Educational Administration: Theory and Practice
2024, 30(5), 12823-12830
ISSN: 2148-2403
https://kuey.net/

Research Article

Educational Administration Theory and Practice

Exploring Cyber Threats Associated With Autonomous And Connected Vehicles

Prof. Pradnya Kashikar[1], Dr. Samita Mahapatra[2], Ms. Latha Chandran[3*]

[1] Research Scholar, MIT ADT University, Loni-Kalbhor, Pune- India. Email: pradnyakashikar@gmail.com
[2]Ph.D. Guide & Assistant Professor, MIT ADT University, Loni-Kalbhor, Pune- India. Email: samita.mahapatra@mituniversity.edu.in
[3] *Technology Specialist, Trivandrum, Kerala, India. Email: lathachandran181@gmail.com

Citation **:**, Ms. Latha Chandran, et al(2024),. Exploring Cyber Threats Associated With Autonomous And Connected Vehicles, *Educational Administration: Theory and Practice*, *30*(5), 12823-12830, Doi: 10.53555/kuey.v30i5.5418

ARTICLE INFO **ABSTRACT**

Autonomous and connected vehicles (ACVs) are transforming the transportation industry by increasing efficiency, reducing costs, and improving safety. However, these developments also create new vulnerabilities and expose ACVs to cyber threats. The consequences of these threats range from mere inconvenience to severe accidents, highlighting the urgent need to address the issue of cyber security in ACVs. This literature review aims to provide an overview of the current research on cyber threats for ACVs to create awareness about the major vulnerabilities faced by modern vehicles. The review covers various types of cyber threats, such as attacks on sensors, communication networks, and control systems, and countermeasures to mitigate these threats.

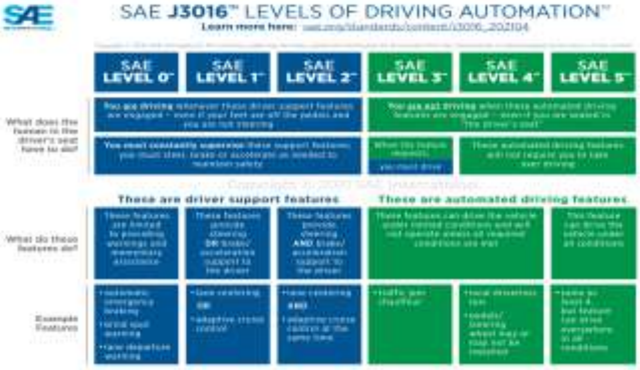
Keywords: Cyber Threats, Autonomous, Connected Vehicles, Vulnerabilities.

I. INTRODUCTION

In today's era where technology is revolutionizing human life by making life easier with new innovative developments, autonomous and connected cars are no less a wonder. Earlier, vehicle drivers just needed to focus on roads to avoid unsafe conditions, however, with the incorporation of Electronic Control Units (ECU), safety is a major concern. The purpose of the ECU is to collect the sensor data and perform the desired task as per the requirements. Several Standards like Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (IEC 61508) and later Road vehicles – Functional safety (ISO 26262) is introduced and mandated for the development of software and hardware components for ECUs which emphasize the safety of electrical and electronics systems. With the introduction of connected cars, security is also a major concern which could have financial, operational, privacy, and safety impacts. This review focuses on the threats and vulnerabilities related to autonomous and connected vehicles and the countermeasures. Let us start with a brief introduction of important terminologies used in this review.

