843. URL https://doi.org/10.1109/ACCESS.2022.3213843.

SAE International. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Technical Report J3016C, SAE International, 2021. URL https://www.sae.org/standards/content/j3016_202104/. Issued 2014-01-16. Revised 2016-09-30; 2018-06-15; 2021-04-30.

Bruce Schneier. The internet of things is wildly insecure — and often unpatchable. *Wired*, January 6 2014. URL https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

Weiqing Sun Shahida Malik. Analysis and simulation of cyber attacks against connected and autonomous vehicles. In *2020 IEEE MetroCAD*, pages 1–5. IEEE, 2020. doi: 10.1109/MetroCAD48866.2020.00018. URL https://doi.org/10.1109/MetroCAD48866.2020.00018.

Muhammad Sameer Sheikh and Jun Liang. A comprehensive survey on vanet security services in traffic management system. *Wireless Communications and Mobile Computing*, 2019:1–17, 2019. doi: 10.1155/2019/2423915. URL https://doi.org/10.1155/2019/2423915.

Steven E. Shladover. Connected and automated vehicle systems: Introduction and overview. *Journal of Intelligent Transportation Systems*, 22(3):190–200, 2017. doi: 10.1080/15472450.2017.1336053. URL https://doi.org/10.1080/15472450.2017.1336053.

P.V. Sontakke and N.B. Chopade. Impact and analysis of denial-of-service attack on an autonomous vehicle test bed setup. In A.P. Pandian, R. Palanisamy, M. Narayanan, and T. Senjyu, editors, *Proceedings of Third International Conference on Intelligent Computing, Information and Control Systems*, volume 1415 of *Advances in Intelligent Systems and Computing*, pages 178–189. Springer, Singapore, 2022. doi: 10.1007/978-981-16-7330-6_17. URL https://doi.org/10.1007/978-981-16-7330-6_17.

Amin Tahmasbi-Sarvestani, Hossein Nourkhiz Mahjoub, Yaser P. Fallah, Ehsan Moradi-Pari, and Oubada Abuchaar. Implementation and evaluation of a cooperative vehicle-to-pedestrian safety application. *IEEE Intelligent Transportation Systems Magazine*, 9

(4):62–75, 2017. doi: 10.1109/MITS.2017.2743201. URL https://doi.org/10.1109/MITS.2017.2743201.

Eric R. Teoh and David G. Kidd. Rage against the machine? google's self-driving cars versus human drivers. *Journal of Safety Research*, 63:57–60, 2017. doi: 10.1016/j.jsr.2017.08.008. URL https://doi.org/10.1016/j.jsr.2017.08.008.

Elena Thomas, Connie McCrudden, Zachary Wharton, and Ardhendu Behera. Perception of autonomous vehicles by the modern society: a survey. *IET Intelligent Transport Systems*, 14(11):1351–1360, 2020. doi: 10.1049/iet-its.2019.0703. URL https://doi.org/10.1049/iet-its.2019.0703.

Russell G. Thompson, Mark Stevenson, and Lauren A. Shluzas. The impact of autonomous vehicles on cities: A review. *Journal of Urban Technology*, 25(4):3–20, 2018. doi: 10.1080/10630732.2018.1493883. URL https://doi.org/10.1080/10630732.2018.1493883.

Qun Wang, Haijian Sun, Rose Qingyang Hu, and Arupjyoti Bhuyan. When machine learning meets spectrum sharing security: Methodologies and challenges. *IEEE Open Journal of the Communications Society*, 3:292–308, 2022. doi: 10.1109/OJCOMS.2022.3146364. URL https://doi.org/10.1109/OJCOMS.2022.3146364.

C. Wu, T. Yoshinaga, Y. Ji, and Y. Zhang. Computational intelligence inspired data delivery for vehicle-to-roadside communications. *IEEE Transactions on Vehicular Technology*, 67(12):12038–12048, 2018. doi: 10.1109/TVT.2018.2871606. URL http://dx.doi.org/10.1109/TVT.2018.2871606.

