Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Computer Engineering (36^{th}cycle)

Cybersecurity for future interconnected and smart vehicles

By

Franco Oberti

******

Supervisor(s):
Prof. Stefano Di Carlo, Supervisor
Prof. Ernesto Sanchez, Co-Supervisor
Prof. Alessandro Savino, Co-Supervisor

Doctoral Examination Committee:
Prof. Giorgio Di Natale, CNRS - Laboratoire TIMA Gernoble, France
Prof. Ioana Vatajelu, CNRS - Laboratoire TIMA, Grenoble, France
Prof. Alberto Bosio, INL, Lyon, France
Prof. Marco Torchiano, Politecnico di Torino, Italia
Prof. Aldo Basile, Politecnico di Torino, Italia

Politecnico di Torino
2024

Declaration

I hereby declare that the contents and organization of this dissertation constitute my own original work and do not compromise in any way the rights of third parties, including those relating to the security of personal data.

Franco Oberti
2024

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

I dedicate this thesis to Matteo, Michela, my beloved parents, and my treasured grandparents. Your constant support and boundless love have been the foundation of my journey. This accomplishment is a testament to your enduring influence in my life.

Acknowledgements

First and foremost, I extend my deepest gratitude to Filippo Parisi and the team at Dumarey Softronix, whose invaluable collaboration made this Industrial PhD a reality.

I am profoundly grateful to my Professors, Stefano Di Carlo, Ernesto Sanchez, and Alessandro Savino, for their extensive support and mentorship. They have not only taught me a great deal but have also shaped my understanding and passion for our field.

Special thanks to Professor Fabrizio Lamberti and Matteo Sonza from SCUDO, whose guidance and insights have been instrumental in refining my research.

I would also like to acknowledge the vibrant community at Lab6. The camaraderie and intellectual stimulation provided by Roberta, Alessio, Lorenzo, Leonardo, Cristiano, Sepide, Tzam, Irene, Giulia, and Luca have enriched my PhD experience immensely. Their youthful spirit has kept me young at heart, even as I've grown quite older throughout this academic journey.

I would like to take a moment to remember Stefano P., who was a very good guy. His positive spirit, friendship, and encouragement will always be cherished. This work is dedicated to his memory too.

To all mentioned and those unnamed who contributed to this journey, I am eternally grateful. Your collective wisdom and encouragement have been a beacon of light throughout my PhD journey.

Abstract

The continual technological advancements mark the modern world, and the automotive industry is no exception. As vehicles rely more heavily on technology and connectivity, cybersecurity has become a pressing concern to ensure safe and reliable transportation. This PhD dissertation extensively explores the intricate relationship between cybersecurity measures and their significant role in the automotive industry. It emphasizes the necessity of robust security protocols to effectively mitigate cyber threats and ensure operational integrity and passenger safety. In response to the growing need for cybersecurity measures in the automotive sector, new Cybersecurity Approval frameworks have been introduced globally. These frameworks, including the United Nations Regulation No. 155 (UNR155) and strict guidelines from the National Highway Traffic Safety Administration (NHTSA) in the United States, highlight the urgent need for enhanced cybersecurity measures. The dissertation comprises several chapters meticulously crafted to examine various aspects of automotive cybersecurity. Starting with an overview of the evolution of automotive technology, the dissertation lays the groundwork for a better understanding of the criticality of cybersecurity in the industry. It then delves into legislative norms and historical and potential cyberattacks, identifies risks, and evaluates economic impacts. Subsequent chapters scrutinize the electrical architecture of vehicles, communication protocols, and security techniques and introduce innovative research projects focusing on hardware authentication, advanced vehicle communication networks, and the authentication of CAN data frames to ensure communication integrity. One of the pivotal contributions of this thesis is the development of novel network architectures that balance high-security standards with the operational demands of real-time automotive systems. The dissertation critically examines the vulnerabilities in current cybersecurity standards within the automotive sector. It proposes enhanced solutions to bolster defences against cyber threats in an increasingly interconnected and automated ecosystem. Through in-depth analysis and the proposition of inno-

vative security mechanisms adapted to automotive communication protocols, this dissertation aims to fortify the automotive industry's resilience against the continuously evolving cyber threat landscape. The research endeavour addresses current challenges and anticipates future developments, striving to significantly contribute to the field of automotive cybersecurity and ensure the sector's security in the digital age.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the dynamic and ever-changing terrain of contemporary technological advancements, the critical importance of cybersecurity in maintaining the operational integrity and safety of passenger cars has become a matter of paramount concern. This dissertation delves deep into the nuanced relationship between cybersecurity measures and their crucial role within the automotive industry, emphasizing the urgent need to implement robust security protocols to thwart cyber threats effectively. The impetus for this research is significantly reinforced by the introduction of new Cybersecurity Approval mandates required across all significant nations, notably including adherence to the United Nations Regulation No. 155 (United Nations Regulation No. 155 (UNR155)), along with the stringent guidelines promulgated by the National Highway Traffic Safety Administration (National Highway Traffic Safety Administration (NHTSA)) in the United States. These regulatory frameworks underscore the acute necessity for bolstered cybersecurity measures within the automotive sector, particularly in the context of the burgeoning connectivity and the increasing dependency on embedded systems that characterize contemporary vehicles. Embedded systems, especially those that manage functions critical to safety, stand at the forefront of areas yet to be fully secured against cyber intrusions. The deployment of conventional Information Technology (Information Technology (IT)) cybersecurity strategies offers only limited protection within these specialized embedded environments, thus highlighting the urgent need for dedicated research to develop security measures specifically crafted for these contexts.

The architectural design of this thesis is meticulously crafted to demystify the complex landscape of automotive cybersecurity. Beginning with an introduction in chapter 2, it lays a solid foundation for a deep dive into the evolution of automotive technologies. This exploration is critical for grasping the paramount importance of cybersecurity in ensuring the safety and integrity of road vehicles. Chapter 3 provides an extensive overview of the legislative norms, standards, and guidelines shaping the realm of automotive cybersecurity, thereby preparing the ground for subsequent analyses.

Chapter 4 delves into the intricate details of historical and potential automotive cyberattacks, identifying likely attack surfaces, assessing associated risks, and evaluating the economic repercussions of such security breaches. Following this, chapter 5 meticulously examines the electrical architecture of vehicles, communication protocols, and prevailing security techniques within the automotive sector. This groundwork is pivotal for the introduction of innovative research projects elaborated in the subsequent chapters.

Chapter 6 addresses critical discussions on hardware authentication, a sensitive area in the automotive field, highlighting the delicate balance between enhanced security measures and the operational demands of automotive systems. Chapter 7 explores research activities on advanced vehicle communication networks, aiming to elevate security standards while addressing the challenges of system throughput and bus load traffic.

Chapter 8 presents an innovative method to authenticate CAN data frames, ensuring the integrity of messaging out of bounds. This chapter underscores the importance of safeguarding communication integrity within automotive systems. Meanwhile, **??** builds upon the concepts and techniques discussed in chapter 8, adapting these security mechanisms to different vehicle communication protocols, the LIN, which currently lack efficient security measures.

Chapter 10 discusses the modeling of vulnerabilities and weaknesses in major automotive cybersecurity standards. It proposes an improved variant that is fully compliant with existing standards yet offers increased fidelity in security analysis. Finally, chapter 11 synthesizes the conclusions drawn from this extensive research endeavor.

This dissertation not only identifies the primary targets of cybersecurity within the automotive domain but also articulates the strengths and achievements of the

research undertaken. It introduces groundbreaking network architectures that not only maintain high-security standards but are also optimized for real-time systems, crucial for adhering to strict operational deadlines. Moreover, it provides a critical examination of the vulnerabilities in current automotive cybersecurity standards and proposes innovative solutions to improve the security landscape. These solutions aim to enhance the defense mechanisms against cyber threats in an automotive ecosystem that is increasingly connected and automated, ensuring the sector's resilience against the evolving landscape of cyber threats. Through this thorough exploration, the thesis aims to make a substantial contribution to the field of automotive cybersecurity, addressing current challenges while anticipating future developments to safeguard the automotive sector in the digital age.

Chapter 2

Evolution of Automotive Technology: A Historical Perspective

2.1 The Birth of the Automobile: Pioneering Days

The history of automotive technology began in the early 20th century, highlighted by the introduction of the Ford Model T in 1908, a seminal moment that redefined transportation. This era marked the onset of continuous innovation, driven by evolving consumer preferences, environmental concerns, and regulatory challenges.

Fig. 2.1 Ford Model T. Source: [1].

The early automotive industry saw significant figures like Karl Benz and Henry Ford, who introduced the first gasoline-powered vehicles. These machines, though primitive by today's standards, initiated a major shift in mobility and societal norms, reducing distances and reshaping urban landscapes.

As cars evolved, so did their impact on society, spurring advancements in engineering, materials, and manufacturing methods. Ford's introduction of assembly line production democratized vehicle ownership, marking the beginning of mass production.

2.2 From Mass Production to Modernization: Automotive Milestones

The automotive industry saw rapid growth with key players like General Motors, Ford, and Renault driving innovation. This period witnessed the development of advanced suspension systems, improved braking mechanisms, and better transmission systems, enhancing vehicle reliability and performance.

Material innovations such as steel alloys made cars lighter and more fuel-efficient. The expansion of road networks accommodated these advances, transforming urban planning and promoting a surge in vehicle ownership.

Automobile racing also influenced technological advancements, pushing the limits of automotive engineering. Regulatory bodies implemented safety and performance standards, ensuring vehicle reliability and fostering an era of standardized automotive production.

Environmental concerns led to the development of eco-friendly vehicles, highlighting a shift towards sustainability in the industry.

2.3 Challenges and Innovations: Shaping the Automotive Landscape

This era introduced critical safety innovations like seat belts and advanced braking systems, becoming standard features that enhanced driver confidence and road safety. Comfort also became a priority, with improvements in car interiors, climate control, and ergonomic designs enhancing the driving experience.

The electronic revolution brought significant changes with the integration of electronic fuel injection systems, improving efficiency and reducing emissions. Semi-autonomous features like cruise control and anti-lock braking systems further augmented driving safety and convenience.

2.4 Automotive Connectivity

Vehicle connectivity has become essential, enhancing road safety through advanced driver assistance systems and enabling eco-friendly driving practices. This connectivity supports efficient traffic management, reducing environmental impacts and improving the overall driving experience. V2X communication extends beyond vehicle-to-vehicle interactions, including communications with infrastructure, pedestrians, and the grid. This network enhances road safety, alleviates congestion, and supports environmental goals by promoting sustainable driving practices. Despite technological advancements, challenges like cybersecurity have emerged, highlighting the need for robust security measures in modern vehicles. The integration of digital technologies has increased vulnerability to cyber threats, emphasizing the importance of cybersecurity in automotive design and functionality.

Chapter 3

Navigating the Legal Landscape and Standard Frameworks of Automotive Cybersecurity

3.1 Introduction to Automotive Cybersecurity Regulations, Standards, and Guidelines

Regulatory frameworks, standards, and recommendations aim to enhance cybersecurity by establishing consistent guidelines and methodologies across the automotive industry. Laws, set by legislative bodies, require high-level authorization. Regulations, defined by government agencies, detail how these laws are implemented. Standards, developed by organizations like International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and International Telecommunication Union (ITU), provide consistent specifications for products and services globally, regionally, and nationally.

Original Equipment Manufacturer (OEM)s work with suppliers and cybersecurity firms to ensure compliance with these regulations, fostering industry-wide cybersecurity governance and enhancing information exchange through collaborations like those between European Automobile Manufacturers' Association (ACEA), European Association of Automotive Suppliers (CLEPA), and Automotive Information Sharing and Analysis Center (Auto-ISAC).

3.2 Functional Safety Assurance and Cybersecurity in Automotive Systems

Functional safety and cybersecurity in automotive engineering ensure vehicles operate as intended and are secure against cyber threats. These disciplines require robust interaction to mitigate risks from digital connectivity and sophisticated electronic integrations. The aim is to maintain vehicle functionality and safety through comprehensive safety measures and advanced cybersecurity strategies.

3.3 Global Consistency in Vehicle Type Approval

The UN Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations (WP.29) sets global vehicle regulations. Recent regulations include United Nations Regulation 155 (UNR-155) and United Nations Regulation 156 (UNR-156), focusing on cybersecurity management and secure software updates. These guidelines require a systemic approach to managing cyber risks, promoting global vehicle safety and security.

3.4 ISO/SAE 21434: A Standard for Securing Road Vehicles

ISO/SAE 21434, a collaboration between ISO and Society of Automotive Engineers (SAE), standardizes automotive cybersecurity practices. It covers the entire vehicle lifecycle, emphasizing a security-by-design approach to manage cybersecurity risks effectively.

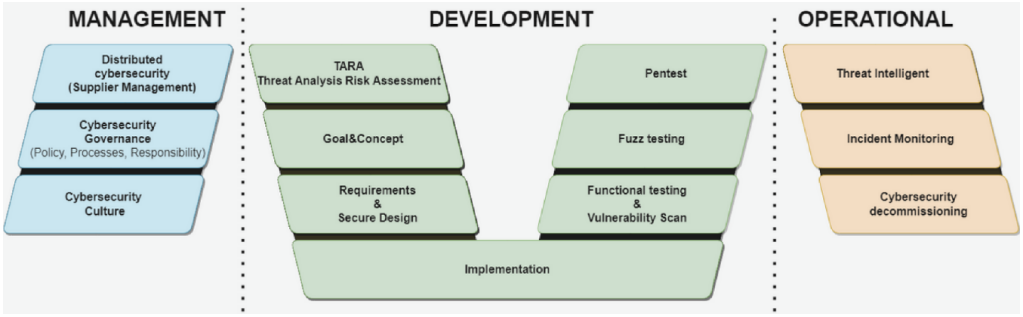


Fig. 3.1 Sample ISO/SAE 21434 Compliance Structure

3.5 ITU-T Intelligent Transport System (ITS)

International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) provides standards for secure communication within Intelligent Transport Systems (ITS), including Vehicle-to-Everything (V2X) systems. Recommendations like ITU-T X.1372 and ITU-T X.1373 focus on securing communication and software updates across vehicle networks, enhancing overall vehicle cybersecurity.

3.6 Other ISO standardization

ISO standards related to automotive cybersecurity include the Extended Vehicle (ExVe) methodology and standards for web services and software updates, ensuring interoperability and security across different vehicle systems.

3.7 Remaining security-relevant standards

Other important standards include the IEC 62443 and ISO 27000 series, which address cybersecurity in industrial and information security management contexts. These standards are increasingly relevant in the automotive sector, especially for cloud-connected services and operational technology security.

This chapter outlines the complex landscape of automotive cybersecurity, emphasizing the importance of compliance with regulatory standards to mitigate risks and ensure vehicle safety and reliability.

Chapter 4

Attack Models in the Automotive Domain

In this chapter, we conduct a thorough analysis of the security landscape and potential vulnerabilities that are inherent in the automotive industry. Furthermore, we provide an extensive discussion on the attack model currently being utilized within this domain. This chapter is a valuable resource for gaining insights into the challenges and risks associated with automotive systems. It provides an in-depth understanding of the attack model in practical application, which can be beneficial in helping stakeholders make informed decisions and take appropriate measures to ensure the safety and security of the automotive industry.

4.1 Understanding Threats and Vulnerabilities Trends in Connected Vehicles

In 2022, the smart mobility ecosystem experienced constant evolution but witnessed increased frequency and sophistication of cyber attacks. The macroeconomic and supply chain challenges and the geopolitical climate exposed new attack vectors likely to compel automotive and smart mobility stakeholders to speed up their cybersecurity investments. Upstream's cybersecurity researchers and analysts have delved into over 1173 incidents since 2010 and monitored hundreds of deep and dark

web forums to compile the comprehensive 2023 Global Automotive Cybersecurity Report.

Although it may seem recent, this journey has unfolded over the last 40 years. The concept of the connected vehicle dates back to the mid-1980s when Formula 1 teams began using on-board computers to send data bursts back to the pit lane via radio signals. In the late 1990s, consumer vehicles first saw the integration of automated accident detection and emergency call functions through telematics data. The early 2000s brought vehicle diagnostics, enabling manufacturers to identify and address system issues swiftly.

The next leap came almost a decade later with the advent of in-vehicle Subscriber Identity Module (SIM) cards and smartphones, which opened up new consumer services like in-vehicle internet, advanced infotainment, and smartphone apps for vehicle access control. The progression continued exponentially, incorporating Over-The-Air (OTA) software updates, connectivity to third-party mobility services, and Internet of Things (IoT) integration for seamless communication with any in-car system or smart device. The volume of data exchanged between vehicles and their back-end systems is expanding rapidly, mirroring the growth in various other IoT applications.

Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Grid (V2G), and V2X are examples of vehicle communications enabled by advanced connectivity. These developments play a crucial role in creating sophisticated smart mobility applications. Moreover, vehicles are evolving into software-defined entities, enabling continuous activation and upgrades, thereby improving customer experiences and generating new revenue prospects for OEM.

The rise of sophisticated mobility services by OEMs, fleet managers, and mobility providers has made connected vehicle services more prone to advanced cyber attacks.

4.2 Developing a Comprehensive Attack Surface Analysis

Emerging attack vectors demand immediate attention from stakeholders in the Automotive and Smart Mobility industry (Figure 4.1). The year 2022 has witnessed a

noticeable surge in cyberattacks, now executed with unprecedented sophistication. The integration of new technologies into this sector has underscored a critical insight: every connectivity point is a potential vulnerability.

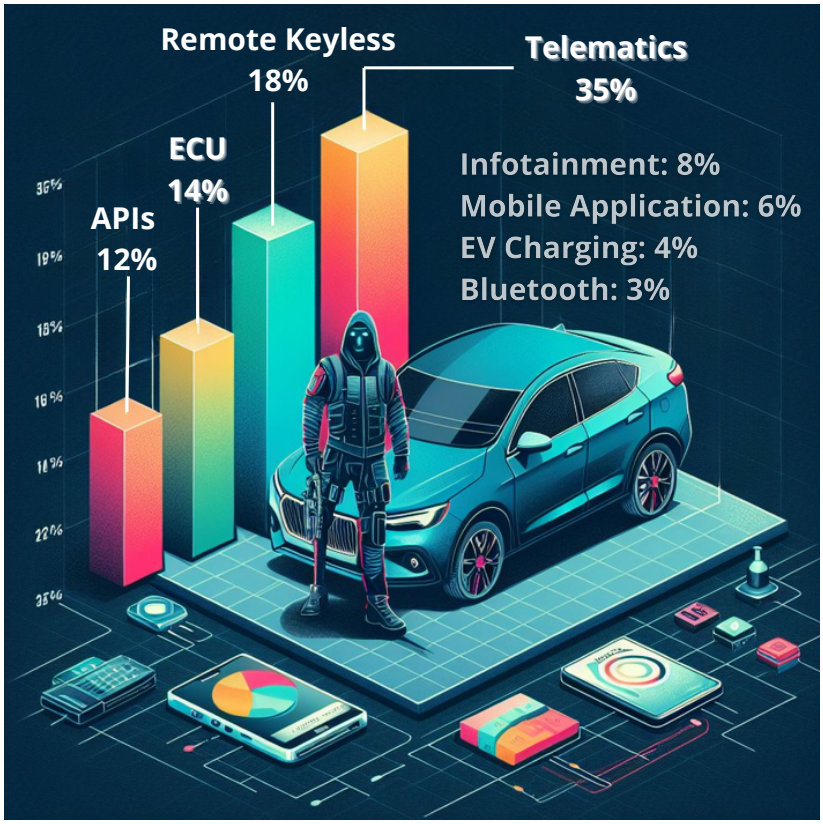


Fig. 4.1 Incidents by Attack Vectors. [1].