Autonomous vehicles, also known as self-driving cars, are vehicles capable of operating without human intervention by sensing their environment using technologies such as LiDARs, RADARs, Cameras, GPS, other sensors, and machine learning algorithms, to detect and respond to their surroundings. Autonomy in vehicles is divided into six levels according to a system developed by SAE International (SAE J3016).In this paper, the term 'vehicle' is used to refer to autonomous and connected cars. This review does not consider the oader

Figure 1: SAE J3016: - LEVELS OF DRIVING AUTOMATION2


SAE
SAE J3016™ LEVELS OF DRIVING AUTOMATION™
Learn more here:
SAE LEVEL 0™
SAE LEVEL 1™
SAE LEVEL 2™
SAE LEVEL 3™
SAE LEVEL 4™
SAE LEVEL 5™
What does the human in the driver's seat have to do?
These are driver support features
These are automated driving features
What do these features do?
Example Features

From levels 3-5, vehicles have automated driving features which is the focus of this article. Connected vehicles refer to vehicles that can communicate with other vehicles, infrastructure, and devices using Wi-Fi or cellular networks. Connected vehicles can exchange information about their location, speed, and direction of travel, which can be used to improve road safety and optimize traffic flow. Connected vehicles can also provide real-time information to drivers about traffic conditions, weather, and other factors that may affect their journey. This is made possible with several sensors in the vehicle.

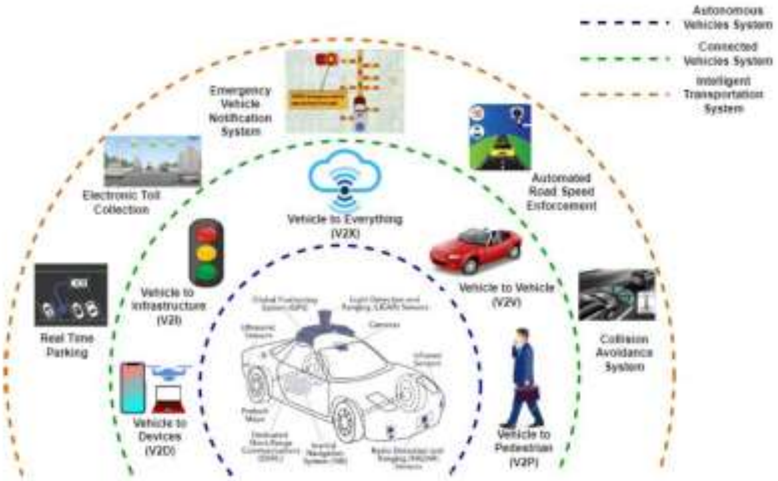

Autonomous Vehicles System
Connected Vehicles System
Intelligent Transportation System
Emergency Vehicle Notification System
Electronic Toll Collection
Automated Road Speed Enforcement
Vehicle to Everything (V2X)
Vehicle to Infrastructure (V2I)
Vehicle to Vehicle (V2V)
Real Time Parking
Collision Avoidance System
Vehicle to Devices (V2D)
Vehicle to Pedestrian (V2P)
Cameras

Figure 2: Overview of connected automated system vehicle infrastructure. 5

Cyber threats refer to any malicious act by a person/thing that possess danger to the assets in terms of confidentiality, integrity, and availability by exploiting the vulnerabilities. A lot of research effort is being invested in identifying vulnerabilities related to different sensors, controls, and connection mechanisms and recommending potential mitigation techniques for connected cars. Cyber-attacks on connected and autonomous cars can also have wider implications for road safety and traffic management.

II. LITERATURE REVIEW

This section provides a comprehensive review of the literature associated with cyber threats on autonomous and connected cars. In Threats and Attacks to Modern Vehicles 6, authors categorize the different sets of systems in ACVs as Control, Communication, and Sensing and layer those into a pyramid. This is depicted in Figure 3.