Yagmur Yigit, Ioannis Panitsas, Leandros Maglaras, Leandros Tassiulas, and Berk Canberk. Cyber-twin: Digital twin-boosted autonomous attack detection for vehicular ad-hoc networks. In *2024 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2024. doi: 10.1109/ICC51166.2024.10622784. URL https://doi.org/10.1109/ICC51166.2024.10622784.

Mingming Yu, Zhen Guo, Shiwen Shen, Yuqiao Ning, Tianling Liu, and Dongqing Sun. An intelligent connected vehicles information security attack matrix model. In *2023 IEEE 5th International Conference on Power, Intelligent Computing and Systems (ICPICS)*, pages 82–86, 2023. doi: 10.1109/ICPICS58376.2023.10235357. URL https://doi.org/10.1109/ICPICS58376.2023.10235357.

Y. Zheng, Y. Zhang, B. Ran, Y. Xu, and X. Qu. Cooperative control strategies to stabilise the freeway mixed traffic stability and improve traffic throughput in an intelligent roadside system environment. *IET Intelligent Transport Systems*, 14(9):1108–1115, 2020. doi: 10.1049/iet-its.2019.0577. URL https://doi.org/10.1049/iet-its.2019.0577.

Acronym	Definition
AV	Autonomous Vehicle
V2X	Vehicle-to-Everything
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2P	Vehicle-to-Pedestrian
V2R	Vehicle-to-Roadside
IDPS	Intrusion Detection and Prevention System
OTA	Over-the-Air
LOC	Lines of Code
AI	Artificial Intelligence
ML	Machine Learning
E/E	Electrical/Electronic
ADS	Automated Driving System
DDT	Dynamic Driving Task
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
V&V	Verification and Validation
R&D	Research and Development
ISO	International Organization for Standardization
SAE	Society of Automotive Engineers
UNECE	United Nations Economic Commission for Europe
USDOT	United States Department of Transportation
WP.29	World Forum for Harmonization of Vehicle Regulations
CSMS	Cybersecurity Management System
ITS	Intelligent Transportation Systems
VSOC	Vehicle System Operator Control
CAV	Connected and Autonomous Vehicle
VANET	Vehicular Ad-Hoc Network
MANNET	Mobile Ad-Hoc Network
OBU	On-Board Unit
RSU	Road-Side Unit
TA	Trusted Authority
BSD	Blind Spot Detection
LDW	Lane Departure Warning
FCW	Forward Collision Warning
AEB	Autonomous Emergency Braking
FCWS	Forward Collision Warning System
WPAN	Wireless Personal Area Network
DSRC	Dedicated Short-Range Communication
MIVC	Multi-Interface Vehicular Communication
SIVC	Single-Interface Vehicular Communication
CAN	Controller Area Network
LiDAR	Light Detection and Ranging
CIA	Confidentiality, Integrity, and Availability
DDoS	Distributed Denial of Service
DLP	Density-Based Location Privacy
SDLC	Software Development Life Cycle
QC	Quantum Computing
QRNG	Quantum Random Number Generator
QKD	Quantum Key Distribution
DT	Digital Twin

Table 3: Definitions of Key Acronyms

Term	Definition
Vulnerability	A weakness of a process that can be exploited by malicious actors.
Threat	A potential danger that breach security and negatively affect an organization.
Threat Model	A structured representation of all possible threats to a system.
Risk	The potential for loss, damage, or destruction of assets.
Threshold	Minimum level of security that must be maintained according to the threat model.
Attack	An attempt to exploit a vulnerability in a system.
Countermeasure	A security control implemented to prevent or mitigate the impact of a threat.
Incident	An event that compromises the confidentiality, integrity, or availability.
Attack surface	All possible points that an attacker can exploit to breach security.
Malicious actor	An individual or group that intentionally breaches security.

Table 4: Definitions of Key Cybersecurity Terms