Two significant attack vectors introduced in 2022 play a crucial role in the smart mobility ecosystem. The first of these vectors targets Application Programming Interface (API)s designed for mobility applications and services. These APIs, which facilitate data exchange and functional interoperability across various software platforms, have become increasingly critical. However, a 380% increase in API-related incidents from the previous year [7] indicates a worrying trend. These APIs are vulnerable due to their broad internet accessibility and the complexity of securing interactions across diverse and often incompatible systems. Unauthorized access through these APIs can lead to severe data breaches, unwarranted control over vehicle functionalities, and major service disruptions.

The second vector focuses on the Electric Vehicle (EV) charging infrastructure, which is essential for overcoming the adoption barriers associated with 'range anxiety' among drivers. As the reliance on a consistent and reliable network of charging stations grows, so does the complexity of the required multi-layered infrastructure. This expansion begins to significantly impact power grids. Furthermore, the rising prevalence of EVs has dramatically increased the attack surface, making the infrastructure vulnerable to both physical and remote attacks. Notable was the disclosure in April 2022 by researchers from the University of Oxford and Armasuisse S+T of a new attack technique named "Brokenwire," which could remotely disrupt the charging of electric vehicles at scale [8]. Such vulnerabilities pose significant risks not only to consumer adoption of EVs but also to the broader electrification of fleets.

The implications of these vulnerabilities have spurred regulatory responses. In June 2022, the UK enforced The Electric Vehicles (Smart Charge Points) Regulations 2021 [9], mandating that charging stations incorporate robust cybersecurity measures, including anti-tampering features, event monitoring, and secure software updates. In light of extensive research and emerging incidents, further regulatory initiatives and standards are anticipated in the near future to enhance the safety and security posture of EV chargers.

Moreover, in October 2022, the Office of the National Cyber Director (ONCD) hosted the Cybersecurity Executive Forum on Electric Vehicles and Electric Vehicle Charging Infrastructure [10]. This event convened leaders from the government and the private sector to discuss cybersecurity issues concerning electric vehicles and their supply equipment. Participants, including representatives from OEMs, component manufacturers, and EV charging infrastructure manufacturers, were invited to share insights on current cybersecurity practices, identify gaps, and recommend improvements across the EV ecosystem.

4.2.1 Enterprise Application and Telematics

Immediate attention must be paid to emerging attack vectors in the Automotive and Smart Mobility industry. The industry now relies on connected vehicles in 2022 as they gather, transmit, and receive vital information. The back-end servers of the OEMs and the vehicle owners are where this information is transmitted. Two types of servers are used in connected vehicles to establish open communication with

OEMs. The first is telematics servers communicating with the vehicle, collecting and transmitting data from various sensors, including location, speed, and performance metrics. Application servers that connect to the vehicle's companion apps, like infotainment systems and mobile devices, are also present. Additionally, certain vehicles possess aftermarket servers that connect with various third parties, including insurance companies, fleets, car rental and leasing companies, Electric Vehicle (EV) charging networks, and more. These servers provide additional services to vehicle owners and enhance their driving experience. However, the use of these servers also brings potential risks. A black hat actor could attack vehicles on the road by exploiting vulnerabilities in the backend servers. They might gain access to sensitive data, like personal information and driving habits, or even manipulate the vehicle's critical systems, leading to accidents or other harm. The Automotive and Smart Mobility industry stakeholders must prioritize implementing robust security measures and regularly updating systems to mitigate risks and ensure the safety of their vehicles and customers.

4.2.2 Remote keyless entry systems

Wireless keyless entry systems, including key fobs (Frequency Operated Button (FOB)s), have become standard in the automotive industry over the past decade. However, this widespread use has led to increased vehicle thefts and break-ins, primarily because of the manipulation of these wireless key fobs. These attacks have increased as hacking tutorial videos and devices are readily available online without registration requirements, enabling malicious actors to carry out their attacks with ease.

Wireless key fobs use short-range radio transmitters to send coded signals to a vehicle's receiver unit when in proximity. These radio signals can be intercepted or tampered with using specific devices designed for signal interference or information theft from the key fob's radio communication. Hackers deploy various methods to attack the communication between the key fob and the vehicle.

In relay attacks, hackers intercept standard communication between the key fob and the vehicle, even if the key fob's signal is out of range. They amplify it using a transmitter or repeater, a method detailed in [11], to intercept the signal from a

key fob inside a vehicle owner's residence. An additional device placed near the car amplifies and relays a message to unlock and start the engine.

Another type of relay attack involves intercepting and storing messages sent from a key fob or vehicle for later use. Possessing the relevant message, as [12] describes, enables hackers to unlock the car's doors or start the engine.

Sophisticated and costly devices allow hackers to reprogram the key fob system and generate a new key for the car to communicate with, rendering the previous key unrecognizable. These reprogramming devices can be legally obtained on online e-commerce platforms and used by authorized mechanics and service centres. They typically connect to the OBD port, making it relatively straightforward for car thieves to gain full vehicle control, as reported by [13].

Additionally, car thieves may use signal jammers to disrupt the communication between the key fob and the vehicle, preventing the vehicle owner from locking the vehicle and granting thieves unrestricted access. Effective countermeasures against such attacks, discussed by [14], include encrypted communication protocols and advanced authentication systems to enhance security.

Recent incidents in 2022 further highlight the severity of these attacks. In Macclesfield, UK, police sought public assistance after five keyless vehicles from a British OEM were stolen using relay attack devices [15]. In October 2022, French police uncovered hackers using a modified version of a popular Bluetooth speaker (Figure 4.2), purchased for €5,000 on the dark web, which contained a 'quick start key' enabling them to start vehicles [16].

Additionally, in November 2022, the US National Insurance Crime Bureau reported a surge in vehicle thefts, nearing record highs, with over 745,000 vehicles stolen in the US in the first three quarters of 2022, marking a 24% increase compared to the same period in 2019 [17].

4.2.3 Electronic Control Units (ECUs)

The (ECUs) in modern vehicles play an indispensable role by overseeing key functions such as the engine, steering, braking, windows, and keyless entry systems. However, the increasing integration of digital technology in automotive systems has exposed ECUs to cybersecurity threats, making them highly vulnerable to cyber-

Fig. 4.2 Speaker Hacking Tool. Source: [1].

attacks that could compromise vehicle safety and functionality. A significant incident occurred in January 2022 when a hacker targeted the firmware of a German OEM Electronic Power Steering ECU. The attacker attempted to exploit the Controller Area Network (CAN) bus— a standard designed to allow microcontrollers and devices to communicate with each other within a vehicle without a host computer. Despite an unsuccessful attempt to directly extract the firmware, the hacker managed to collect enough data to brute force the ECU's authentication, gaining access to the password-protected diagnostics mode. This breach enabled the decryption and unauthorized modification of the ECU firmware, which could have led to severe consequences, including a total loss of control over the vehicle's steering capabilities.

Further illustrating the vulnerability of vehicle systems to cyber threats, in February 2023, the NHTSA issued a recall for approximately 17,000 acSUVs manufactured by a Japanese OEM. The recall was prompted by a flaw in the software of the Hybrid Vehicle Control ECU, responsible for calculating and limiting the hybrid battery's output. This software inadequacy risked causing the hybrid system to shut down under certain conditions. The root cause of this issue remains unidentified, but

it highlighted a potential cyber risk that could be exploited to compromise vehicle functionality.

In another instance, in November 2023, a sophisticated cyber-attack was launched against a Japanese OEM vehicle, wherein a hacker utilized a device equipped with a microcontroller to read and manipulate the CAN bus. This manipulation allowed the hacker to keep the vehicle's accessory ACC relay energized even after the engine had been turned off, maintaining power to the stereo and infotainment system. This type of attack not only poses privacy concerns but also raises the possibility of further exploitation of the vehicle's systems.

These incidents underscore the critical need for vehicle manufacturers to implement robust cybersecurity measures to safeguard ECUs and other vital vehicle systems from unauthorized access and cyber-attacks. Measures such as secure boot processes, regular software updates, encryption, and secure communication protocols are essential. Additionally, conducting regular security audits to identify and address vulnerabilities is crucial to preventing potential exploits. Educating vehicle owners about the cybersecurity risks associated with connected vehicles is also vital in mitigating the risk of cyber-attacks. The evolution of automotive technology demands a proactive approach to cybersecurity, ensuring the safety and integrity of modern vehicles against emerging digital threats.

4.2.4 Application Programming Interface (API)

Smart mobility services and connected vehicles rely heavily on numerous Application Programming Interface (API)s, resulting in many monthly transactions, reaching into billions. These APIs play a crucial role in the functionality of different components such as OEM mobile applications, infotainment systems, OTA and telematics servers, EV charging management, and billing applications. However, APIs can also pose significant cybersecurity threats, opening up avenues for various malicious attacks, such as stealing personal information and remotely manipulating vehicles.

API hacking is particularly concerning due to its accessibility to individuals with limited technical expertise, using well-established techniques that incur lower costs than targeting other system types. Moreover, these attacks can be done remotely without requiring specialized hardware. There has been a notable increase in API-

based attacks in the automotive sector, representing 12% of all incidents in 2022 (Figure 4.1), a substantial surge from the 2% reported in 2021.

One instance from November 2022 highlights the vulnerability of these systems. A group of ethical hackers, commonly known as white hat hackers, revealed how they gained unauthorized access and control over several vehicles manufactured by various OEMs. Their exploit was focused on a flawed BOLA in an API [18–27]. By sending API requests with a Vehicle Identification Number (VIN) in a unique ID field through a telematics system, they were able to remotely start, stop, lock, and unlock vehicles from several OEMs worldwide. Additionally, the hackers were able to access sensitive information about vehicle owners.

In September 2022, Anonymous hackers targeted a taxi-hailing app, coordinating an action that directed all available taxis to converge simultaneously in the same location in Moscow. This orchestrated convergence resulted in significant traffic congestion [28], with various videos showcasing the chaotic situation circulating on social media platforms.

4.2.5 Mobile applications

OEMs have utilized vehicle connectivity to offer remote services via companion applications that establish a link between smartphones and vehicles. This connectivity enables vehicle owners to remotely manage critical functions, including locating their vehicles, monitoring their routes, remotely unlocking doors, initiating engine start, and activating auxiliary devices. However, these very apps that enhance the digital user experience for drivers also present vulnerabilities that attackers can exploit to gain unauthorized access to both the vehicle and the backend servers supporting these applications. Cybercriminals can exploit vulnerabilities in companion apps, such as weaknesses in open-source software, hardcoded credentials, or flaws within the mobile app's API or backend server to acquire credentials and compromise private user information. In July 2022, researchers [29] discovered six vulnerabilities in a widely used Chinese Global Positioning System (GPS) tracker, which enabled attackers to access acGPS location data and send SMS commands directly to the GPS trackers, masquerading as if the commands originated from the legitimate owner's phone number. This acGPS tracker is currently deployed in over 1.5 million vehicles worldwide. These discoveries raise significant concerns regarding privacy

and security, underscoring the potential for hackers to manipulate the GPS tracker to track users, deactivate security alarms, and manipulate data.

4.2.6 Infotainment systems

Modern vehicles are vulnerable to cyberattacks through their In-Vehicle Infotainment (IVI) systems, which can be targeted due to their connections to the internet and short-range communications with phones and Bluetooth-enabled devices. While IVI systems provide convenience and entertainment to the vehicle occupants, they also expose sensitive information, such as contact details and messages, making them a cybersecurity concern. Additionally, IVI systems can pose a significant security risk as they integrate with a vehicle's internal networks. Malicious software can infiltrate the internal systems through IVI systems, potentially compromising critical functionalities.

The vulnerability of IVI systems was highlighted in July 2022 when a hacker gained control over the head unit of a Korean OEM vehicle by exploiting its dashboard API. The hacker bypassed all authentication mechanisms designed to protect firmware updates and reverse-engineered the code to create subversive update files that granted unauthorized access to the root shell of the head unit. The attacker then reverse-engineered the app framework to create a custom application that allowed them to monitor the vehicle's status. This incident exposed the severe consequences of a compromised IVIsystem.

4.2.7 EV charging infrastructure

It is of utmost importance to establish a reliable and secure charging infrastructure to speed up the widespread adoption of electric vehicles. Several vulnerabilities exist in many charging stations, making them vulnerable to physical and remote manipulation. These vulnerabilities can lead to various negative consequences, such as impeding the proper functioning of the chargers, putting electric vehicle users at risk of fraud and ransom attacks, and having far-reaching effects on the overall charging network, local power grid, and even entire fleets of electric vehicles. The year 2022 saw various noteworthy incidents related to electric vehicle charging. In February, a Ukrainian supplier of EV charging components conducted a hack on

Russian electric vehicle chargers as part of a cyber warfare initiative[30], causing them to become disabled. Security researchers found a new attack method in April that specifically targets the widely used Combined Charging System (CCS)[31], posing a threat to the charging process of electric vehicles on a large scale. In May, experts reported increased hacking incidents targeting charging stations[32]. These incidents included hackers installing ransomware on chargers to hinder their functioning or render them completely non-operational. In addition, hackers could lock users out of their profiles until a ransom was paid.

4.2.8 Bluetooth

Bluetooth is a wireless technology that enables devices to connect and exchange data via radio frequencies. Among the various protocols for exchanging data between devices, Bluetooth Low Energy (BLE) is the most commonly used. This protocol facilitates communication between smartphones, laptops, smartwatches, vehicles, residential and commercial locks, and access control systems.

However, in May 2022, a research team associated with the NCC Group [33] unveiled a new tool to exploit a specific type of BLE relay attack. This attack operates at the link layer and circumvents current relay attack countermeasures, posing a significant security threat. They demonstrated the vulnerability using a popular American electric vehicle model, and this security flaw extends to almost all devices that use the BLE protocol.

The researchers showed that they could unlock and control a vehicle using an iPhone outside the vehicle's standard BLE range. This discovery highlights the potential risks associated with BLE and raises concerns about its use across various domains.

It is crucial to address these issues to ensure that devices using BLE are secure to prevent unauthorized access and data breaches. As such, security experts are continually developing new security measures to address the security flaws in BLE and make it safer for use in various applications.

4.2.9 Over-the-air (OTA) Update

The OTA programming has become a pivotal technology in remote software management. It enables the wireless distribution of software, firmware, or configuration settings from a central hub directly to devices connected to the network. This technology is prevalent in the automotive industry, where it is used to update the software of modern vehicles, enhancing their functionality and performance. However, the convenience of OTA updates is accompanied by significant security risks. Unlike physical updates, which require direct access to the vehicle, OTA updates can be more susceptible to cyber threats, such as malware and hacking attempts. These digital attacks can have widespread implications, potentially impacting multiple vehicles or even an entire fleet almost instantaneously. Therefore, while efficient, OTA programming is considered a high-risk activity because of the scale and speed at which problems propagate. An illustrative example of these risks occurred in May 2022, when hackers identified a vulnerability in a vehicle produced by a Chinese OEM [34]. They could execute unauthorized software upgrades on these vehicles. Remarkably, the compromised vehicles were accessible for updates over the network and physically via the OBD port. This breach was alarming because it extended beyond minor feature enhancements; the unauthorized updates included critical aspects such as engine power and safety features. The incident highlighted a crucial issue with OTA updates: the potential for pirated or malicious installations to cause significant malfunctions in vital vehicle systems, including those responsible for active safety. Such disruptions compromise the vehicle's functionality and severely threaten the driver's and passengers' safety. Given these concerns, it is imperative to prioritize the security of OTA updates. Implementing robust and resilient cybersecurity measures is crucial for safeguarding against unauthorized access and ensuring the integrity of distributed updates. This approach is crucial to maintaining the reliability and safety of vehicles equipped with OTA capabilities, protecting them from the ever-evolving landscape of cyber threats.

4.3 Evaluating Attack Scenarios in Automotive Systems

The increasing connectivity of modern embedded systems has made them vulnerable to security threats. In particular, modern vehicles are a prime example of such systems, as they communicate with various entities such as traffic lights or other vehicles. Although the automotive industry previously prioritized functionality and safety aspects, the significance of security has now been elevated due to the increasing connectivity of modern vehicles.

Modern vehicles consist of multiple Electronic Control Units (ECU)s following the Automotive Open System Architecture (AUTOSAR), and attackers can exploit these systems through various attack vectors. These attacks can range from general types like denial of service to domain-specific attacks such as traffic control manipulation or camera/radar/LiDAR spoofing. The evolution of attacks in terms of both quantity and complexity poses a challenge in keeping track of existing threats.

Reflecting on work conducted by other researchers, a systematic review in the automotive domain highlighted significant vulnerabilities. According to their study, 48 specific ways in which attacks can take place were identified, encompassing various aspects of vehicular systems [35]. Based on this review, a taxonomy was created to classify these mechanisms, and a scheme was proposed to explore the characteristics of specific attacks, mapping them to the AUTOSAR architecture. This analysis revealed that the most prevalent attack vectors include GPS spoofing, message injection, node impersonation, sybil, and wormhole attacks, primarily targeting the application and services layers of the AUTOSAR architecture.

4.3.1 Classification of Attack Domains

Attack vectors in cybersecurity can be organized according to the domain they impact. This organization is heavily informed by the methodologies listed in the Common Attack Pattern Enumeration and Classification (CAPEC) [36] database, which is a vital resource providing a catalogue of common attack patterns that adversaries use to exploit system vulnerabilities. Security practitioners utilize this database for thorough analyses, robust testing, and educational outreach to forge effective security measures against ongoing threats.

As delineated by CAPEC, attack vectors are categorized into six principal domains, each highlighting a specific area of potential risk:

Software: Targets software applications by exploiting coding errors or design flaws.

Hardware: Focuses on the vulnerabilities present in the physical components of devices.

Communication: Involves attacks on the data exchange processes and protocols, including but not limited to Vehicular Ad Hoc Network (VANET), CAN, and LIN.

Supply Chain: Concerns disruptions or manipulations within the supply chain aimed at espionage, sabotage, or theft.

Social Engineering: Deals with techniques that manipulate individuals to bypass security measures through deception or psychological manipulation.

Physical Security: Relates to the exploitation of flaws in the security measures that protect physical assets.

These distinct domains form a framework that aids cybersecurity professionals in pinpointing vulnerabilities and crafting precise strategies to address and mitigate risks. This structured approach enhances the industry's ability to safeguard against varied and evolving security threats efficiently.

4.3.2 Categorization of Attack Vectors

The systematic classification of attack vectors in modern vehicular systems is critical, as these systems are complex and layered, making them vulnerable at various interaction points [37–43, 36, 44–46]. The susceptibility to attacks increases due to the inherent weaknesses in these layers, which include multiple electronic components like ECUs, wiring, and communication networks such as vehicular ad hoc networks VANET. Attack vectors can be systematically broken down into three primary categories of access points:

1. **Physical Access:** This category includes attacks that require direct physical interaction with the vehicle's components. Attackers may gain access to

critical vehicle systems such as the onboard diagnostic port (OBD-II), ECUs, computer modules, and the vehicle's media systems including radios and navigation systems.

2. **Short-Range Communication Attacks:** Attacks within this category occur when an adversary is physically close to the vehicle. They may manipulate or intercept data transmitted to and from short-range communication devices embedded within the vehicle, such as Bluetooth (BT), Remote Keyless Entry (RKE)s, Passive Keyless Entry (PKE)s, Tire Pressure Monitoring System (TPMS), Dedicated Short-Range Communications (DSRC), Wireless Fidelity (WiFi), Wireless Access for Vehicular Environments (WAVE), and systems like Voice-Controllable System (VCS)/Speech Recognition System (SRS).