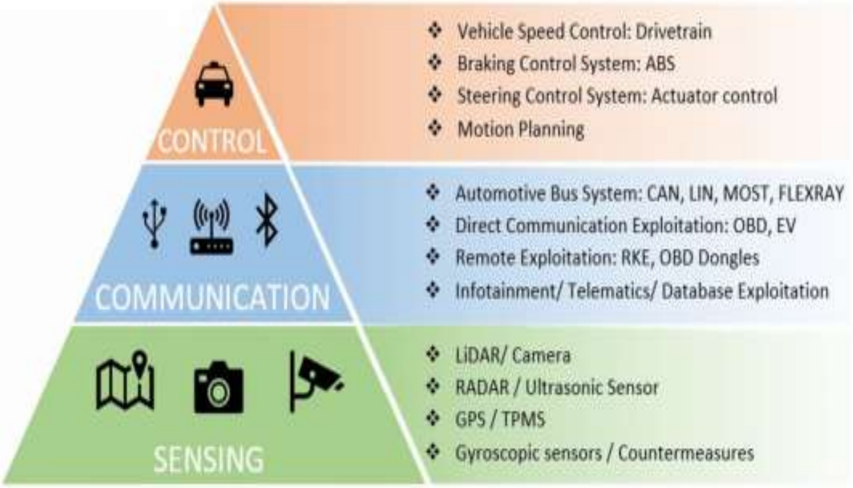

CONTROL
Vehicle Speed Control: Drivetrain
Braking Control System: ABS
Steering Control System: Actuator control
Motion Planning
COMMUNICATION
Automotive Bus System: CAN, LIN, MOST, FLEXRAY
Direct Communication Exploitation: OBD, EV
Remote Exploitation: RKE, OBD Dongles
Infotainment/ Telematics/ Database Exploitation
SENSING
LiDAR/ Camera
RADAR / Ultrasonic Sensor
GPS / TPMS
Gyroscopic sensors / Countermeasures

Figure 3: The Autonomous Vehicular Sensing-Communication-Control (AutoVSCC) 6

The authors discuss in detail the threats related to each of the layers- the sensing, communication layers, and control and the corresponding countermeasures. An overview of important threats related to each of these layers is discussed below.

A. Threats on Sensing Layer

Autonomous connected cars rely heavily on sensing systems to gather data about the environment and make decisions about driving actions. However, the sensing layer of an autonomous connected car is also vulnerable to cyber threats. Hackers can exploit vulnerabilities in the sensing systems to gain access to sensitive data or to take control of the car.

The cyber threats to the sensing layer of an autonomous connected car discussed here include environmental sensors, such as GPS, Cameras, LiDARs, and vehicle dynamic sensors such as magnetic encoders, inertial sensors, and Tyre Pressure Monitoring Systems (TPMS)11.

1) GPS:

GPS (Global Positioning System) is a critical component in autonomous connected cars. It provides real-time location and navigation data. GPS is vulnerable to cyber threats, which can result in incorrect location data or even loss of GPS connectivity. As GPS is an open standard and is freely accessible, the authors of 7 highlight the easiness of generating rogue signals by hackers to mislead or jam the GPS. This is termed as Jamming and Spoofing attacks on GPS. Authors of 6 define a spoofing attack as a situation in which a person or program is successfully identified as another by falsifying data, to gain an illegitimate advantage. GPS spoofing happens when someone uses a radio transmitter (SDR) to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal. 8 also mention spoofing and jamming as one major threat to in-vehicle elements. The spoofing attack is illustrated in Figure 4:Illustration of Spoofing attack7. Jamming is done by sending noise on the GPS channel to disable the GPS.

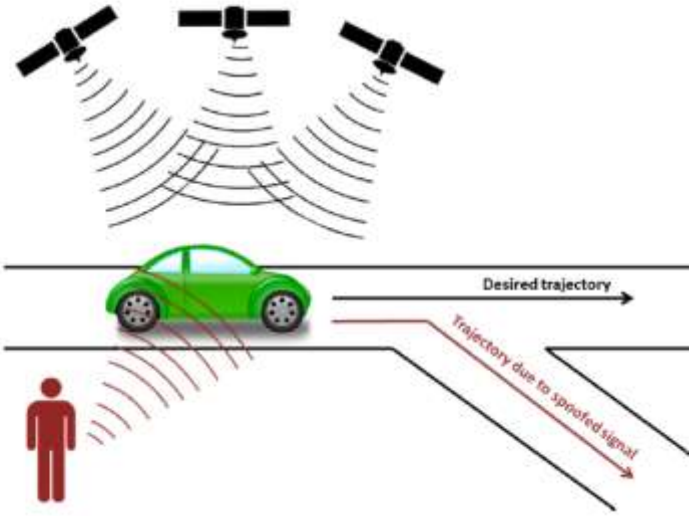


Figure 4: Illustration of Spoofing attack7

Defence mechanisms for GPS threats are summarised in the below table. The studies also highlight that currently available devices are still in danger of spoofing and jamming attacks. Jamming attacks are easier to notice since the ACVs change their direction abruptly.