   Indirect Physical and Short-Range Access: Despite direct physical access being limited, modern vehicles host numerous interfaces that can be exploited. For example, the OBD port allows for substantial manipulation of vehicle systems through connected devices. While typically used for diagnostics and maintenance, if compromised, such access could lead to widespread manipulation of vehicle functionalities.

   Entertainment Systems: These include interfaces like USB ports, CD players, and proprietary connections such as Apple's iPod Out, which could serve as entry points for malicious inputs or attacks aimed at overriding system functions.

   Bluetooth and Wireless Communications: Given their ubiquity in vehicular systems for tasks such as hands-free calling, these technologies offer potential gateways for cyber attacks. Techniques to extend their operational range exist and can exacerbate their vulnerability [47].

   Emerging Technologies: Innovations such as DSRC are designed for improving vehicular safety communications but also introduce new attack surfaces due to their wireless nature.

3. **Long Range Attacks:** This level involves attacks that can be conducted remotely, possibly over significant distances. Such attacks could target communication channels like GPS, cellular networks, and other forms of remote vehicle connectivity. Long-range attack vectors are particularly concerning

because they can be executed anonymously and can target multiple vehicles or systems simultaneously.

Broadcast Channels: These channels do not target specific vehicles but can affect any within range. They could be used for mass disruptions or widespread attacks.

Addressable Systems: These include more targeted attacks through systems like telematics, which offer continuous connectivity and can thus be uniquely vulnerable to sophisticated cyber threats.

This refined framework for understanding vehicular attack vectors emphasizes the multi-layered nature of modern vehicle systems and the broad spectrum of potential cyber threats they face. It is imperative that security measures address all these layers to effectively protect against and mitigate these risks.

4.3.3 Characterization of Cyber Attacker Profiles

The analysis of cyber attacker profiles is an integral component of cybersecurity strategies. According to various studies [48–50], understanding an attacker's profile requires a framework that divides characteristics into four primary bipolar categories.

Membership: The Membership category classifies attackers based on their level of access and familiarity with the target network, breaking down into two distinct types:

- **Insider:** These are authenticated individuals who have extensive knowledge of and access to the network, often with legitimate user credentials.
- **Outsider:** These attackers lack authorized access and typically have minimal direct knowledge of the network's internal workings.

Objective: This dimension categorizes attackers by their underlying motives, which can vary widely:

- **Malicious:** Attackers with the intent to harm the network or its users for reasons beyond personal gain, often driven by ideology or vendetta.

- **Rational:** These attackers are motivated by profit or personal gain, with their actions often being more predictable and financially driven.

Activity: Attackers are also differentiated by the nature of their activities within the network:

- **Active:** This involves direct engagement with the network through data manipulation, system compromise, or the creation of network traffic anomalies.
- **Passive:** Passive attackers focus on monitoring and stealthily gathering information without affecting the network directly.

Scope: The Scope category addresses the extent of the attacker's reach within or across networks:

- **Local:** These attackers operate within a confined or localized area, often targeting specific components or systems.
- **Extended:** These attackers have capabilities that extend over larger networks or multiple domains, capable of conducting widespread attacks.

Understanding these profiles facilitates the development of tailored cybersecurity measures. By recognizing the varied motivations and methods of potential attackers, organizations can better strategize their defences and countermeasures to protect their digital assets effectively.

4.4 The Pervasiveness of Remote Attacks in Modern Automotive Systems

In the transition from 2021 to 2022, the nature of cyber attacks on the automotive industry underwent a significant change, with a shift in the pattern and severity of incidents. Physical attacks were more frequent in 2021, requiring the hackers to have physical access to their targets. For example, an Asian OEM's infotainment unit was hacked using a USB device, granting root shell access. Short-range attacks were also common, with a UK incident involving a European-made vehicle hacked outside its owner's home using a relay attack device on a remote keyless entry system.

However, long-range attacks were less prevalent and typically occurred in controlled environments. Nevertheless, experts predicted an increase in long-range attacks due to the growing connectivity and proliferation of connected components in vehicles.

In contrast, the landscape changed significantly in 2022, with remote attacks becoming more prevalent, and physical attacks almost disappearing. This year, long-range attacks increased significantly, overshadowing short-range attacks. For instance, a security researcher used inexpensive tools and software to execute a short-range Bluetooth attack on an American OEM vehicle, exploiting vulnerabilities in the phone-as-a-key keyless entry system. Long-range attacks became more prominent, as seen in a ransomware attack on a Japanese automotive supplier that affected its computerized production controls, and a cyberattack targeting IT providers, leading to the shutdown of Denmark's largest train company. These incidents highlighted the increased reliance on network connectivity and APIs, and the potential of these attacks to impact multiple vehicles or infrastructure systems simultaneously.

The data from these two years demonstrate the evolving nature of automotive cybersecurity threats, with a growing emphasis on remote, particularly long-range, attacks. This trend is likely to continue as vehicles become more connected and integrated into broader technological ecosystems. In the Figure 4.3 visual comparison illustrates these trends:

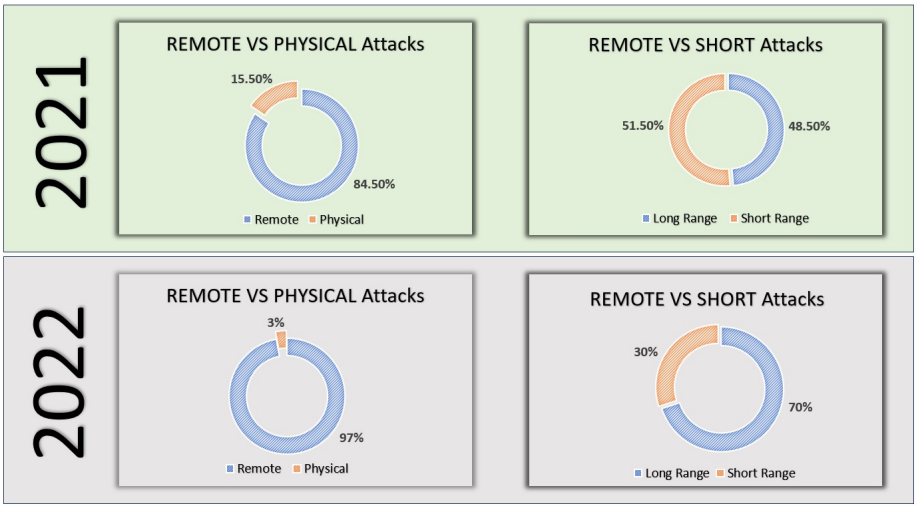


Fig. 4.3 CVEs' trend in Automotive field

4.5 CVE monitor is essential

The scoring of vulnerabilities based on their innate properties, including base, temporal, and environmental aspects, is done through the Common Vulnerability Scoring System (CVSS) [51] . It provides a standardized and open approach to evaluating and rating Common Vulnerabilities and Exposures (CVEs)[52]. The primary objective of CVSS is to aid organizations in prioritizing and coordinating their responses to vulnerabilities. The vulnerabilities' severity is categorized into levels ranging from Critical to None based on their assigned CVSS scores. CVSS scores are essential in assessing vulnerability risks, with security teams, developers, and researchers using various methods to evaluate risks. These scores are used practically throughout a product's supply chain, aiding in identifying exploited vulnerabilities, guiding prioritization efforts for patching, and facilitating the efficient allocation of time and human resources.

The integration of the CVSS into the risk assessment framework of the ISO/SAE 21434 standard plays a pivotal role in evaluating attack feasibility in the context of automotive cybersecurity. This integration is crucial for fleet managers and operators, as it necessitates vigilant monitoring of Common Vulnerability and Exposure (CVE)s. The significance of CVEs extends beyond mere tracking; they are instrumental in determining the composition of vehicle fleets and influencing the overall risk assessment of the entire fleet.

Proactive identification and mitigation of these vulnerabilities are essential steps in enhancing the cybersecurity posture of automotive fleets. By addressing these vulnerabilities in a timely manner, fleet managers can bolster the resilience and security of their vehicles, safeguarding them against potential cyber threats.

The accompanying document features a graph, labelled as Figure 4.4, that highlights an important trend. It shows an increase in the number of CVE related to the automotive industry from 2019 to 2023. The period between 2020 and 2021 marks a slight increase in CVEs, indicated by the yellow line that intersects between two flat zones in the bienniums 2019/2020 and 2021/2022. The modest increase in 2020 and 2021 indicates an evolution and intensification of cybersecurity challenges in the automotive sector. However, compared to the recently published data for 2022 and 2023, where a historic peak was recorded with a more than double surge, emphasizing the importance of remaining vigilant and adapting cybersecurity strategies.

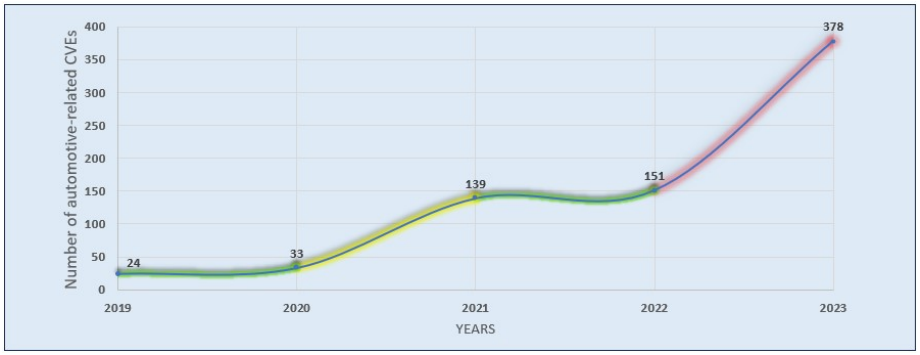


Fig. 4.4 Trend in automotive-related CVEs from 2019 to 2023.

The 150% increase in CVEs in 2023 is mainly attributed to the ongoing proliferation of connected components, coupled with increased awareness among stakeholders in proactively identifying vulnerabilities. It is noteworthy that it is too early for the results of 2024, just started, which adds an element of uncertainty to the analysis of future trends. It will be interesting to see if the trend remains flat, experiences another significant increase like in 2023, or shows a decrease.

4.6 Reputational Repercussions: The Impact of Cyber Attacks on Trust in the Automotive Industry

The repercussions of automotive cyber-attacks can be both direct and indirect, resulting in significant financial consequences. Direct costs may include expenses related to recalls, production stoppages, financial payouts, and even vehicle theft. Indirect damage can include security breaches resulting in compromised accounts and sensitive data, eroding brand reputation and customer trust, ultimately damaging revenue streams. This grim reality is evident in the data presented in the Figure 4.5. It's crucial to emphasize that these incidents encompass more than just traditional IT threats.

As the connected vehicles market continues to grow, projected to reach $197 billion by 2030, cyber attacks targeting the automotive industry will continue to have far-reaching effects. In recent years, a growing number of companies within the industry have fallen victim to increasingly sophisticated cyber assaults, some of which have had lingering effects for months before full recovery is achieved.

Accenture's research [53] further highlights the alarming financial toll of cybercrime on the automotive sector, projecting losses of $505 billion over five years from 2019 to 2023. These figures serve as a stark reminder of the critical need for robust cybersecurity measures within the automotive industry to safeguard both its financial health and the trust of its stakeholders. The graph mentioned earlier visually represents the extensive impact these cyber incidents have had on the industry from 2010 to 2022.

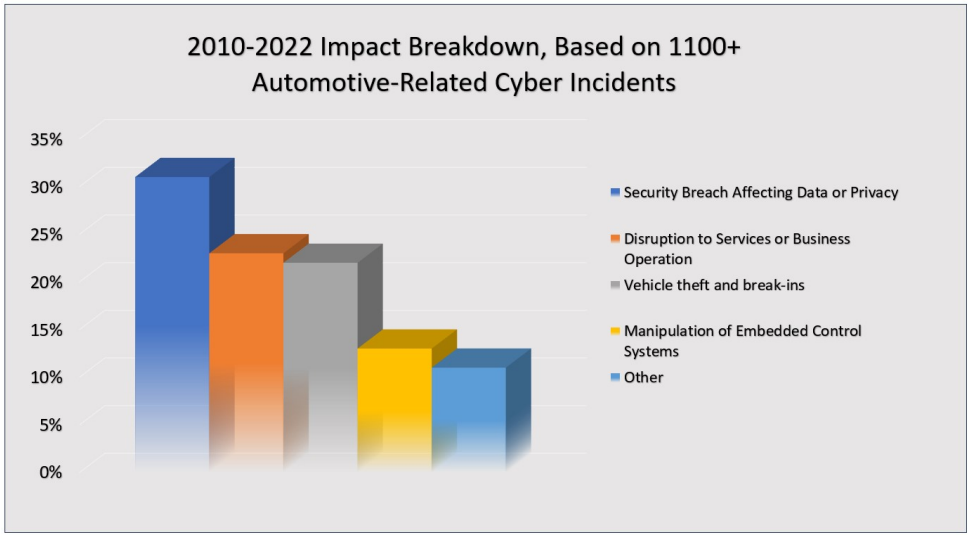


Fig. 4.5 Analysis of 1100+ Automotive-Related Cyber Incidents: 2010-2022 Impact Overview

4.6.1 Security Incidents Involving Data and Privacy

A company's most valuable asset is its private data, which includes Personal Identifiable Information (PII), customer databases, billing details, employee records, vendor databases, contractual agreements, and internal trade secrets. This data is fiercely protected, but ransomware attacks have put it at risk, exposing businesses and individuals to serious threats.

Cybercriminals have developed a tactic known as "double extortion" in their ransomware assaults. In this tactic, they encrypt sensitive files and demand a ransom for the decryption key. At the same time, they maintain an online presence on a "leak site," where they threaten to release and sell stolen data on the dark web if the victim does not comply with the extortion demand.

Black Basta [54] is a Ransomware-as-a-service (RaaS) group that gained notoriety in 2022. They breached the security of over 89 organizations from April to October, focusing primarily on the United States, the European Union, and the United Kingdom. They targeted a wide range of industries, including the transportation sector. There are speculations that Black Basta is a rebranded version of the infamous Conti RaaS [55].

In August 2022, a prominent UK-based car dealership with nine franchises and 23 locations fell victim to a severe ransomware attack that encrypted critical systems and caused irreparable damage to some of them. The attackers demanded a substantial ransom payment and threatened to delete critical data permanently. As a result, the company's network infrastructure suffered significant harm, and personal employee data and other sensitive information were compromised.

These examples highlight the growing threat of ransomware attacks and emphasize the urgent need for robust cybersecurity measures across all industries to protect valuable data and organizations' integrity.

4.6.2 Automobile Theft and Unauthorized Access Incidents

The rise of wireless car unlocking and starting technologies has led to an increase in keyless car thefts. Online toolkits containing the necessary tools and technologies to manipulate vehicles are readily available, contributing to a surge in cyber incidents involving car thefts and break-ins over the past decade. Keyless car thefts now account for over a quarter of all incidents in the automotive industry, posing a serious challenge in many countries.

In 2022, police departments across the world warned of a significant increase in keyless vehicle thefts:

- The Cheshire UK police raised concerns in February about a spike in British OEM vehicle thefts equipped with keyless ignition and provided safety tips for drivers.
- In April, the Birmingham UK police reported a 36

- The Ottawa, Canada Police Service warned residents in May about a rising trend in car thefts, specifically targeting a particular model of Japanese OEM, with 21 vehicles stolen over a two-week period.
- Police in New Orleans, LA, reported a significant increase in keyless relay attacks in August, resulting in the theft of nearly 1,900 cars in 2022.
- Chicopee, MA police in September noted a surge in keyless car thefts and suggested ways for keyless car owners to safeguard against such incidents.
- In October, Greater Manchester UK police issued a warning about a specific model of an American OEM. In late September, eight vehicles were stolen using short-range radio waves, emphasizing the need for vigilance.

These incidents illustrate the growing prevalence of keyless car thefts and highlight the importance of adopting security measures to protect vehicles and reduce the risk of theft.

4.6.3 Financial Consequences for Insurance Providers

Automotive cybersecurity threats are now a major concern for insurance stakeholders who are worried about the impact they may have on insurance premiums [56]. There is also growing concern about issues related to ransomware and cybersecurity underwriting. The emergence of connected Self-Driving Vehicles (SDV)s has the potential to revolutionize the insurance industry by introducing behaviour-based monitoring capabilities that insurers can use to improve their risk assessment processes. However, this increased connectivity and reliance on software-based features also bring fresh cyber risks and safety concerns. Keyless entry systems have contributed to a rise in vehicle thefts and unauthorized access incidents, which has forced insurers to evolve their traditional theft risk considerations. The increasing incidence of car thefts through relay attacks has prompted the Insurance Crime Bureau to issue a warning in May 2022 [56]. Many insurance providers have responded to this shifting risk landscape by changing their stance and not covering claims for property lost in keyless attacks. They also exclude coverage for high-value items within vehicles unless clear signs of forced entry exist. Due to the significant surge in vehicle thefts, insurance providers are now taking a keen interest in understanding the various attack

vectors and vulnerabilities associated with vehicle theft. Additionally, underwriters face the challenge of evaluating emerging cybersecurity risks, such as partial or complete vehicle "bricking" due to ransomware attacks. To effectively manage these complexities, they must gain a comprehensive understanding of the cybersecurity posture of each vehicle make and model, along with an assessment of the potential frequency and severity of cyber attacks.

4.7 Financial Impact of Cybersecurity Incidents in the Automotive Sector

Cybersecurity incidents within the automotive and innovative mobility sectors have substantial financial consequences, including costs associated with recalls or OTA updates, production halts, ransomware payments, and vehicle thefts. These events often result in significant data and privacy breaches, which tarnish the brand's reputation, erode customer trust, and could lead to hefty regulatory fines and reduced revenue. It is crucial for Vehicle Security Operations Centers (VSOCs) teams to thoroughly assess the economic ramifications of these events, with nearly half of the cybersecurity incidents in 2023 affecting a wide range of mobility assets, from thousands to millions.

In June 2023, a prominent semiconductor manufacturer based in Taiwan experienced a cybersecurity breach when a ransomware group targeted one of its IT hardware suppliers. This attack exposed critical information about the initial setup and configuration of systems. The attackers demanded a $70 million ransom for decrypting the data and preventing its online release, marking the highest ransom demand recorded. Despite the potential impact on various automotive stakeholders, the manufacturer assured the incident did not compromise its business operations and customer data at its supplier. Following the breach, the company also immediately ended its data exchange with the implicated supplier.

Another significant incident occurred in November 2023, when the same ransomware group attacked a large Australian automotive group, including 12 dealerships and many employees. This attack led to the theft of over 50 Gigabytes (GBs) of sensitive data, encompassing over 91,000 files that included payroll details, lease agreements, financial settlements, service quotations, invoices, crash help docu-

mentation, Customer Relationship Management (CRM) entries, vehicle registration forms, and employee identification and vehicle sales licenses. The hackers revealed the stolen data to the public in late November, after the ransom deadline passed.

Assessing the financial aftermath of cybersecurity incidents in the automotive sector is a daunting task, as these events pose risks to driver and passenger safety, disrupt business operations, compromise data privacy, and result in financial losses for Original Equipment Manufacturers (OEMs) as well as the entire supply chain.

Chapter 5

Electrical/Electronic (E/E) vehicle architectures and Security state of art

5.1 Introduction

The vehicle's Electrical/Electronic (E/E) architecture is a complex network of electronic components, advanced networking technologies, electrical harnesses, and sophisticated software applications. This intricate system is responsible for various vehicular functions that enhance the user experience while controlling the vehicle. Integrating software and electronics has revolutionized vehicle feature development and deployment and increased the potential for cybersecurity threats. Therefore, understanding E/E architecture is critical for analyzing vehicle security.