TABLE 1: GPS THREATS AND DEFENCES610

Attacks on GPS	**Defence Mechanisms**
GPS Spoofing	Advanced Signal-Processing-Based Techniques for a Single-Antenna Receiver
	Encryption-Based Defences
	Defences Based on Drift Monitoring
	Signal-Geometry-Based Defences
	Multipronged Spoofing Defences Strategies
GPS Jamming	Using secondary measurement systems

2) LiDAR:

LiDAR (Light Detection and Ranging) sensors use eye-safe laser beams to generate a 3D map of the vehicle's environment for localization, obstacle avoidance, and navigation. However, there is no guarantee of the validity of the constructed 3D model. The authors of 7 highlight the Spoofing and jamming attacks on LiDARs.

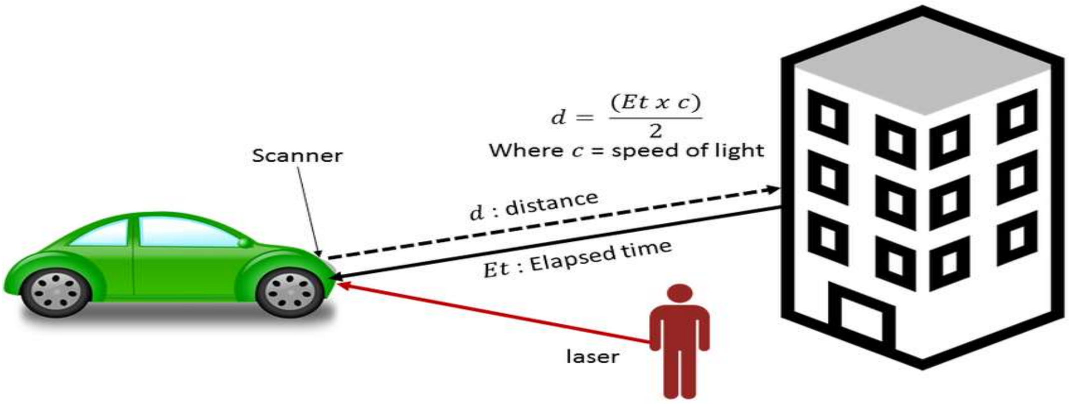


Figure 5:illustration of LiDAR System

Different Attacks on LiDAR are summarised11 in the below table based on 1112

TABLE 2: ATTACKS ON LIDAR [11][12]

Attacks on LiDAR	Description
Replay Attack	Attackers can receive and record signals sent by the LiDAR which enables attackers to initiate a replay attack by sending the recorded signals back to the LiDAR to cause the LiDAR to map non-existent objects.
Relay Attack	Replay attacks are extended to carry out a relay attack. The received signals are sent to the receiver at a different location which leads to the interruption of the lidar.
Spoofing Attack	Spoofing attacks cause LiDARs to detect non-existent objects.
Jamming Attack	This type of Attack directly emits light back at the scanner unit on the vehicle that uses the same frequency band as the laser.
Denial of Service attack (DoS)	Attackers can conduct denial of service attacks on LiDARs by injecting an enormous number of fake objects created using jamming or spoofing

In 13, authors showcase an experimental setup where they conducted a spoofing attack on Velodyne's LiDAR. A similar attack has been discussed in 714, where researchers from the University of Cork managed to compromise a LiDAR laser using low-cost hardware (Raspberry Pi and a low-power laser), and also manage to make the vehicle's control unit assume that there is a large object in front of the vehicle and force it to stop.
The defence mechanism suggested by authors of 7 is to utilize different wavelengths to reduce the potential for jamming and spoofing attacks. Another approach suggested in 11 is to modulate the LiDAR laser with side-channel information, thereby preventing attackers from injecting false reflection signals since they do not know the side channel's secret key.

3) Camera Sensor Attacks:

In autonomous and connected vehicles (ACVs), cameras play a crucial role in detecting obstacles, recognizing objects, and providing a 360-degree view when combined with other sensors7. These sensors help in detecting traffic signs, identifying objects that are difficult to see in low-light conditions, assisting drivers in parking by showing nearby obstacles, and avoiding collisions by tracking nearby objects and verifying the accuracy of data from other sensors11. The researchers classify the camera sensor attacks as blinding and auto-control attacks. A blinding attack involves using a powerful laser beam to obstruct the camera feed, causing complete blindness to the vehicular sensory inputs15. On the other hand, Auto-Control Attack involves the continuous emission of bursts of light directed at the camera to manipulate the auto controls, causing instability in the image.
In 7, the authors highlight different events due to camera blinding such as the recent tragic events of Tesla where neither the car nor the driver identified a white commercial trailer against the brightly lit sky. So, an attacker can perform an attack of this nature by directing a bright light at a vehicle.
The Defence Mechanism proposed by authors of 15 is by incorporating multiple cameras with the same view and near-infrared light filters for eliminating infrared light interference during daylight hours. Another mechanism recommended in 7 is the usage of multiple cameras in different locations of vehicles.

4) Vehicle dynamics sensor attacks:

Vehicle dynamics sensors such as magnetic encoders, inertial sensors, and Tyre Pressure Monitoring Systems (TPMSs) provide measurements of a vehicle's state. Authors of 11 list different attacks and countermeasures on Vehicle dynamic sensors.

One type of Magnetic encoder mentioned is the wheel speed sensor which measures the wheel's rotational speed using magnetoresistance Integrated Circuits and is often used within Anti-Lock Braking Systems (ABS). Inertial sensors include acceleration sensors and rotation-rate sensors (gyroscopes). TPMS includes four Tyre pressure monitoring sensors for each tyre and a receiving unit. Packets are sent by TPM Sensors with sensor ID, temperature, and pressure data to receiving unit.

Attacks on Vehicle dynamic sensors are summarised in the below table

TABLE 3: ATTACKS AND DEFENCE MECHANISMS ON VEHICLE DYNAMIC SENSORS.11

Sensors	Attacks	Defence Mechanisms
Magnetic Encoders	**Disruptive Attack:** Attacker disrupts the magnetic field by placing an electromagnetic actuator in the magnetic field.	- Checking signal limits
	Spoofing Attack: The attacker shields the original magnetic field by placing an electromagnetic actuator so that the malicious magnetic field will have a significant effect on the output of speed sensor. This can lead to Eavesdropping attack as attacker can spoof the pressure reading such that driver must stop the vehicle for checking.	- Physical Challenge-Response Authentication
Inertial Sensors	**Spoofing Attack:** attacker inject sound waves to deceive inertial sensors using speakers or transducers, directivity horns, and amplifiers	- Creating a physical barrier against the noise, utilizing differential comparator, & tuning the resonance frequency.
	Acoustic Attack: Attackers target gyroscopes and accelerometers which have a load resonant frequency and then falsify acoustic waves with a frequency matching the load resonant frequency of the cyber-physical system.	- Low-pass filter - Secure amplifier - Acoustic dampening materials - Software defense mechanism
Tyre Pressure Monitoring Systems	**Reverse-Engineering Attack:** Attackers deconstruct vehicular systems and reverse-engineer the vehicle firmware to find vulnerabilities to carry out future attacks such as replay and relay attacks	- Basic error checking, detect when conflicting information has been received, and filter out false activation signals.
	Spoofing Attack: Attackers gain unauthorized entry to TPMSs and modify tyre pressure sensor measurements.	- Encryption for TPMS packets
	Eavesdropping Attack: Attackers monitor sensor readings and transmissions. Eavesdropping threatens location privacy, as each TPMS sensor has a sensor ID that remains fixed for the duration of its lifetime.	- Allow TPMSs to broadcast only when the wheel is at an orientation that limits signal propagation.