To gain a comprehensive understanding, we will initially focus on various hardware platforms used within the electronic control units (ECUs) and their respective reference software architectures. We will then examine how these ECUs are organized into specific domains interconnected through sophisticated networking technologies and represent unique functional subsystems with distinct responsibilities.

With a grasp on ECUs and their networking framework, we will explore the sensors and actuators that are key to the vehicle's ability to perceive and interact with its environment. This will lead us to different architectural topologies within vehicle systems, highlighting current trends and future directions in this field. By

adopting this structured approach, we can construct a layered understanding of potential vulnerabilities within the vehicle.

As we navigate the various layers of E/E architecture, we will pose thought-provoking questions encouraging exploring potential threats to vehicle components. A concise list of answers at the end of this chapter will serve as a reference point. Subsequent chapters will delve deeper into these discussion topics, thoroughly examining the cybersecurity threat landscape.

5.2 Fundamental Components of Vehicle E/E Architecture

Before delving into the intricate domains of the E/E architecture, it's essential to understand its foundational elements, which include a diverse array of ECUs[57], sensors, and actuators. These components are intricately linked through a complex network of both hardwired and network-based connections, creating multiple layers within the E/Esystem. The interconnectivity between ECUs, sensors, and actuators via in-vehicle communication networks forms the backbone of this architecture, enabling a variety of configurations and, consequently, numerous versions of the vehicle's E/E. At the core of the E/E architecture, ECUs encompass processing elements essential for executing the designated vehicle functions. These units are interconnected through the vehicle's network, enabling them to communicate and function collaboratively. It is common to integrate more than 70 ECUs controlling various physical subsystems [58] including:

- Engine Control Module (ECM)
- Transmission Control Module (TCM)
- Adaptive Cruise Control (ACC)
- Body Control Module (BCM)
- Telematics Control Unit (TCU)
- Onboard Diagnostic System (OBD)
- Diesel Exhaust Fluid Controller (DEFC)
- Variable Geometry Turbine (VGT)
- Chassis Control Module (CCM)
- Stability Control Module (SCM)

- Light Control Module (LCM)
- Infotainment Control Module (ICM)
- Seat Control Unit (SCU)
- Door Control Unit (DCU)
- Windows Control Unit (WCU)
- Belt Control Unit (BCU)
- Gateway

A simplified illustration in Figure 5.1 showcases the organized grouping of channels and components.

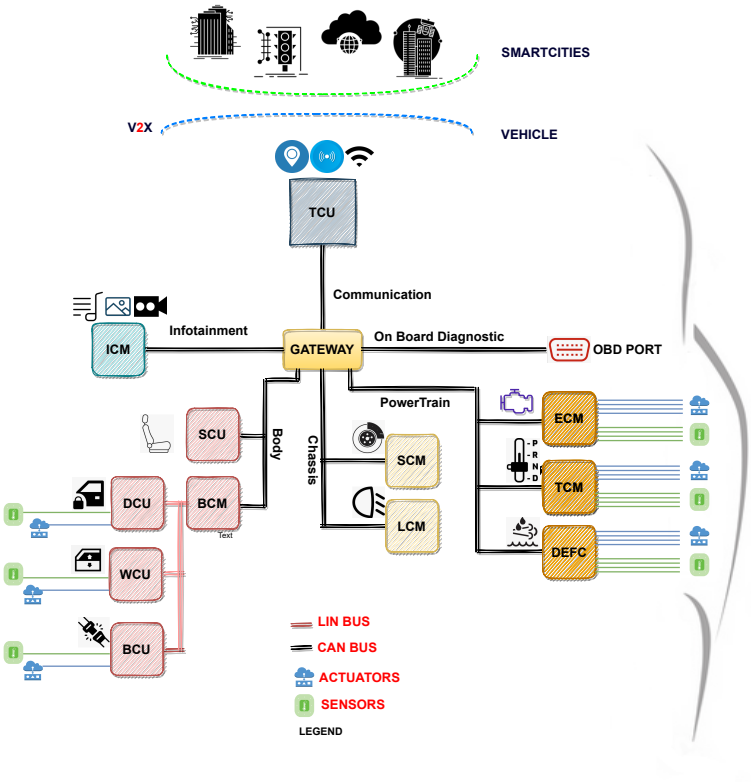


Fig. 5.1 Light Automotive architecture sample

An array of in-vehicle networking channels interconnects these ECU domains. These networks facilitate communication between ECUs, ensuring coordinated operation across different vehicle systems. In addition to ECUs, vital components like sensors and actuators are integrated into the system. These components are linked through direct hardware connections and network-based interfaces, allowing for real-time data exchange and control.

The orchestration of ECUs, sensors, actuators, and network channels can be configured in multiple ways. This versatility leads to diverse architectural variants within the E/E system of vehicles. Each configuration is tailored to meet specific vehicle requirements, balancing performance, safety, and cost factors.

Illustrating these concepts, Figure 5.1 presents a simplified representation of an E/E architecture. This diagram serves as a visual guide to understanding how the different components are arranged and interconnected within the vehicle's E/E system.

5.3 Overview of ECUs

ECUs are central to the functionality and complexity of modern vehicles' E/E architecture. They embody the integration of hardware and software to perform a vast array of vehicle functions, ranging from essential control systems to advanced driver assistance and infotainment systems.

5.3.1 ECU Construction

External View

Closed Box View of an ECU

ECUs are designed to endure the demanding conditions of automotive environments, including exposure to heat, vibration, and electromagnetic interference. Encased in a sealed enclosure, ECUs connect to the vehicle's network via a wire harness, facilitating communication with other components of the E/E architecture (Figure 5.2).

Internal Components

Upon opening an ECU, one would find a Printed Circuit Board (PCB) adorned with a mixture of passive and active components.

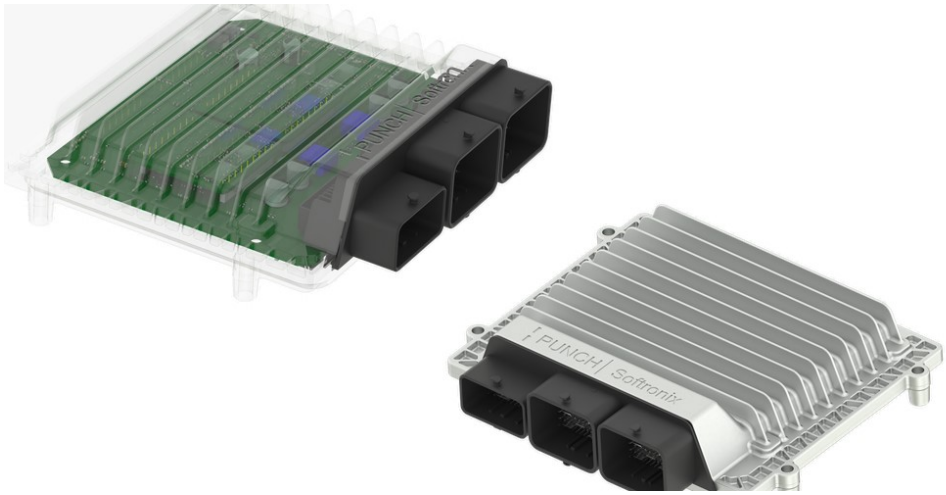


Fig. 5.2 Automotive ECU rendering. Source:[2].

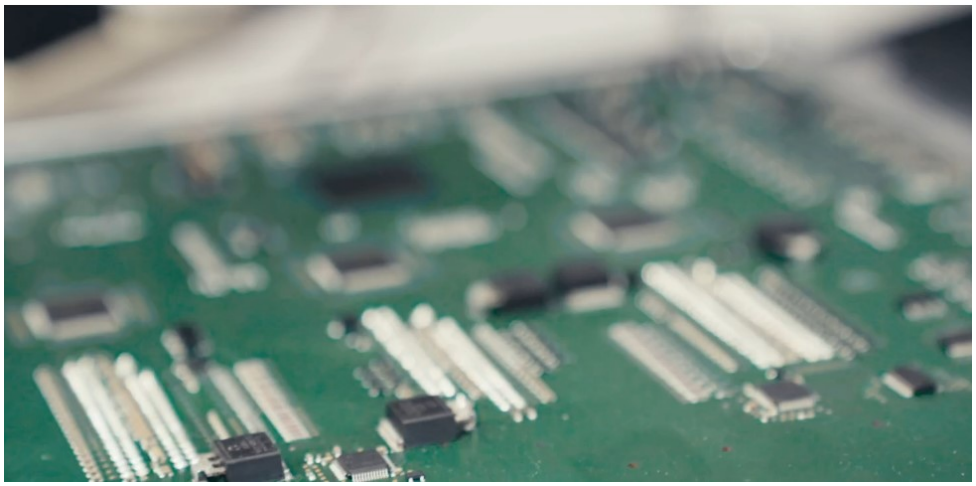


Fig. 5.3 Internal Components of an ECU. Source:[2].

- **MCUs** are pivotal for tasks requiring real-time execution with efficient power consumption and timing performance, running software directly on the CPU within the MCU.
- **SoCs** offer an integrated solution combining multiple electronic components into a single chip, well-suited for resource-intensive applications, including infotainment systems and autonomous driving technologies.

ECUs represent a blend of sophisticated engineering and technological innovation essential for modern vehicles' myriad functionalities. Their design reflects a careful

balance between performance, cost, and resilience to environmental challenges, underscored by the ongoing need to address cybersecurity in the automotive domain.

5.4 Microcontroller Units in Vehicle ECU Applications and Cybersecurity Implications

Microcontroller Units (MCUs) within ECUs are specialized for executing software directly from their internal flash memory, adhering to the stringent real-time requirements essential for automotive control systems. This design principle ensures that critical control software must meet hard real-time constraints and be executed efficiently and predictably. While MCUs can also interface with external flash memory, this is typically designated for non-critical data storage, such as multimedia files in the case of an instrument cluster ECU.

5.4.1 MCU Design and Application

MCU are designed with various configurations to suit specific applications within the vehicle, each variant optimized for particular tasks. For instance:

- An MCU for engine control might be equipped with numerous high-precision timer units necessary for managing engine timing and fuel injection.
- An MCU for body control likely features a broad array of general-purpose Input/Output (I/O) pins to manage a variety of sensors and actuators related to the vehicle's interior functions.

The architecture of an MCU is tailored to its intended function, influencing the peripheral devices and interfaces it supports. This customization is crucial in defining the functionality and potential cybersecurity vulnerabilities of the ECU.

5.4.2 Cybersecurity Implications

The cybersecurity perspective of MCU-based ECU is nuanced, focusing on protecting the integrity of the software and data stored within the MCU's memory. This is

particularly critical for OEM and suppliers, who seek to safeguard their intellectual property and prevent unauthorized access or manipulation of the vehicle's control systems.

Figure 5.4 in the discussion likely illustrates a 32-bit microcontroller, showcasing its multiple peripherals and networking interfaces, which could potentially serve as entry points for cyber-attacks or unauthorized data access.

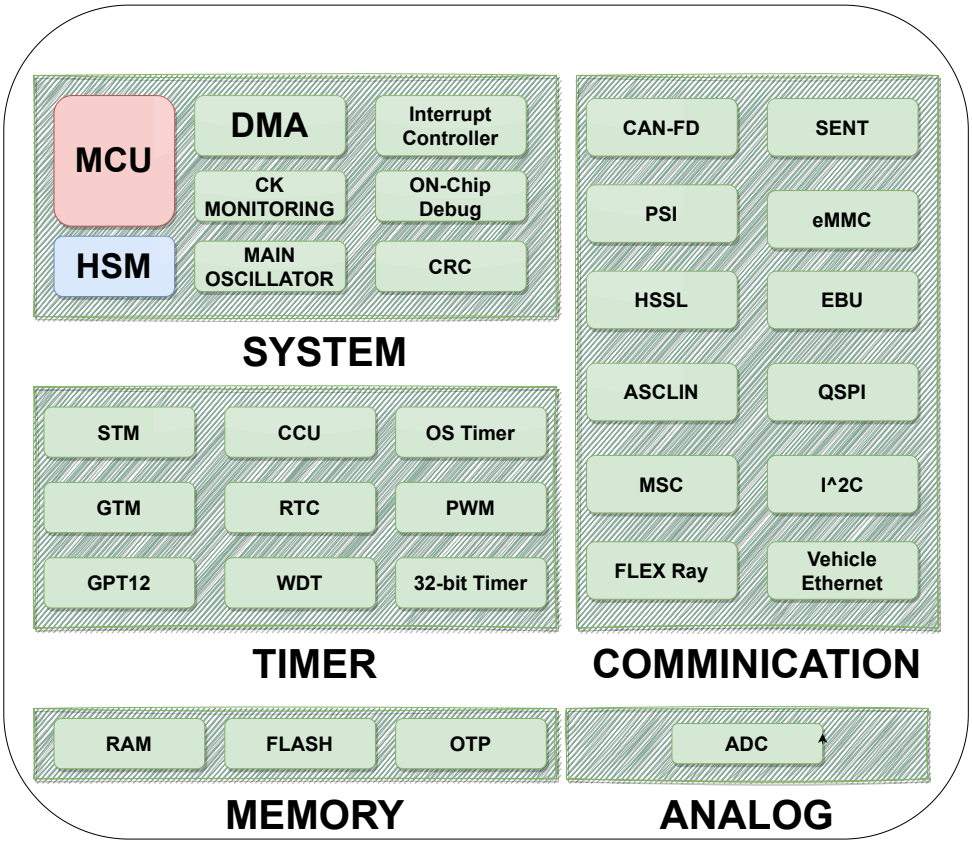


Fig. 5.4 Automtive MCU Block Diagram.

Given the embedded nature of the MCU's memory, direct probing or unauthorized access to the stored contents poses a significant challenge to potential attackers. However, an individual in possession of the ECU could attempt to exploit:

- On-chip debug features
- Serial flash programming interfaces

These avenues might offer indirect methods to access or manipulate the software and data, underscoring the importance of robust security measures in the ECU design phase. OEMs and ECU manufacturers must prioritize the security of these interfaces to mitigate the risk of sophisticated cyber-attacks that could compromise vehicle safety and privacy.

5.5 Hardware Secure Module

In the rapidly evolving landscape of automotive MCUs, the Hardware Security Module (Hardware Secure Module (HSM)) encapsulated into the MCU (Figure 5.4) stands as a critical bulwark against the increasing cyber-attack threats. The HSM aims to protect the integrity and confidentiality of in-vehicle communications and control systems by implementing advanced cryptographic functions and secure key storage. These functions include encryption, decryption, digital signature generation and verification, and secure booting processes, ensuring that a vehicle's software and hardware components are safeguarded against unauthorized access and manipulations.

The E-safety Vehicle Intrusion Protected Applications (EVITA) project, co-funded by the European Union's Seventh Framework Programme, began in 2008. Its objective is to improve the security of automotive on-board networks by creating, testing, and building a framework that guards security-critical components against tampering and protects sensitive data. The project has successfully showcased various security measures for automotive applications through desktop and vehicle demonstrations. Notably, the EVITA standards have been widely adopted by major MCUs vendors, showcasing its significant impact on the industry [59].

- **EVITA** Light: This level is tailored for automotive systems that require essential protection against attacks. It is often deployed in non-critical vehicle components where the risk of attack is relatively low but still presents a potential threat. The Light level focuses on securing the system against common threats and ensuring data integrity for in-vehicle communication. Although it provides a foundational security layer, it does not encompass the extensive protective measures at higher levels. This makes it suitable for applications

where the compromise of the system would have a limited impact on the vehicle's overall security posture.

- **EVITA** Medium: Stepping up the security measures, the Medium level is designed for systems that handle sensitive information and require a higher degree of protection. This level includes enhanced security features such as more robust encryption, secure key storage, and rigorous authentication protocols. It aims to protect components that, if compromised, could pose a significant risk to the vehicle's operational safety but are not deemed critical to its immediate control systems. The Medium level balances robust security and automotive systems' computational and power constraints.

- **EVITA**High: The High level represents the pinnacle of HSM security within the EVITA framework and is reserved for the most critical vehicle systems, such as those directly involved in the control and safety functions. This level implements the highest security standards, including state-of-the-art encryption techniques, dynamic key management, and comprehensive intrusion detection systems. The High level is designed to defend against sophisticated and targeted cyber-attacks, ensuring the resilience of systems crucial for the vehicle's safe operation. This rigorous security measure is crucial for systems where a breach could result in catastrophic consequences, including threats to human life.

Table 5.1 Comparison of EVITA Levels

	EVITA Light	**Evita Medium**	**Evita Full**
Independent MCU		X	X
Internal NVM		X	X
Host Bridge	X	X	X
TRNG	X	X	X
Counter		X	X
Symmetric Cryptography HW	X	X	X
Asymmetric Cryptography HW			X

By categorizing security needs into these three levels, EVITA provides a structured approach to automotive cybersecurity, allowing manufacturers to apply the most appropriate and cost-effective security measures for different components within the vehicle (Table 5.1). This tailored approach not only enhances the overall

security posture of the automotive sector but also ensures that resources are allocated efficiently, balancing the need for protection with the practical considerations of automotive design and functionality.

5.6 Understanding MCU-based ECU Software Layers and AUTOSAR

AUTomotive Open System ARchitecture (AUTOSAR) significantly standardizes ECU software architecture across the automotive industry, improving design and security. This consortium involves vehicle manufacturers, suppliers, and technology companies that collaborate to enhance security measures for ECU software architectures.

The AUTOSAR Classic architecture, supported by the AUTOSAR Real-Time Operating System (RTOS), ensures safety and security for automotive applications by isolating memory, timing, and hardware resources. Essential components include the Microcontroller Abstraction Layer (MCAL) for hardware abstraction, communication and diagnostic layers to secure messaging and diagnostics, and memory and crypto services layers to protect memory contents and cryptographic keys. The runtime environment, Runtime Environment (RTE), separates base software modules from application components, promoting interchangeability and enhancing security among suppliers.

The Flash Bootloader plays a critical role in system integrity and software updates. It manages hardware initialization and software execution securely, including during OTA updates, which is crucial for maintaining system security.

ECU domains organize ECUs into clusters based on their functional objectives, which improves communication efficiency and reduces network load. The Fuel-based and Electric Drive Powertrain domains manage power transmission in vehicles, focusing on performance control and battery management respectively. These are key for vehicle control and safety. The Chassis and Safety Control domain manages vehicle stability and safety systems such as braking and airbag deployment, essential for emergency handling.

The Interior Cabin and Infotainment and Connectivity domains enhance passenger comfort and provide entertainment and connectivity. Given their functionalities, robust security measures are crucial to prevent unauthorized access and theft, and to secure interactive features against cyber attacks.

Cross-domain communication acts as a centralized hub for secure data exchange across different ECU domains, which is fundamental for maintaining overall network security. This streamlined approach ensures that all domains are integrated cohesively, enhancing both vehicle functionality and security.

5.7 Enhancing Security in In-Vehicle Communication Systems

In the field of automotive engineering, the complexity of Electronic Control Units (ECUs) and their specific application areas is critical for enabling the exchange of information across vehicle network systems. These networks are designed with precision to support the flow of data through various in-vehicle networks, leveraging protocols like Controller Area Network (CAN) and Local Interconnect Network (LIN). These protocols ensure reliable data transmission despite the challenging conditions typical of automotive settings. The significance of ECU domains within the vehicle's E/E architecture is their capacity to maintain uninterrupted communication among the network of ECUs, sensors, and actuators. This integration is key to sustaining high performance, even in harsh environmental conditions.

The growing need for increased network bandwidth, spurred by the rising demand for advanced vehicle features, introduces unique challenges, especially in the adoption of automotive bus technologies such as CAN FD, FlexRay Protocol (FlexRay), and Ethernet (Ethernet). These technologies play a vital role in enabling higher data transmission rates and are essential for addressing the intricate security challenges prevalent in the automotive industry. Understanding these technologies thoroughly and recognizing their specific security concerns is crucial for thoroughly examining the various networking protocols utilized within vehicles.

5.8 CAN

The CAN bus is one of the primary vehicle networks, functioning as a versatile multicast serial bus that supports reliable communication, even in noisy environments [58]. The CAN electrical signal transmits information using differential voltages to minimize the impact of noise generated by motors, ignition systems, and switching contacts. The bus consists of a CANH and a CANL, with the differential voltages applied to the bus defining different throughput capabilities, including the High Speed (HS) (ISO 11898-2 [60]) and Low Speed (LS) (ISO 11898-3 [61]) interfaces. In HS CAN, a differential voltage above 0.9V is considered dominant (logic 0), whereas anything below 0.5V is deemed recessive (logic 1). When transmitting a recessive bit (logic 1), both CANH and CANL maintain a 2.5V supply with a minimal voltage difference. In contrast, the transmission of a dominant bit (logic 0) involves CANH increasing to 3.5V and CANL decreasing to 1.5V, resulting in an approximate 2V voltage difference between the two lines. This method enables reliable communication in noisy environments and ensures safe and efficient data transfer within the CAN network. Using twisted-pair conductors is common for physical transmission lines to ensure that both channels experience an equal contribution of magnetic interference. Figure 5.6 displays a generic CAN electrical signals associated with the logical representation in a CAN bit stream.

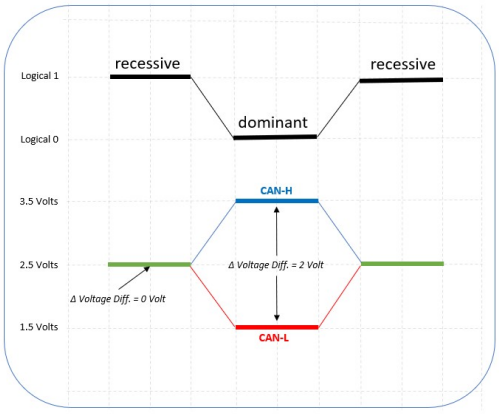


Fig. 5.5 CAN-Bus differential signal. Logic 1 is encoded with both CANH and CANL supplying 2.5V, while logic 0 is encoded with CANH sending 3.5V and CANL sending 1.5V.

Several variants of the CAN protocol exist, supporting different transmission speeds and frame payload sizes, as illustrated in Figure 5.7. CAN FD and CAN

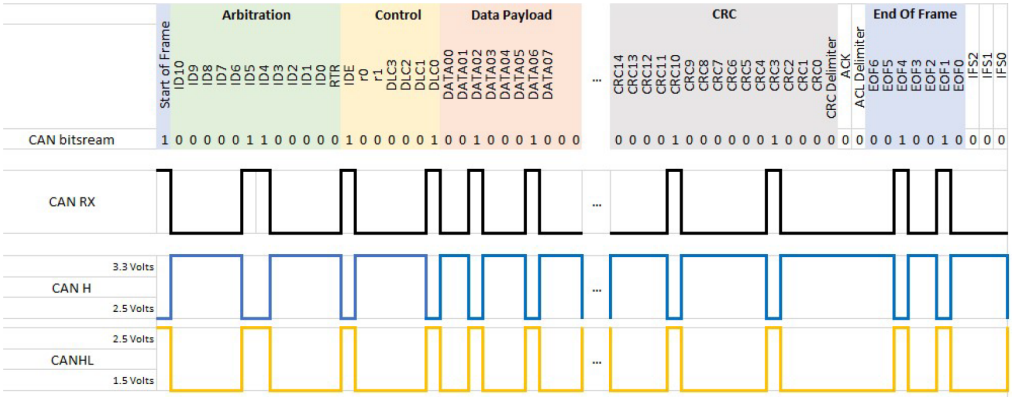


Fig. 5.6 Physical Electrical CAN Scheme

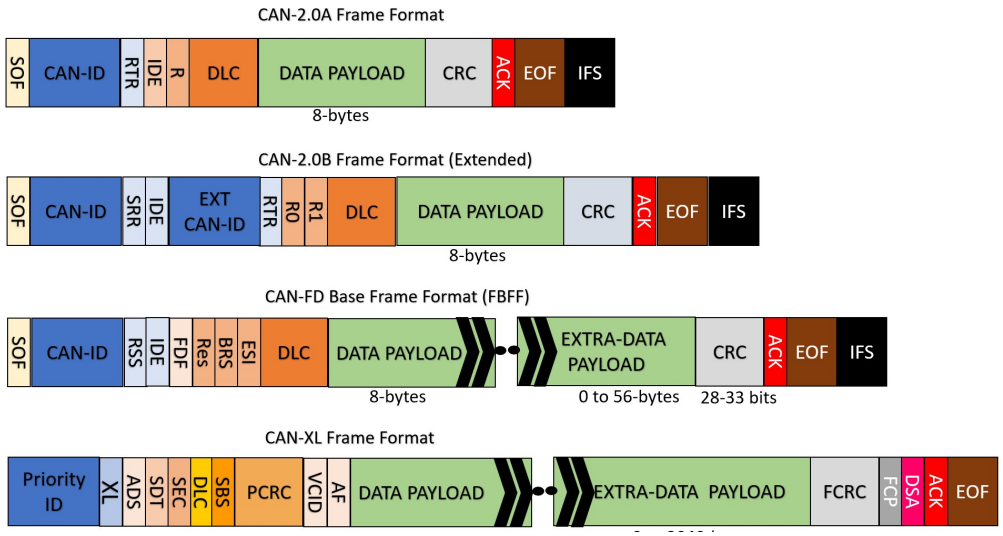


Fig. 5.7 CAN frame structure for different variants of the protocol: CAN 2.0A, CAN 2.0B, CAN FD, CAN XL.

2.0 protocols differ regarding maximum transmission speed and payload data frame size. While CAN 2.0 is limited to 8 bytes, CAN FD extends the frame to 64 bytes. However, in many cases, CAN FD applications still utilize 8-byte payloads to ensure compatibility with existing vehicle CAN databases. A newer version, CAN XL, has been introduced to meet ISO/TC 22/SC 31 Data communication standards [62]. CAN XL offers features such as extended data payload capability (up to 2048 bytes) and a higher communication speed ranging from 500 k/bits to 5 Mbit/s, with the potential to reach 12 Mbit/s in the CAN SIC XL FAST configuration. The CAN SIC XL FAST baud rate is comparable to the 10BASE-T1S technology, a new variation

of the Ethernet standard, also known as Vehicle Ethernet, providing a bandwidth of 10 Mbit/s over a single-pair physical layer, as depicted in Figure 5.8.

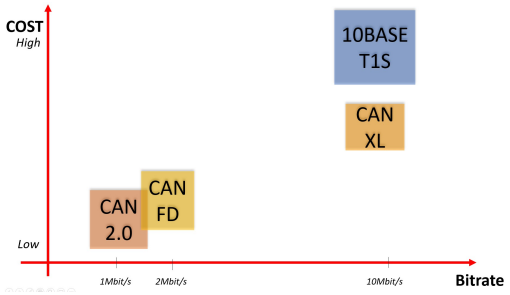


Fig. 5.8 A summary graph for comparing cost and performances among vehicle protocols

From a security standpoint, the CAN protocol introduces various accessibility (i.e., visibility outside the car) and security (i.e., confidentiality, integrity, and authenticity) requirements. Regulations based on country-specific legislation establish a set of messages that are pertinent to legislation and must be accessible through an OBD port in every vehicle [63, 64]. These messages should be in plain text to ensure the information can be accessed using a standard scan tool. However, plain-text messages and external port access pose significant risks to vehicle security. To enhance security, regulations for emission legislation allow for implementing only two of the three security pillars of the CIA triad, integrity and authenticity, while excluding confidentiality [65]. To ensure integrity and authenticity, each CAN data frame is usually instrumented to include an appropriate MAC digest associated with the data payload [66, 67]. Presently, the highest-level security standards for these properties utilize Cipher-based Message Authentication Code (CMAC) [68] signatures or keyed-Hash Message Authentication Code (HMAC), depending on the availability of crypto hardware accelerators. Figure 5.9 illustrates the standard scheme. To protect the system from replay attacks [69], a rolling counter shall be included in each transmitted frame [70].

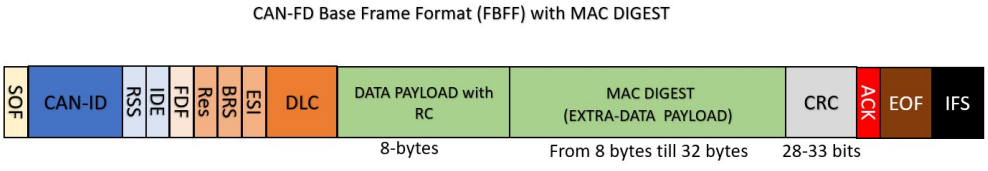


Fig. 5.9 A standard CAN-FD with MAC encapsulated into the payload field.

Utilizing MAC in CAN communication necessitates allocating a portion of the data frame for the authentication digest. According to security guidelines, a truncated MAC digest smaller than 4 bytes no longer ensures cyber resilience. In CAN version 2.0, these four reserved bytes significantly restrict data interchangeability, and the remaining data payload bytes cannot meet the demands of automotive communication. Consequently, CAN 2.0 applications are presently unprotected. Given their data frame size capacity, a 4-byte MAC digest is currently employed in secure CAN FD and CAN XL. However, transitioning the entire vehicle network to these new technologies would incur high costs, as discussed in [71].

5.9 LIN

Modern automotive applications embed over one hundred Electronic Control Units (ECUs). ECUs are connected to other ECUs, sensors, and actuators for managing vehicle systems [58]. Many control strategies are processed in real time, enhancing the network's complexity. The main communication protocols used on standard vehicle networks are the Local Interconnected Network (LIN) and Controller Area Network (CAN). While the CAN provides high-speed communication with solid reliability, the LIN serves domains where high performance and reliability are not primary targets. Thus, the LIN protocol is a viable solution for building a low-cost vehicle communication network. The LIN is a broadcast network with serial master-slave communication and 16 nodes connectable to the bus. A single master manages up to 15 slave nodes for each LIN network (Figure 5.10).

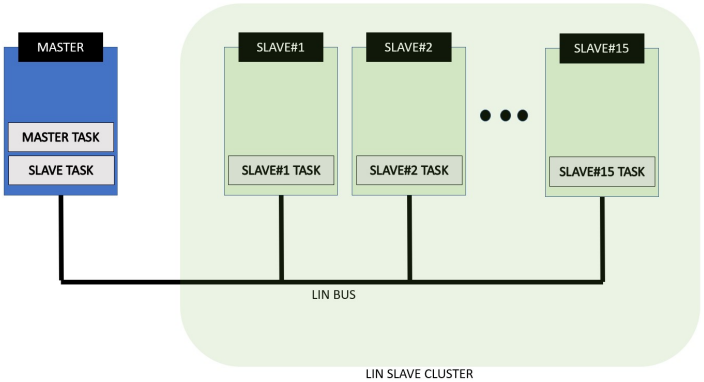


Fig. 5.10 LIN Network Scheme

The main advantages of the LIN are the simplified wiring (i.e., a single wire supported by the major manufacturers), no licenses, and self-synchronization. These are the reasons the LIN is very competitive in terms of costs. The limitations are a slow baud rate of up to 20K bit/s and a small data frame of 8-byte. The master manages the LIN network, always initiating communication with the slaves. A slave contacted by the master replies with a data message. In this scheme, the master polls each slave on a time base. The master assigns a time slot for the slave to reply. This approach makes collision detection unnecessary on a LIN network, meaning that only one device, the master, requires a precise oscillator. The LIN nodes are based on microcontrollers. The LIN is compatible with the Universal Asynchronous Receiver Transmitter (UART) and the Serial Communications Interface (SCI) specifications, making hardware and software implementations simple.

The LIN single-wire bus can reach up to 19.2 kbit/s, with a maximum length of 40 meters, although the LIN 2.2 specifications have increased the communication speed up to 20 kbit/s. The LIN master and slave frames differ (Figure 5.11). The master frame comprises three fields: break field, synch field, and a protected identifier (PID), i.e., a 6-bit field identifying the target slave. The slave data frame includes up to 8 data bytes followed by an 8-bit Cycling Redundancy Check (CRC). The battery

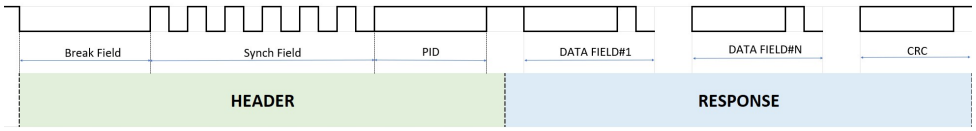


Fig. 5.11 LIN Frame Format

voltage provides the nominal operating voltage for the LIN bus. The sender and receiver have different voltage level requirements. For the dominant bit (logic 0), the sender forces a voltage up to 20% of the battery level on the LIN bus. The receiver interprets a dominant bit when it reads a voltage on the bus lower than 40% of the battery level. For a recessive bit (logic 1), the sender applies 80% of the battery voltage on the bus. At the same time, the receiver interprets a recessive bit reading at a level higher than 60% of the reference battery voltage (Figure 5.12). Different voltage thresholds between sender and receiver handle the possibility of ground shiftings in a vehicle bus, making the system more robust to occasional voltage dropping.

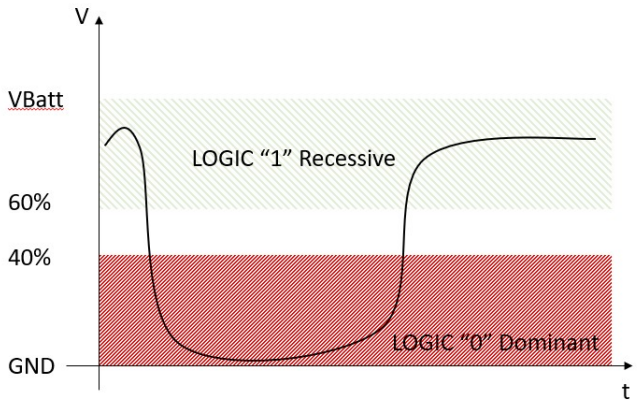


Fig. 5.12 LIN Electrical Signal

Typical automotive applications of the LIN include cruise windshield wipers, turning signals, climate sensors, mirrors, door locks, seat motors, and sensors and actuators belonging to the Powertrain perimeter, like the Mass Air Flow (MAF) sensor and cooling fans.

5.10 Secure Boot

Secure Boot is a vital security feature crucial for protecting systems against cyber threats and ensuring software integrity during startup. This feature is particularly important in Automotive Electronic Control Units (ECUs), where safety and security are paramount.

Secure Boot acts as a vigilant gatekeeper, blocking unauthorized or malicious software from running on the system. It starts verifying at the initial boot sequence and checks digital signatures to confirm the software’s authenticity and integrity. This functionality is also employed during runtime to validate the FLASH content, maintaining security throughout operation.

The significance of Secure Boot in the automotive industry is underscored by several factors:

- ***Enhanced Safety:*** The high safety demands in automotive applications mean any compromise in software integrity could lead to severe consequences, such as accidents or system failures. Secure Boot is crucial in maintaining the integrity of critical software components, thereby reducing the risk of malfunctions due to tampering or malware.
- ***Regulatory Adherence:*** Global regulatory bodies, including the National Highway Traffic Safety Administration (NHTSA) in the U.S., mandate strict standards for automotive safety and security. Compliance often requires robust security measures like Secure Boot.
- ***Data Security:*** Modern vehicles manage large volumes of sensitive data, such as personal information and performance metrics. Secure Boot helps ensure that only authorized software runs on the Engine Control Modules (ECMs), mitigating the risk of data breaches.
- ***Prevention of Unauthorized Modifications:*** Secure Boot is essential in preventing unauthorized modifications to vehicle software, preserving the manufacturer's intended functionality and ensuring the vehicle operates within safe parameters.

5.10.1 Challenges and the Shift to Authenticated Boot

Despite its benefits, Secure Boot can extend the boot time, which is a concern in safety-critical automotive applications that require rapid startup times.

Authenticated Boot offers a solution by maintaining strong security through a Root of Trust (Root of Trust (RoT)) and trust zone, yet facilitates a quicker boot time using One-Time Programmable (One Time Programmable (OTP)) technology. It optimizes the authentication process for elements like Bootstrap, application software, and calibration. After successful authentication, control transitions to the bootstrap portion.

The choice between Secure Boot and Authenticated Boot reflects a balance between security and startup speed, tailored to specific project requirements and constraints.

5.11 Secure Coding

Secure coding is crucial in the automotive industry, especially as vehicles increasingly rely on complex software systems. This section discusses the importance of secure coding for embedded systems, the integration of security with safety, established coding standards, and the adoption of new programming languages like Rust. Embedded systems, such as Engine Control Modules (ECMs), demand high reliability and resilience. Secure coding practices are vital for protecting these systems from cyber threats, thus enhancing vehicle safety.

Standards like MISRA and CERT-C guide safer and more secure software development. MISRA covers safety and security coding practices, while CERT-C focuses on security in C programming. BARR-C promotes explicit coding practices for C and C++ to prevent vulnerabilities.

The Rust programming language, known for its safety and security features like memory safety and strict compiler checks, is becoming popular in automotive applications. Its adoption demonstrates the industry's commitment to improving the safety and security of automotive software systems.

5.12 Memory

Memory security in embedded systems is critical. Systems usually include Memory Protection Units (Micro Process Units (MPUs)) or Memory Management Units (Memory Management Units (MMUs)s, which are essential for security. The choice between MPU and MMU depends on the system's complexity. Bus attacks, a significant threat to memory security, can compromise system integrity. An Input-Output Memory Management Unit (Input-Output Memory Management Unit (IOMMU)) is vital for mitigating this risk.

System designs should incorporate different privilege levels to enhance security. High privilege levels, such as root or supervisor mode, are restricted to specific operations to minimize security risks.

5.13 Anti-Tampering

The automotive industry faces significant challenges from tampering, including debug port attacks and unauthorized modifications through tampering devices available online. Tampering can range from fake data injection, signal conditioning, to subsystem emulation, posing substantial risks to vehicle integrity and safety.

To combat these threats, diagnostic systems and continuous monitoring strategies, possibly enhanced by Artificial Intelligence (Artificial Intelligent (AI)), are essential. These measures help detect and prevent tampering attempts, ensuring compliance with emission standards and maintaining vehicle safety.

5.14 Communication

The attack surface of a CAN presents numerous potential vulnerabilities attackers could exploit. This encompasses strategies for unauthorized access, undermining data integrity, data breaches, executing hijacking maneuvers, or hindering the system. Despite the variety of attack vectors against CAN networks, two main types of attacks have been reported in the literature: (i) Man in the Middle (MitM) [72] and (ii) Replay Attacks [73].

Figure 5.13 illustrates three prevalent automotive attack settings that target the CAN protocol. Each setting is effectively utilized in **MitM** and Replay Attacks. Figure 5.13-A demonstrates an attack through a compromised CAN node, where unauthorized software takes control. This can occur via the corruption of the CAN controller's firmware or by exploiting software module vulnerabilities, such as a buffer overflow. In Figure 5.13-B, an attack is facilitated by a hardware module that isolates the victim node from the rest of the vehicle network, enabling the interception and manipulation of CAN traffic. The final scheme, depicted in Figure 5.13-C, involves connecting an external module to the vehicle's OBD port, granting direct access to the CAN bus. Various commercially available, low-cost CAN modules that feature Bluetooth connectivity support this approach, allowing for programmability via mobile applications. These settings are crucial in laying the groundwork for advanced CAN attacks, exemplified by the Janus Attack [74] and the Cloak Attack [75].