B. Threats on the Communication Layer

The communication layer on ACVs handles the connectivity and routing of messages among the devices. The communication Layer on ACVs can be broadly classified into In-Vehicle communication (IVC) and Vehicle to Others (V2X) communication. Communications in a connected car environment as per 16 are depicted below.

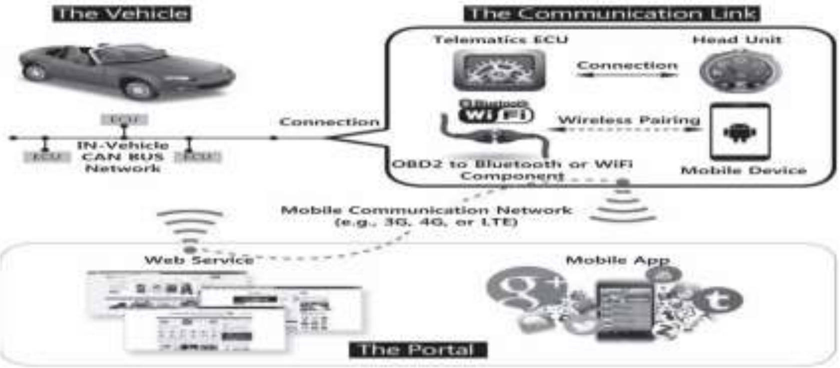


Figure 6: Connected Car Environment16

Controller Area Network (CAN), FlexRay, LIN, and automotive Ethernet are popular protocols for in-vehicle communication networks (IVNs) for connecting the ECUs. However, these protocols were not designed with security in mind and hence have several vulnerabilities, such as a lack of message authentication, lack of message encryption, and an ID-based arbitration mechanism for contention resolution.

The major attacks on CAN communication are listed in 6 since CAN is a widely used protocol for creating efficient networks of Electronic Control Units (ECUs). To provide an overview of the CAN protocol, it functions by allowing any device in the network to generate a "data frame" using a standardized message format and transmitting it sequentially. If multiple devices transmit simultaneously, the device with the highest priority proceeds while the others wait. The frames are received by all ECU nodes in the network and contain an ID, a message, and other elements such as error correction bits.
The vulnerabilities in the CAN network are the usage of multicast messages (any node can receive the message), lack of authentication of nodes, lack of encryption of messages, and lack of node registration.

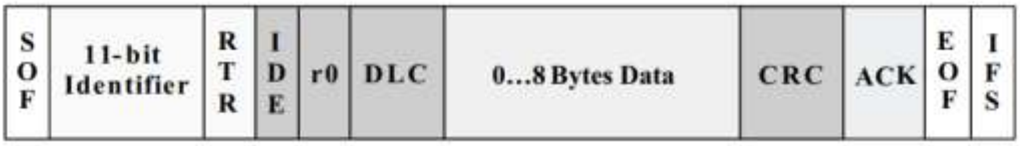


Figure 7: Standard CAN Frame19

Major attacks on in-vehicle communication are
1) Frame Sniffing: A compromised node can intercept all frames transmitted via the CAN bus and access an in-vehicle network through available interfaces, allowing attackers to discover different functions and weaknesses in selected Electronic Control Units (ECUs).17
2) Frame Falsifying: Attackers can send fake frames via the CAN bus containing false data, such as changing the speedometer reading or displaying failure information on the instrument panel cluster, misleading legitimate ECUs and potentially causing dangerous behaviour.17
3) Frame Injection: Attackers can use a malicious node, such as a laptop connecting the On-board Diagnostic (OBD) port, a reprogrammed ECU, or an infected telematics system, to inject frames to the network, setting appropriate frame IDs to make the target node accept these fake frames.17
4) Replay Attack: An attacker can intercept a valid message and replay it later to manipulate the system to perform actions such as opening the door, starting the engine, and driving the car away.17
5) DoS Attack: Attackers can abuse the frame ID to command the malicious node to broadcast a frame with high priority all the time, disabling communication of individual components on the CAN bus via a DoS attack.17
6) Physical Layer Attacks: This attack involves physically tampering with the CAN bus network, such as by cutting wires or inserting a device to intercept or manipulate the signals on the network.
7) Spoofing attack: An attacker can impersonate a legitimate ECU by sending messages with a spoofed ID, leading to unauthorized access to the system.17