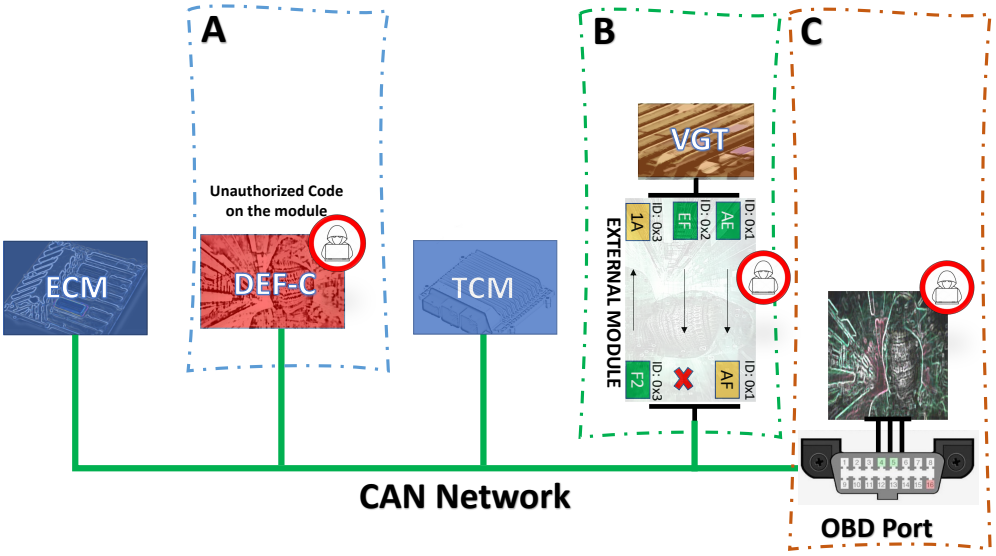


Fig. 5.13 Vehicle CAN network surface attack scheme. A small CAN vehicle network scheme composed of 4 modules: ECM, TCM, DEFC, and VGT. These ECUs communicate with sensors and actuators in real-time, making integration essential for their operation. (A) Corrupted vehicle CAN node runs unauthorized code. (B) Attack vector through external CAN module plugged upstream to CAN victim node. (C) The external CAN module directly accesses the OBD port inside the vehicle cabin.

The **Janus Attack**, a new and sophisticated threat in CAN protocol [74], leverages the CAN protocol synchronization rules and targets devices with different sample points. It involves transmitting a single CAN frame with dual payloads, causing targeted devices to interpret divergent data compared to others in the network. This undermines the atomic multicast principle of CAN, critical for system integrity. It operates by coercing all CAN controllers to synchronize simultaneously, then manipulating the CAN bus level after the first one has sampled the bus but before another does, resulting in valid frames with differing payloads as it exploits the characteristics of the two different payloads to have the same size.

A **cloak attack** in cybersecurity involves manipulating bit signals to deceive networked ECUs [75]. The main idea is that the attacker leverages the different sampling times of two receivers to craft two different frames (FrameA and FrameB). The difference is represented by a selection of bits the attacker alters after the first receiver samples the frame (FrameA). Appropriately crafted, the bit-changes in the second frame (FrameB) can avoid triggering re-synchronization mechanisms, aiming for an optimized bit-string with minimal detection and errors in the Cyclic

Redundancy Check (CRC) field (as the CRC code will be based on the original content of FrameA). If the attacker achieves such duplication, it can generate out-of-sync data in ECUs.

The **Replay Attack** shares similarities with MitM attack. To execute this attack, the attacker must perform a learning phase by monitoring the network and collecting a certain amount of CAN frames. Later, the attacker replays these previously collected frames on the network to achieve a target behavior. Unfortunately, this attack does not require the attacker to possess specific skills, expertise, or advanced knowledge about vehicle CAN networks. These clusters of attacks can be successfully mitigated by linking a CAN Frame payload to a unique MAC that is directly derived from the frame data. Yet, the MAC alone is insufficient for replay attacks due to the CAN payload with identical data producing the same digest. Hence, adopting a rolling counter tied to the data is advised to achieve different digests while maintaining data parity.

The MAC effectively mitigates threats but may also introduce weaknesses in the framework system. This is especially significant in safety-critical, hard real-time systems like ECM, TCM, etc. Ikumapayiet al. formalizes the impact that authentication schemes have on the real-time performance of messages over CAN, CAN FD, and CAN XL based on response time analysis. A CAN frame is schedulable if its Worst-Case Response Time (WCRT) is less than or equal to its deadline. Message deadlines may be implicit, i.e., equal to their period, or explicit (constrained). In particular, Ikumapayi et al. [76] demonstrated that adding a MAC to the payload of CAN, CAN FD, and CAN XL messages might impact the schedulability and the meeting of deadlines based on the percentage of utilization. In particular, on classical CAN, after 70% of utilization, almost all messages fail to meet the deadlines. On the other hand, CAN FD and CAN XL exhibit higher schedulable resilience (it drops when the percentage of bus utilization rises to 80-90%) thanks to the faster bit rate. Nevertheless, pushing such high bus utilization can be malevolent.

When the CAN frames include the MAC in their payload before utilizing the data, the MAC shall be verified as a success. Modern ECUs are generally equipped with a HSM, a dedicated System-on-Chip (SoC) module that manages all cryptographic and security functions, including verifying MACs. The host system is momentarily suspended during the verification process by the HSM. In the context of real-time systems, an attacker might take advantage of this by injecting or flooding the CAN

vehicle network with secure CAN frames that possess a legitimate ID but include counterfeit data and MAC. This situation leads to the HSM being overwhelmed with MAC verification requests that fail, while the host system is forced into repeated waiting periods, causing abnormal delays [77]. These delays can significantly disrupt the system's capacity to adhere to its real-time deadlines, necessitating the initiation of safety system recoveries to address the failure to meet these critical timing constraints.

5.14.1 Bus Overload Attack

The Bus Overload Attack represents a straightforward denial-of-service (DoS) strategy, where the attacker floods the CAN network with frames at the highest possible rate. This flood aims to consume the network's bandwidth, resulting in legitimate frames being delayed or entirely dropped. Such disruptions can lead to partial or total system failures, especially if critical messages fail to arrive in time. The effectiveness of this attack largely depends on the network's configuration and any protective measures in place. For example, on an unprotected bus, sending a frame with a CAN ID of 0 will monopolize the network due to its highest priority status. However, if a gateway filters the frames based on I.D., only those with lower priority might be affected. Notably, standard OBD-II diagnostic messages are assigned low-priority I.D.s (0x7df and above), making them less likely to disrupt critical communications.

5.14.2 Basic Frame Impersonation

Frame impersonation involves tricking a receiver into accepting a fraudulent frame as genuine. This can be accomplished by either connecting directly (e.g., through the OBD-II port) and inserting frames into the network, or by compromising an ECU (such as the infotainment system) to send deceitful messages. A significant challenge with this method is that both authentic and counterfeit frames coexist on the network, potentially causing conflicting actions. A more nuanced issue arises from the CAN protocol's arbitration process, which prevents simultaneous transmission of frames with identical I.D.s. This can lead to arbitration conflicts, increasing the likelihood of errors and potentially causing a "Doom Loop" where two contending frames force each other into repeated error states.

5.14.3 Sophisticated Frame Spoofing

Addressing the limitations of basic spoofing, sophisticated frame spoofing involves timing the transmission of a fraudulent frame to follow immediately after a legitimate one. This tactic aims to replace the genuine data in the receiver's buffer with fake data, exploiting the brief window when the authentic information is present. The challenge here is the precise timing required to intercept and replace the legitimate frame without causing a collision on the network.

5.14.4 Stealthy Error-Inducing Spoofing

This method refines spoofing techniques by exploiting the CAN protocol's error-handling mechanisms. It involves two stages: first, driving a target ECU into an "error passive" state by deliberately inducing errors during its transmission, then intercepting and altering the frame's content after it wins arbitration. This attack is sophisticated because it manipulates the protocol's error-handling features and requires direct access to the CAN bus, bypassing traditional CAN controllers.

5.14.5 Physical Bus Manipulation Attack

If an attacker gains physical access to the CAN bus, they can partition the network and spoof frames to isolated segments. This approach can be usemaliciouslyes, such as altering odometer readings, by intercepting and modifying communication between ECUs. This attack requires a deep understanding of the CAN protocol and the ability to manipulate it at a low level.

5.14.6 Bus Disconnection Attack

This attack aims to isolate a specific ECU from the CAN network, effectively silencing it. By continuously targeting the ECU's transmissions and forcing its Transmit Error Counter (Transmit Error Counter (TEC)) above a critical threshold, the ECU enters a "bus-off" state and ceases all communication. This can have serious implications, potentially forcing the vehicle into a restricted operational mode or triggering fail-safe responses.

5.14.7 Network Freezing Attack

The Network Freezing Attack exploits a legacy feature of the CAN protocol to arbitrarily delay communication across the network. By injecting dominant bits at strategic points in the communication process, an attacker can extend the error recovery phase indefinitely, effectively halting all network traffic. This attack is particularly insidious as it does not increase error counters, making it difficult to detect and diagnose.

Denial of Service attacks

The Denial of Service (DoS) attack is a common technique attackers use to damage a company's reputation. This attack is often carried out by professional attackers who receive compensation for their work. The attack is executed by gaining public access to the CAN network, causing a bus off, CAN frame inhibition, or task overrun event. These remote attacks typically target infotainment systems or exploit the presence of unofficial OBD Bluetooth devices and associated apps.

One way to trigger a DoS attack is to inject unauthorized CAN frames into the network, which increases the bus load until a bus-off event occurs [78, 79]. A more sophisticated approach exploits the arbitration and collision strategy defined by the CAN protocol. During CAN bus arbitration, an attacker sends an unauthorized CAN frame with the correct timing to force a collision with the victim's CAN frame. As illustrated in Figure 5.14, the attacker's frame (`0x24`), with a higher priority than the victim's frame (`0x26`), overrides the original frame, preventing it from being sent.

These techniques can provoke task overrun events in safety-critical hard real-time systems. The check of MAC digests requires non-negligible computational time. Injecting false CAN frames in a secure CAN network can overwhelm the system. The check of counterfeit MAC wastes system resources, causing a high peak of throughput that forces the system into unstable conditions.

To prevent DoS attacks, a secure and safe automotive architecture shall include a CAN gateway that acts as a firewall. This gateway is usually inserted downstream of the OBD port and protects the system from attacks originating from this port. Additionally, setting the I.D. CAN frame filter by hardware can reduce the occurrence of false CAN frames flowing on the vehicle network.

Insider Threats

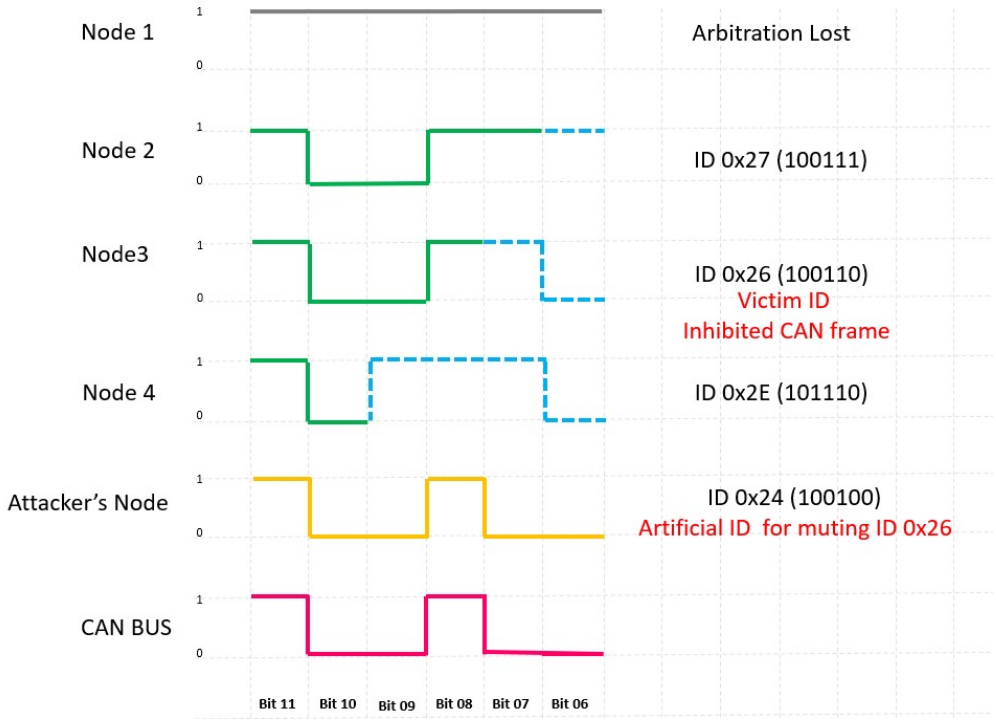


Fig. 5.14 DoS attack schemes

In this context, threats originate from within the system, such as a software bug leading to incorrect cycle implementation. This could erroneously direct numerous CAN frames across the network unchecked, increasing bus load to the point of causing a DoS by forcing the network into a bus-off state. While Man-In-The-Middle (MITM) attacks could theoretically induce a DoS, it's less likely as the intent behind MITM attacks often revolves around gaining unauthorized control or disabling systems for cost savings rather than outright denial of service.

A significant challenge in protecting the vehicle CAN network lies in the legislative requirement for transparency in data transmission, necessitating the transmission of certain information in clear text. This requirement shapes the security approach, focusing on ensuring message authenticity and integrity while foregoing confidentiality to remain compliant with legislation.

5.14.8 Mitigating Attacks on the CAN Bus Network

Mitigating attacks on the CAN bus network involves a multifaceted approach, incorporating various techniques to protect against unauthorized access and ensure the integrity and authenticity of communications. Here's an overview of these strategies:

Intrusion Detection Systems (IDS)

Intrusion Detection System (IDS) monitor network traffic for unusual activity, providing valuable insights into potential breaches. Although they might not stop an attack without additional hardware capabilities, they are crucial for intelligence gathering and forensic analysis post-incident.

Security Gateways

Implementing a security gateway involves using a device equipped with multiple CAN interfaces to segregate and protect network traffic. It acts as a buffer, allowing only verified communication from a secure vehicle control network to pass through to potentially compromised external devices.

Encryption and Message Authentication

Encrypting data payloads is a common security measure; however, it's not always feasible for certain types of CAN messages, such as those required for emission legislation. These messages must remain accessible to a wide range of diagnostic tools and therefore cannot be encrypted. Instead, security for these communications relies on Message Authentication Codes (MACs), which ensure the message's authenticity and integrity without compromising confidentiality. This method safeguards against unauthorized modifications while keeping the data readable for necessary diagnostic evaluations. The MAC effectively mitigates threats but may also introduce weaknesses in the framework system. This is especially significant in safety-critical, hard real-time systems like ECM, TCM, etc. Ikumapayiet al. formalizes the impact that authentication schemes have on the real-time performance of messages over CAN, CAN FD, and CAN XL based on response time analysis. A CAN frame is schedulable if its WCRT is less than or equal to its deadline. Message deadlines

may be implicit, i.e., equal to their period, or explicit (constrained). In particular, authors [76] demonstrated that adding a MAC to the payload of CAN, CAN FD, and CAN XL messages might impact the schedulability and the meeting of deadlines based on the percentage of utilization. In particular, on classical CAN, after 70% of utilization, almost all messages fail to meet the deadlines. On the other hand, CAN FD and CAN XL exhibit higher schedulable resilience (it drops when the percentage of bus utilization rises to 80-90%) thanks to the faster bit rate. Nevertheless, pushing such high bus utilization can be malevolent. When the CAN frames include the MAC in their payload before utilizing the data, the MAC shall be verified as a success. Modern ECUs are generally equipped with HSM, a dedicated SoC module that manages all cryptographic and security functions, including verifying MACs. The host system is momentarily suspended during the verification process by the HSM. In the context of real-time systems, an attacker might take advantage of this by injecting or flooding the CAN vehicle network with secure CAN frames that possess a legitimate ID but include counterfeit data and MAC. This situation leads to the HSM being overwhelmed with MAC verification requests that fail, while the host system is forced into repeated waiting periods, causing abnormal delays [77]. These delays can significantly disrupt the system's capacity to adhere to its real-time deadlines, necessitating the initiation of safety system recoveries to address the failure to meet these critical timing constraints.

5.14.9 Related Works

As the original version of CAN protocol did not include any security support, researchers have come a long way to support it on top of the existing infrastructure or by proposing enhanced versions.

First attempts to improve the security of the CAN protocol and improve resistance to attacks involved including a MAC digest for integrity and authenticity assurance [67], often employing CMAC or HMAC signatures, depending on hardware support. The CAN+ protocol, introduced by Ziermann et al. in [80], aimed to enhance CAN data rates by relaxing constraints during specific transmission time slots. While the CAN application can benefit from the increased speed, its assessment lacked consideration for Electromagnetic Compatibility (EMC) and disturbance handling, which is crucial in the automotive domain. Furthermore, CAN+ relies on media access characteristics not present in the latest CAN FD and CAN XL protocols,

which offer higher payload sizes and data rates. Despite advancements, minimizing latency in MAC signature reception and checking remains essential in CAN FD and CAN XL, which offer increased payload size and data rates.

Significant advancements have been made to enhance broadcast authentication mechanisms, capitalizing on the increased data rate of CAN+. Van Herreveg et al. introduced CanAuth [81], a backward-compatible broadcast message authentication protocol for the CAN bus. This protocol meticulously follows CAN specifications, prioritizing ID-oriented authentication while addressing authentication delays and time synchronization concerns. However, Groza et al. [82] point out that CanAuth's drawback lies in managing many keys associated with message IDs, raising security concerns. In response, they propose the LIBrA-CAN protocol as an alternative. Both LiBrA-CAN and CanAuth share the goal of enhancing CAN communication security but adopt distinct approaches and mechanisms. LiBrA-CAN emphasizes decentralized broadcast-based arbitration and lightweight implementation, ensuring resilience against replay attacks and flexibility in configuration. On the other hand, CanAuth focuses on message authentication and verification, providing robust protection against unauthorized access and tampering. To preserve the integrity of the physical layer, Hazem et al. [83] put forth LCAP, a Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks.

All previous works point out that the MAC size can significantly impact the resistance to attacks, i.e., the MAC size and the time required to elaborate it. To tackle the time constraints, authors in [84] proposed a truncated MAC, justified by the average data size of 15,768 messages from a 2010 Toyota Prius during a 12.27-minute use case. They noted that only a part of the 8 bytes available in the CAN frames were used, making room for a short MAC. Following a similar direction, to further reduce the schema complexity and support all possible CAN protocols, very recently, Luo et al. [85] proposed a lightweight schema based on the introduction of the MAC in place of the CRC field in the 2.0 version of the protocol. While the authors demonstrated the capability of their approach, the back compatibility with standard hardware is not guaranteed, as they will check a CRC value that is not correct.

In general, both approaches go against National Institute of Standards and Technology (NIST) guidelines, stating that a truncated MAC digest below 4 bytes compromises cyber resilience [86]. Ikumapayi et al. [76] have explored the impact of

adding authentication codes as separate messages, noting potential strain on timely delivery, especially given size constraints. As the authors noted, the effect of reserving more than four bytes in CAN 2.0 (i.e., 24Bit-CMAC-8Bit-FV) limits data interchangeability as it requires adding an extra frame to contain the remaining bytes that do not fit into the original frame. However, secure CAN FD and CAN XL protocols support MAC digest sizes from 4 to 16 bytes, accommodating complex protocols like authentications as demonstrated by [82]. Yet, upgrading an entire vehicle network to these protocols involves benefits and extra costs [87], which are left to the manufacturer to evaluate.

Eventually, it is worth mentioning that some recent works support authentication and confidentiality without resorting to MAC [88]. They include only cryptography techniques in the handshake phase, leading to a tiny increase in the latency, limited to hundreds of µs, paying with reduced security if compared with schemas resorting to MAC [89, 90, 82].

Modulation techniques are not new in the security of the CAN protocol; recent efforts by Michaels et al. [91] introduced modulation techniques to enhance the security of the CAN protocol. Their proposal incorporates a rolling secret (watermark) aligned with primary bus messages through multiplexing based on Binary Phase Shifting Keying (BPSK) modulation. While this multiplexed watermark significantly improves security by ensuring transmitted message authentication, it solely addresses this aspect, leaving incomplete coverage to attacks such as MitM, as the watermark can be forged.

Chapter 6

Addressing Automotive Control Modules Hardware Replacement Attacks Through Hardware Signature Mitigation

6.1 Introduction

The automotive market pushes competition in terms of costs to its limit by exploiting the economy of scale. As depicted in Fig. 6.1.a, several suppliers provide the same hardware platform to several customers who act in different heterogeneous domains (e.g., automotive, marine, agriculture, general-purpose equipment) with different cyber-security requirements [92].

Non-secure hardware modules can be readily modified to function in another domain utilizing the same hardware infrastructure, as depicted in Figure 6.1.b. In scenarios where cyber-security measures like secure boot are mandatory, substituting such hardware could circumvent code signature verification, enabling the execution of unauthorized software. Hence, hardware platforms must ensure authenticity.

The employment of Physically Unclonable Function (PUF) and Logic Locking techniques represents a forward-thinking approach in hardware security, as highlighted in the literature [93]. These methods aim to enhance device security by

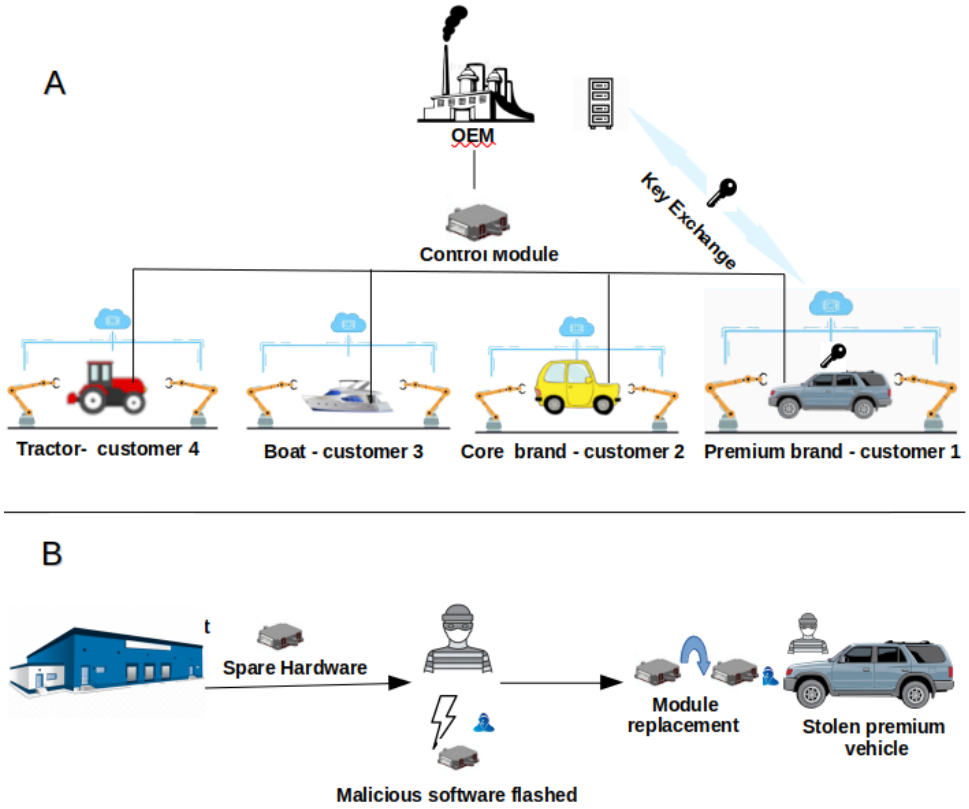


Fig. 6.1 Attack Model Overview: (a) the same control module is in several application domains, and (b) a module can be easily reworked from one domain to another.Source:[3].

granting a unique identity or protecting intellectual property. Nonetheless, their application within the automotive sector is met with significant hurdles. The primary obstacle is the wide array of environmental adversities automotive electronics are subjected to, including but not limited to, extreme temperatures, vibrations, and electromagnetic disturbances. These factors could adversely affect the reliability of PUF outputs and the effectiveness of Logic Locking, emphasizing the need for robust reliability, especially in safety-critical devices.

The automotive industry's demanding conditions pose a substantial challenge for implementing PUF and Logic Locking. Vehicles are exposed to diverse environmental factors such as temperature fluctuations, pressure changes, and humidity levels, which can greatly influence the performance of PUF challenges [94], [95]. Additionally, verifying these challenges often necessitates a specialized infrastructure that works with the existing CAN Bus system, further complicating integration efforts.

The issue of hardware replacements adds another layer of complexity, requiring a sophisticated system capable of associating control modules with specific customers, rather than merely identifying each hardware piece.

Logic Locking involves incorporating a security mechanism within a circuit that triggers incorrect outputs upon receiving an incorrect key [96], [97], [98]. While effective for safeguarding intellectual property, its application in automotive systems is problematic, as incorrect outputs could lead to dangerous conditions or breach safety standards.

To overcome these obstacles, future research must focus on enhancing the resilience and adaptability of PUF and Logic Locking technologies. This includes developing solutions that can withstand environmental variations and protect against complex cyber-attacks, such as hybrid MitM assaults. In such scenarios, attackers might intercept and modify the communication between two parties, potentially bypassing the initial security layers provided by PUF or Logic Locking.

Furthermore, it is essential to establish mechanisms that maintain security throughout the entire lifecycle of automotive components, extending beyond the point of initial verification. Achieving these goals would significantly improve the security and reliability of automotive systems, thereby preserving the integrity and trustworthiness of critical automotive technologies.

PUF and Logic Locking, despite being innovative hardware fingerprinting techniques recommended in scholarly articles, face challenges in the automotive realm. The diverse environmental conditions in which vehicle control modules operate—such as varying temperatures, pressures, and humidity—can negatively impact the success rate of PUF challenges [94], [95]. Additionally, the need for external hardware or control modules to authenticate these challenges calls for extra infrastructure parallel to the CAN Bus, complicating hardware replacement processes. While PUFs excel in uniquely identifying each hardware device, the automotive industry prioritizes the ability to track control modules linked to particular customers. Logic Locking, a method that integrates a security feature into circuits causing them to malfunction with the wrong key, raises safety concerns due to the potential for hazardous outputs and contravention of automotive safety norms [96], [97], [98].

6.2 Countermeasure: Hardware Signature for Automotive Secure modules

In the context outlined in Chapter 4, employing a hardware signature mechanism based on challenge-response presents a robust solution. This method involves equipping each control module board with a specialized Integrated Circuit (IC) designed to create a discontinuity in compatibility among hardware platform subdomains. Should a breach in hardware integrity occur, a corrective measure initiated by supplementary controllers can isolate non-authentic hardware to the greatest extent, thereby preserving system integrity. Certifying subdomains acts as a strategy for distinguishing various customer groups and ensuring the segregation of their respective products.

This segregation is crucial in preventing the utilization of identical control module subdomains across different application domains, even if produced by the same OEM.

Figure 6.2 illustrates a high-level block diagram of the proposed Hardware Signature system for Automotive Control Modules (HSMACM) architecture. This design is intentionally crafted to enhance security by integrating cryptographic elements and secure hashing algorithms, all orchestrated by a dedicated ECU. The ECU plays a vital role in managing security processes and devising authentication protocols essential for protecting automotive communications. The system's core security parameters are securely stored in Read-Only Memory (ROM), ensuring the permanence and protection of critical security data from unauthorized modifications.

A pivotal feature of the HSMACM's operation is the advanced X-RNG, which supports the challenge-response authentication system. It achieves this by producing unpredictable random numbers, thus bolstering the security of communications. The X-RNG is fundamental to the secure transmission of authentication data, facilitated by the CAN FD controller. This controller is key in enabling fast data transfer while maintaining high-security standards, a vital requirement for automotive systems' real-time functionality.

The ECU constitutes the central unit of the module, containing all authentication procedures and strategies. It conducts cryptographic operations and secures communication among automotive control modules against unauthorized access. Employing

elementary secure hashing and cryptographic elements, the ECU lays down a robust basis for verifying the integrity and authenticity of messages within the automotive network.

This comprehensive arrangement provides automotive control modules with a secure and efficient mechanism for authentication and communication, significantly strengthening the security infrastructure of automotive systems. By integrating secure hashing, cryptographic elements, and an innovative random number generator, all meticulously managed by the central ECU, the system establishes a strong defense against cyber threats. This holistic strategy ensures the reliability and safety of automotive operations, enhancing the overall security stance of automotive systems.

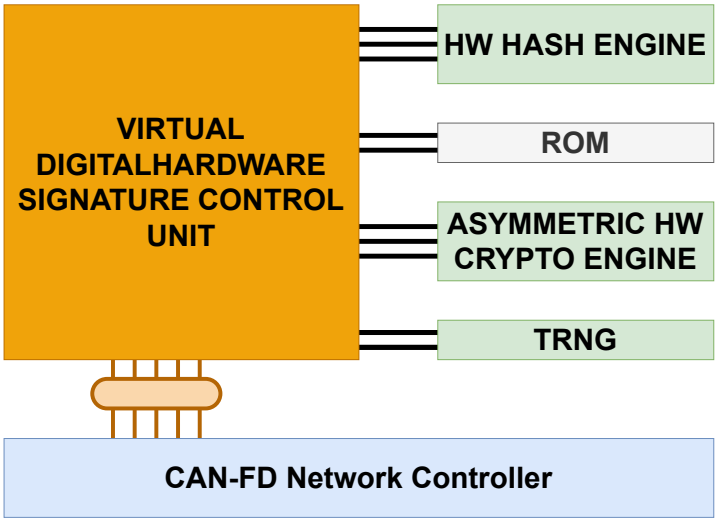


Fig. 6.2 Hardware Signature block diagram: Secure hashing and crypto managed by a Control Unit, with ROM-stored parameters and X-RNG for CAN FD challenge-response.Source:[3].

Modules engage in mutual authentication at arbitrary intervals via a secure challenge-response mechanism. A module's challenge, transmitted over the CAN bus, requires validation by a specified number of network nodes. This validation process is repeated until every device on the CAN network is authenticated. Should a validation attempt fail, the process restarts. Implementing a threshold for the allowable consecutive failures can trigger the system's transition into recovery mode to maintain security integrity.

Key distribution leverages the existing infrastructure. Silicon vendors supply ICs preloaded with the correct company signature in ROM, simplifying the process by adopting a universal signature for each customer. For customers not requiring

enhanced security, the OEM programs the hardware signature ROM with a default value. Consequently, if such components are installed in a vehicle requiring security, the challenge-response authentication will not succeed, prompting the system to enter recovery mode.

In the event of a carmaker's signature key compromise, the risk is mitigated because all platforms and spare parts are pre-equipped with the correct secret key signature in ROM. Following this approach, the additional costs associated with implementing this security measure are marginal, not exceeding 2% of the total ECU cost. A preliminary assessment involves a simulated automotive system architecture running a virtual hardware signature, offering a cost-effective method for evaluating the system's security efficacy.

6.3 Remaining vulnerabilities

While the proposed idea addresses the considered attack models, some minor vulnerabilities remain and must be addressed.

As for all security devices, the Hardware Signature Module must store secret keys. The authentic hardware system is compromised if an attacker violates the OEM's keys.

The hardware signature IC from a secure device could be desoldered to steal the secret key and then soldered on an equivalent board not targeting secure applications to make it compatible with secure vehicles.

Chapter 7

EXT-TAURUM P2T: Extending Secure CAN-FD Architecture for Enhanced Security in Automotive Networks with the TAURUM Paradigm

7.1 Introduction

This chapter explores the complex security vulnerabilities associated with the CAN FD architecture in road vehicles, as discussed in academic research [99]. It introduces the EXT-TAURUM P2T as a revolutionary approach aimed at bolstering the security framework of road vehicles. By directly tackling the vulnerabilities present in the CAN FD system, the EXT-TAURUM P2T not only enhances security measures but also ensures compliance with UNECE standards. This solution maintains all the essential features of its forerunner, including:

- Minimal cost and hardware requirements for enhanced security;
- A dynamic security mechanism through a rolling secret key system;
- Segregated privileges to heighten safety protocols;

- Self-sufficient secret key generation, reducing reliance on external key management infrastructures;
- Increased throughput for secure transactions;
- Protective measures against physical intrusion attempts.

Building on this solid foundation, EXT-TAURUM P2T introduces two innovative functionalities that significantly advance automotive security architectures:

- A cutting-edge speculative MAC calculation feature, seamlessly integrated with an Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug (OSEK) operating system, to improve system resilience against potential overload scenarios often associated with DoS attacks.
- A unique hardware signature framework within the EXT-TAURUM P2T Secure CAN network, designed to counteract emerging hardware replacement threats. This approach, initially suggested in recent research [100], proves that EXT-TAURUM P2T encompasses a full array of security primitives, bridging the gap between theoretical models and practical applications.

EXT-TAURUM P2T marks a significant step forward in "by design" vehicle security, establishing a novel onboard secure communication network that facilitates the protected exchange of critical data across various ECUs responsible for vehicular operations. By creating a security ecosystem that covers the entire security framework without depending on centralized key distribution systems, EXT-TAURUM P2T simplifies data management for automobile manufacturers. This innovative strategy streamlines administrative tasks and significantly reduces associated risks, heralding a safer era in automotive technology.

7.2 Background

In the automotive domain, ECUs are classified into three categories:

1. *hard-real-time*, performing highly safety-critical tasks,
2. *soft-real-time*, for mixed-critical functionalities, and

3. *non-real-time*, for performing the remaining tasks.

Automotive safety-critical systems (i.e., hard- and soft-real-time) adopt specific RTOS compliant to the OSEK open standard [101]. OSEK was founded by a German automotive company consortium supported by the Karlsruhe Institute of Technology and included specifications for an embedded Operating System (OS), Communications Stack (COM), and Network Management Protocol (NM) for automotive embedded systems.

The OSEK specifications impact the embedded software architecture executed on an ECU. Applications are organized into "tasks" that are statically defined at compile time with a fixed priority. Every task can assume three execution states: `SUSPENDED`, `READY`, and `RUNNING`. `READY` tasks are scheduled according to their priority. First In First Out (FIFO) scheduling is used for tasks with equal priority (i.e., round-robin scheduling is not permitted). When scheduled, a basic task runs to completion except when a higher-priority task preempts it or an interrupt is detected. To make sure that real-time deadlines can be guaranteed, deadlocks and priority inversion are prevented by a priority ceiling algorithm [102].

In most OSEK implementations, there is a zero-priority (i.e., low-priority) idle task, also known as the background task. The ECU executes this task until an interrupt moves a different task from `SUSPENDED` to `READY`. The background task can be exploited to perform important activities such as:

- Idle time monitoring;
- Low power microprocessor management;
- Watchdog tickling;
- Non-real-time custom activities;
- Future extensions.

EXT-TAURUM P2T architecture exploits the custom activities provided by OSEK OS to optimize the computational effort to guarantee security as described in subsection 7.3.2.

7.2.1 Automotive Cyber-Security Key Provisioning Infrastructure

CMAC signatures guarantee the authenticity and integrity of CAN messages in automotive applications for all safety-critical and sensitive ECUs. The ECU security hardware architecture defines the number of keys required for CMAC calculation for each secure vehicle [103]. CMAC calculation is a computation-intensive task that requires hardware acceleration. Therefore, the maximum number of secret keys a vehicle can handle strictly depends on the key length and the storage capability of the target Crypto Engine. The typical storage capability of a Crypto Engine today is around 256B. Assuming a 16B key size, it can potentially store 16 keys. The next generation Crypto Engines is expected to increase their storage up to 1 Kbyte, thus accommodating 64 16B keys.

Carmakers must properly handle these secrets. Let us consider a big carmaker selling 10 million secure vehicles per year. If each car in the entire fleet uses a unique set of sixty-four 16B MAC secret keys, the total amount of storage required to handle the keys would be approximately 9GB. This value may increase by a 3x factor by considering complementary information, such as Vehicle Identification Numbers (VIN) or module part numbers.

Interestingly, these numbers do not represent a technical issue for an IT infrastructure. Nevertheless, key management requires significant security investments since data must be shared among different worldwide actors, including manufacturing plants, suppliers, services, and dealers (see Figure 7.1). Maintaining trusted environments and avoiding leakages in this context is not always easy. Any violation compromises the entire vehicle fleet. Carmakers desire to dismiss the IT infrastructure having local key provisioning directly at the vehicle level, with a self-build method to mitigate the above risks.

7.3 Extended TAURUM P2T

EXT-TAURUM P2T is a secure infrastructure addressing the issues discussed in Section 5.14. EXT-TAURUM P2T is based on two independent CAN networks (see Figure 7.2). The "Public CAN" network (depicted in black) transports the standard vehicle CAN raffic and is accessible through the standard CAN Gateway (CGTW).

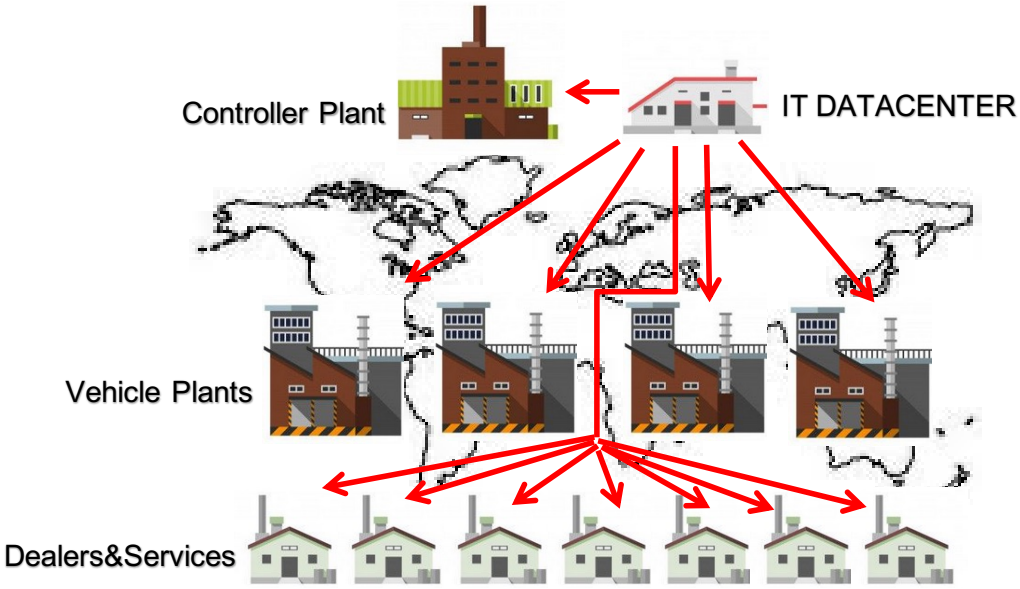


Fig. 7.1 Generic shared secret key proliferation

The "Secure CAN" network (depicted in red) exchanges sensitive information to manage shared keys, security violations, and signatures. Frames exchanged over the "Secure CAN" network are encrypted, and the EXT-TAURUM P2T Secure Gateway (SGTW) ensures controlled access to this network. It establishes privilege levels and manages secret keys required for computing MAC signatures. The main features provided by EXT-TAURUM P2T include:

- A key-sharing mechanism capable of defining isolated "trust zones";
- Sub-domain management of the bus to ensure segregation;
- A rolling MAC secret key infrastructure to implement countermeasures against MitM and replay attacks;
- Dynamic key length adjustment mechanisms and speculative MAC calculation to maximize throughput and increase the complexity of Denial of Service (DoS) attacks;
- A challenge-response hardware authentication mechanism to counter hardware replacement attacks.