The Famous Jeep Chrysler cyber security attack is also an example of attacks through the CAN network. Defence mechanisms proposed for in-vehicle communication network attacks are summarised below.
1) Authentication: To prevent message injection and manipulation attacks, authentication can be used to verify the identity of the sender and receiver of messages on the CAN bus network.6
2) Encryption: To protect sensitive data from being intercepted and manipulated, encryption can be used to encrypt messages sent over the CAN bus network.6
3) Physical security measures: Physical security measures such as tamper-proof enclosures and shielding can be used to protect the physical network from physical layer attacks.

In addition to the above-listed attacks, authors of 5 list the threats/attacks on Vehicle to Other network (V2X) communication also Sybil Attacks, Remote Attacks, Relay attacks, Malware, Impersonation Attacks, Man-In-The-Middle Attacks, and Black Hole attacks.

C. Threats to Control Layer

Threats to any of the sensing and communication layers can largely affect the control layer. The authors of [6] mention that the control layer of autonomous connected cars is vulnerable to attacks, which can have catastrophic consequences, such as compromising the car's steering, brakes, engine, and transmission. Attacks on the control layer can occur through physical tampering or by compromising the sensing and communication layers. Control override attacks attempt to take control of the vehicle from the driver, while injection attacks involve injecting malicious messages into the in-vehicle network. In-vehicle network access attacks involve gaining access to the OBD port, which provides access to the in-vehicle network and can lead to the installation of malware.
Countermeasures for control layer attacks include designing cars in a way that makes it difficult for attackers to access internal components, such as OBD ports, USB, wireless/remote, and electrical charging. Code obfuscation and proper code signing could be implemented to prevent unauthorized code, and only certified and well-tested apps should be allowed to connect with the car's internal organs. More secure designs and

implementations of the smartphone to in-vehicle infotainment platforms are also recommended to prevent injection attacks6. Bosch Car Dongle cyber security attack is an example of attacks through OBD ports.

III. CONCLUSIONS

Till 2020, automotive OEMS were focusing only on the Functional Safety of vehicles which mainly deals with the development of safety-related electrical and electronic systems in road vehicles. The emergence of autonomous and connected cars has brought many benefits, including enhanced safety, convenience, and efficiency. However, cyber security risk which can cause physical harm to drivers and passengers, as well as financial and reputational damage to car manufacturers has increased. So, compliance for vehicle networks to security pillars - confidentiality, integrity, availability and authenticity, and non-repudiation is very important. An international security standard ISO 21434 was introduced in the year 2020 that focuses on cybersecurity in the automotive industry, specifically for connected and automated vehicles. It provides a framework for addressing cybersecurity risks throughout the entire automotive development process of vehicle systems, from concept and design to production and operation. Development for ACVs will start with asset identification and Threat Analysis and Risk assessment (TARA) for each of the identified assets and derivation of cyber security goals. As per one of the experienced professional in the automotive Functional Safety domain, the researchers recommend an improvised standard consolidating functional safety and cyber security standards for ACV developments. In the current software industry, it is observed that system development, software development, cyber security, and functional safety team works as different teams, and communicate through only requirements. A more collaborative approach comprising functional safety and cyber security process is desired. Automotive software development methodology standard AUTOSAR also provides a framework for implementing security measures in the underlying hardware and operating system.

The rapidly changing and fast-growing automobile sector is highly impacted by the information technology adoption in an exponential and transformational manner. The connected and Autonomous cars will be in demand considering the high performance and efficiency expectations of the consumers. The over-the -air updates and V2V and V2I networks are susceptible to cyber attacks. Moreover, cybersecurity is one of the most complex and dynamic fields in the data-driven world, involving a constant battle between hackers and defenders. As internet connectivity reaches every corner of our lives, cybersecurity is now an essential component for automobiles. Yet, many are surprised to find out that cybersecurity in the automotive industry is entirely different from what we are used to encountering in the IT industry, and this means that there are challenges in terms of preparation and prevention. The researchers attempted to indicate the possible threats due to cyber security issues in automotive industry; and the factors impacting the vehicular network security.

References

1. M. Guériau and I. Dusparic, "Quantifying the impact of connected and autonomous vehicles on traffic efficiency and safety in mixed traffic," 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 2020, pp. 1-8, doi: 10.1109/ITSC45102.2020.9294174.
2. sae-updates-j3016-automated-driving-graphic. [CrossRef]
3. CAAT Staff. "Automated and Connected Vehicles". autocaat.org
4. Sun, X.; Yu, F.R.; Zhang, P. A Survey on Cyber-Security of Connected and Autonomous Vehicles (CAVs). IEEE Trans. Intell. Transp. Syst. 2021, 23, 6240–6259. [CrossRef]
5. P. Sharma and J. Gillanders, "Cybersecurity and Forensics in Connected Autonomous Vehicles: A Review of the State-of-the-Art," in IEEE Access, vol. 10, pp. 108979-108996, 2022, doi: 10.1109/ACCESS.2022.3213843.
6. S. G. Philipsen, B. Andersen and B. Singh, "Threats and Attacks to Modern Vehicles," 2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), Bandung, Indonesia, 2021, pp. 22-27, doi: 10.1109/IoTaIS53735.2021.9628576.
7. S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898-2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.
8. S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber and J. Delsing, "Connected cars — Threats, vulnerabilities and their impact," 2018 IEEE Industrial Cyber-Physical Systems (ICPS), St. Petersburg, Russia, 2018, pp. 375-380, doi: 10.1109/ICPHYS.2018.8387687.
9. Lim, K.; Tuladhar, K.M.; Kim, H. Detecting location spoofing using ADAS sensors in VANETs. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11 January 2019; pp.
10. M.L. Psiaki and T.E. Humphreys, "GNSS spoofing and detection," Proc. IEEE, vol.104, no. 6, pp.1258-1270, Jun. 2016.
11. Z. El-Rewini, K. Sadatsharan, N. Sugunaraj, D. F. Selvaraj, S. J. Plathottam and P. Ranganathan, "Cybersecurity Attacks in Vehicular Sensors," in IEEE Sensors Journal, vol. 20, no. 22, pp. 13752-13767, 15 Nov.15, 2020, doi: 10.1109/JSEN.2020.3004275.

12. Mudhivarthi, B.R.; Thakur, P.; Singh, G. Aspects of Cyber Security in Autonomous and Connected Vehicles. Appl. Sci. 2023, 13, 3014.
13. H. Shin, D. Kim, Y. Kwon and Y. Kim, "Illusion and dazzle: Adversarial optical channel exploits against lidars for automotive applications" in Cryptographic Hardware and Embedded Systems—CHES, New York, NY, USA:Springer, pp. 445-467, 2017.
14. Researcher hacks self-driving car sensors, https://spectrum.ieee.org/researcher-hacks-selfdriving-car-sensors
15. J. Petit, S. Bas, M. Feiri and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar", Black Hat Eur., vol. 11, pp. 2015, Nov. 2015.
16. S. Woo, H. J. Jo and D. H. Lee, " https://www.ti.com/lit/an/sloa101b/sloa101b.pdf?ts=1682050267211&ref_url=https%253A%252F%252Fwww.google.com%252F," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 993-1006, April 2015, doi: 10.1109/TITS.2014.2351612.
17. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., "Experimental -security analysis of a modern automobile," in 2010 IEEE Symposium on Security and Privacy. IEEE, 2010, pp. 447–462.
18. K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319180.
19. Introduction to the Controller Area Network (CAN) By TEXAS Instruments. https://www.ti.com/lit/pdf/sloa101