To be ready for the automotive industry, EXT-TAURUM P2T is entirely built, resorting to state-of-the-art cryptography and security standards.

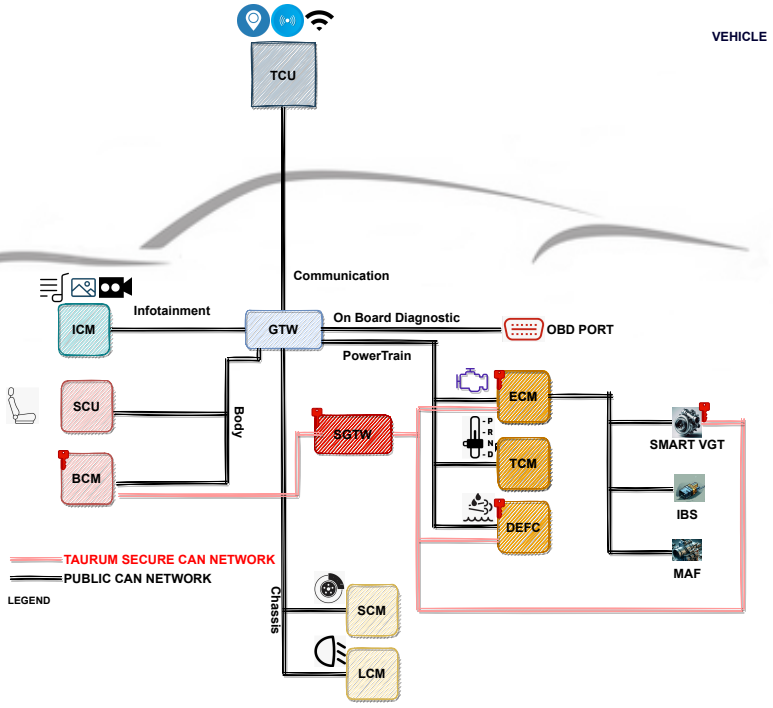
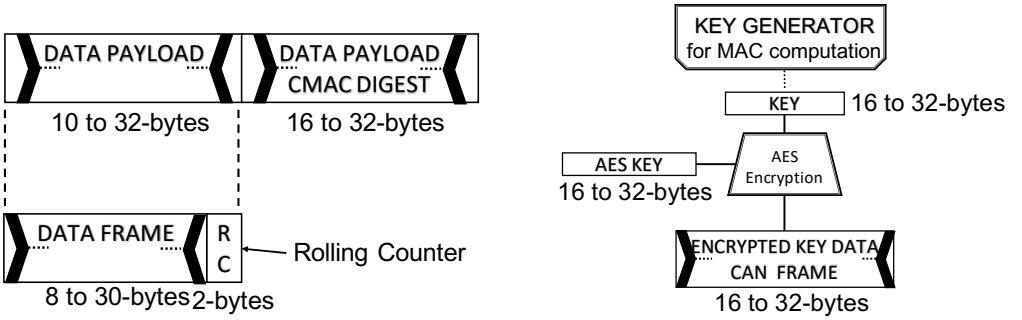


Fig. 7.2 This schematic illustrates the dual-layer configuration of the TAURUM P2T Advanced Secure CAN Network in an automotive setting. The black lines represent the public CAN network, managed by the Gateway (GTW), facilitating standard communication across vehicle systems. In contrast, the red lines depict the Secure CAN network, controlled by the Secure Gateway (SGTW), which handles encrypted and secure data transmissions, ensuring enhanced security for critical vehicle operations. Source:[4].

EXT-TAURUM P2T requires a data rate of up to 8 Mbps and 64B data frames to be implemented. These requirements are met by the CAN FD extension of the original CAN bus protocol [99]. The two communication networks transport the two classes of data frames depicted in Figure 7.3: the Public CAN FD frame transmitted over the Public CAN (Figure 7.3a) and the Secure CAN FD frame transmitted over the Secure CAN (Figure 7.3b).

The integrity and authenticity of Public CAN FD frames are ensured by appending a CMAC digest of the data payload to each frame. The computation of the CMAC signature, however, is a process that demands considerable time.

Through profiling the CMAC computation times on actual automotive hardware, it was determined that the most secure architecture capable of meeting the worst-case throughput demands would utilize a 256-bit length for both the data and the CMAC



(a) PUBLIC CAN-FD Frame: a payload 26 bytes to 64 byte long divided into data payload and CMAC digest required for authenticity and integrity purposes

(b) SECURE CAN-FD Frame: encrypted message sent by the SGTW to all the secure modules for key update and security management purposes.

Fig. 7.3 TAURUM P2T Frames.Source:[4].

digest. This setup provides the highest level of cryptographic security, allowing for less frequent updates of the secret key. Achieving comparable security levels with a shorter digest length is possible but would necessitate more frequent updates of the secret key, thus offering a balance between the digest size and the key refresh rate. Nevertheless, CMAC alone may not suffice for safeguarding data transmitted over the public CAN network. Messages that convey steady-state information, which do not change over time, are vulnerable to replay attacks. To mitigate this risk, Public CAN FD frames include two bytes dedicated to a rolling counter, enhancing protection against such threats [70].

The generation of a CMAC digest necessitates the sharing of a secret key between the sending and receiving ECUs. In the intricate environment of vehicle systems, the requirement for secure communication is not uniform across all ECUs. Each ECU is tasked with secure communication with specific groups of other ECUs, based on the functions they perform. To bolster security, communications between tasks executed on different ECUs should be segregated wherever feasible. To address this challenge, EXT-TAURUM P2T incorporates the notion of Privilege Level (PL) in communication strategies, as depicted in Figure 7.4.

Privilege separation is a fundamental security feature introduced by EXT-TAURUM P2T. Every secure ECU, a Secure Node (SN), is associated with a PL. Each PL holds a dedicated secret key (K_{PLi}) used for MAC signature computation between tasks executed at the same level. Privileges are organized in a hierarchy with low numbers indicating higher privileges. An ECU working at PL_i holds all secret keys

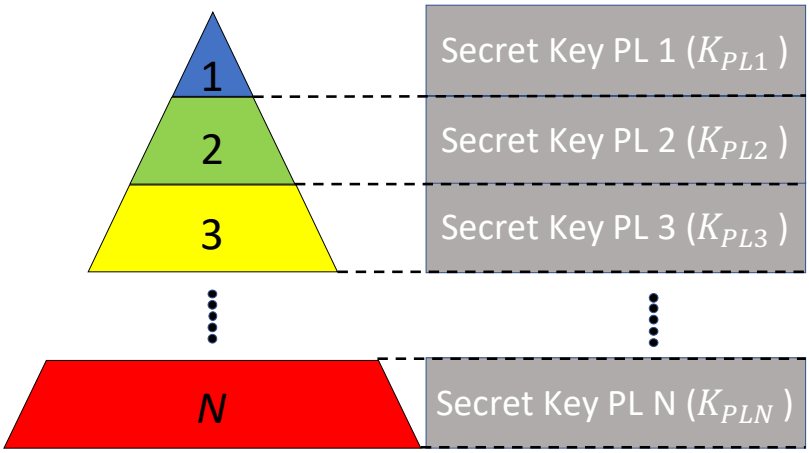


Fig. 7.4 TAURUM P2T Privilege Hierarchy Block Scheme. Lower numbers indicate higher privilege levels. Level 1 usually represents the SGTW. Source:[4].

form PL_i to PL_N (i.e., $K_{PLi}, K_{PLi+1}, \ldots, K_{PLN}$). It, therefore, can communicate with its counterparts at the same PL or with counterparts at lower PLs.

With this mechanism, EXT-TAURUM P2T implements security segregation. Suppose an attack on an ECU succeeds in compromising its secret keys. In that case, only the ECU privilege level and all lower levels will be compromised until the activation of recovery countermeasures or updates of the private keys occurs. Communication at higher PLs remains active, thus minimizing the attack's impact on the vehicle's functionalities.

EXT-TAURUM P2T privilege separation also implements an additional feature to handle specific vehicles' security requirements. Road vehicles are often equipped with so-called secondary controllers. Usually, these modules have reduced hardware capability for meeting security requirements (e.g., key length restrictions). Directly connecting these devices to the entire network would decrease the overall security of the whole system. To avoid this, EXT-TAURUM P2T exploits PLs to define so-called security sub-domains. In a security sub-domain, the strength of the secret keys can be reduced (e.g., 8B or less) to fit the system throughput constraints better, helpfully allowing other parts of the system to work with more robust protections. This requires a more frequent update of the secret keys in sub-domains using shorter keys.

Figure 7.5 provides an example of how sub-domains can be exploited. In this example, the SGTW works at level 1, while all non-critical devices of the network

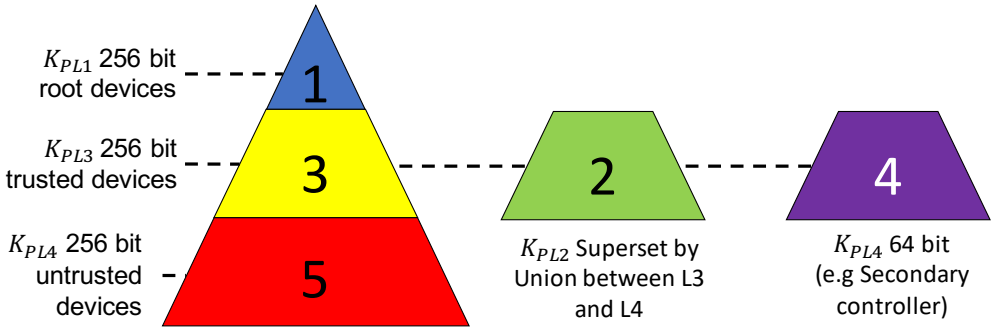


Fig. 7.5 TAURUM P2T Privilege Hierarchy with different key size. Source:[4].

work at level 5. All safety-critical modules work at level 3, except a secondary controller with limited computing power that works at level 4. Finally, level 2 is associated with a sub-domain gateway module, thus keeping the secondary controller isolated from the other nodes of the CAN network.

The way privilege levels are assigned is application-dependent and aims to fulfill the architecture's security requirements.

7.3.1 Secure CAN and Key Provisioning

The role of the EXT-TAURUM P2T secure CAN is to provide a secure channel to implement key provisioning and therefore share the secret keys (K_{PLi}) required by all SNs for CMAC digest calculation.

Communication on this channel must be fully secure and guarantee confidentially integrity and authenticity. State-of-the-art symmetric cryptography based on the Advanced Encryption Standard (AES), implemented with the Cipher Block Chaining (CBC) modality, represents the best approach to secure this communication channel [104]. The same PL secret keys (K_{PLi}) used for CMAC digest calculation are also used for encrypting communication at different PLs on the secure CAN network. To keep a high level of security, these secret keys are periodically rolled. The rolling time and the digest size are parametrized to ensure the highest flexibility.

This secure communication infrastructure setup requires a mechanism to distribute the secret keys to the different ECUs. As discussed in subsection 7.2.1, the secret key distribution infrastructure is among the main challenges for carmakers in developing a large fleet of connected vehicles. EXT-TAURUM P2T removes this

bottleneck by introducing a mechanism to generate all secrets on-board through the SGTW and securely share them with all connected nodes. This solution reduces the need to find trusted users and sustain a secure infrastructure.

Figure 7.6 outlines the EXT-TAURUM P2T key provisioning protocol. During the first vehicle initialization at the plant (step 1), the SGTW performs a network discovery phase to map all SNs connected to the Secure CAN (i.e., those that require exchanging CMAC signed frames on the public CAN). It then generates using its local Crypto Engine the first set (time 0) of all PL secret keys ($K^0_{PL1}, \cdots, K^0_{PLN}$) and securely stores this information in its internal memory (step 2). After a complete network discovery, the SGTW handles the key provisioning node by node.

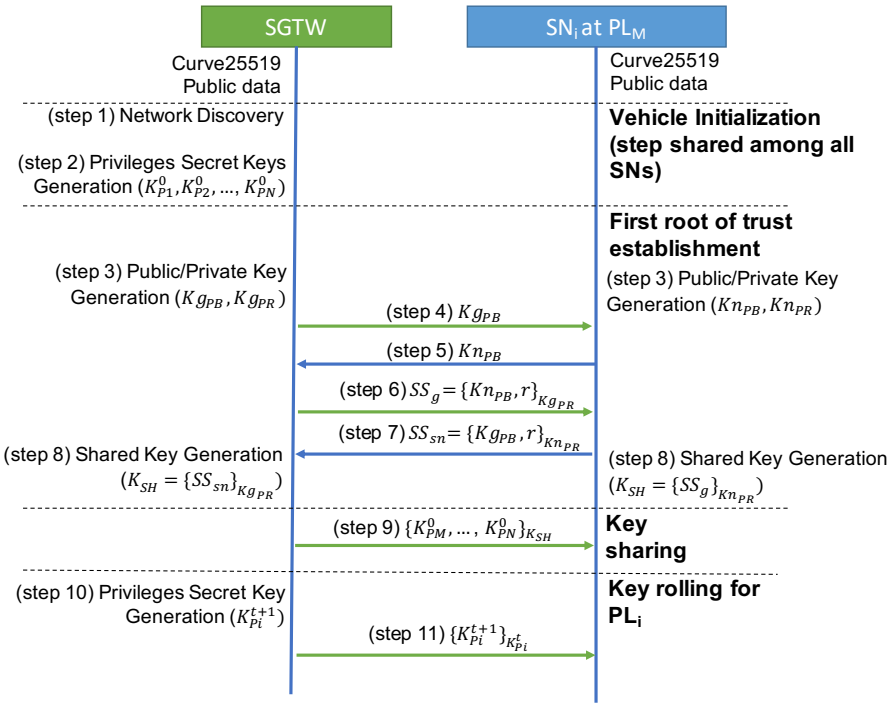


Fig. 7.6 TAURUM P2T Secure CAN key provisioning protocol based on symmetric cryptography. Source:[4].

To establish the first root of trust between the SGTW and a given secure node (SN_i) with privilege PL_M, EXT-TAURUM P2T resorts to elliptic-curve cryptography (ECC) [105]. Every ECU connected to EXT-TAURUM P2T stores the same curve as public data in its flash. Curve25519 has been selected since it is one of the fastest ECC curves enabling it to fit hard real-time constraints, it offers 128 bits of security (256 bits key size), and any known patents do not cover it [106].

ECC shared keys are used to provision MAC secret keys during the network's initialization or when an attack is detected. They make it possible to build a secure point-to-point network between the SGTW and each ECU.

The SGTW and the SN start the establishment of the first root of trust (step 3) by generating a public/private key pair ((Kg_{PB}, Kg_{PR}) for the SGTW and (Kn_{PB}, Kn_{PR}) for the secure node). The SGTW uses a different key pair for every node. The SGTW and SN exchange their public key (steps 4 and 5) and use it to build two shared secrets (SS_g and SS_{sn}), adding a nonce to the received public key. After encryption, these secrets are exchanged using the local private keys (steps 6 and 7). The shared secrets are used to generate the first shared key K_{SH} (step 8). This shared key is used to securely transfer the secret keys starting from PL_M (the PL of the SN) down to PL_N ($K^0_{PLM}, \cdots, K^0_{PLN}$ in step 9). At this point, the node holds the secret keys and can start communicating with other nodes on the public network using CMAC signed frames.

Generated keys are valid for a limited time frame. Each PL sets a rolling timer to decide when to roll its related key. Whenever the rolling key time of PL_i expires, the SGTW generates a new key (step 10) and then transmits the new key to all nodes connected to that level using the previous key. The secret key update is not only time-based but can also be event-based. A specific event, like init, shutdown controller procedure, etc can force an update.

EXT-TAURUM P2T implements a deprecated key functionality. When the violation of an ECU is detected, the SGTW can mark the related PL secret key as deprecated. Figure 7.7 shows an example of this mechanism. Starting from a valid condition with several ECUs connected at PL_3 (Figure 7.7A), the SGTW detects a compromised DEFC module (Figure 7.7B). The secret key for K^t_{SH} is then marked as deprecated (Figure 7.7C). All ECUs connected at the same PL or higher are informed and receive a new key K^{t+1}_{SH} encrypted using their K_{SH}. This isolates the compromised node on that level through privilege downgrading.

EXT-TAURUM P2T also includes a Short Secret Key mode providing each SN with an additional short key (e.g., 16B) in specific conditions. Forcing the network to work with shorter digests and keys saves throughput and computation resources. This mode helps to gain extra hardware resources for counterattacking or managing high throughput peaks.

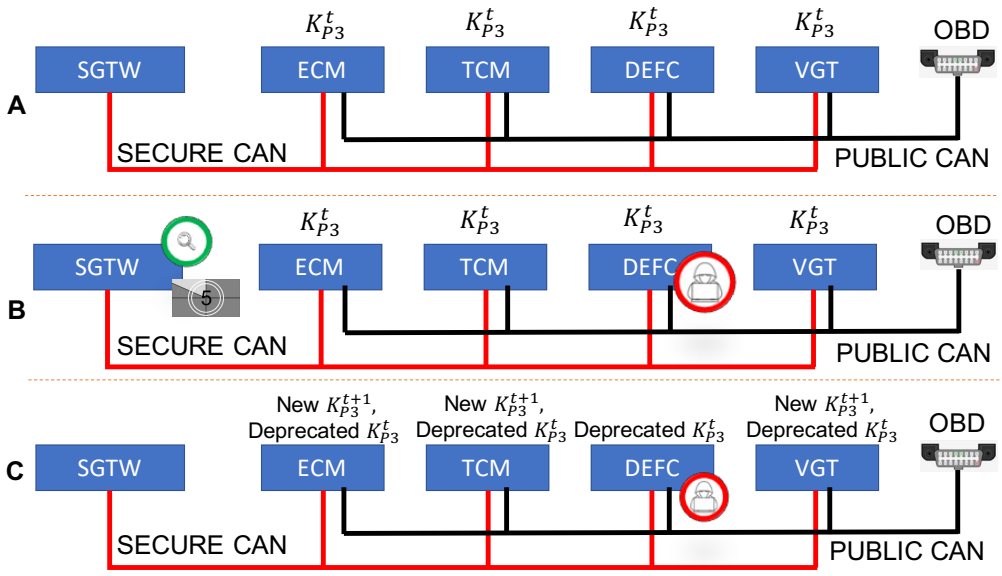


Fig. 7.7 TAURUM P2T Secret Key Deprecate Status. Source:[4].

To summarize, Figure 7.8 shows the secret keys that every module must handle in an EXT-TAURUM P2T architecture. EXT-TAURUM P2T centralizes hardware resources into the SGTW, allowing for a more flexible and lighter security resource into the rest of the connected modules. All controllers can implement a minimal encryption function with limited storage capacity.

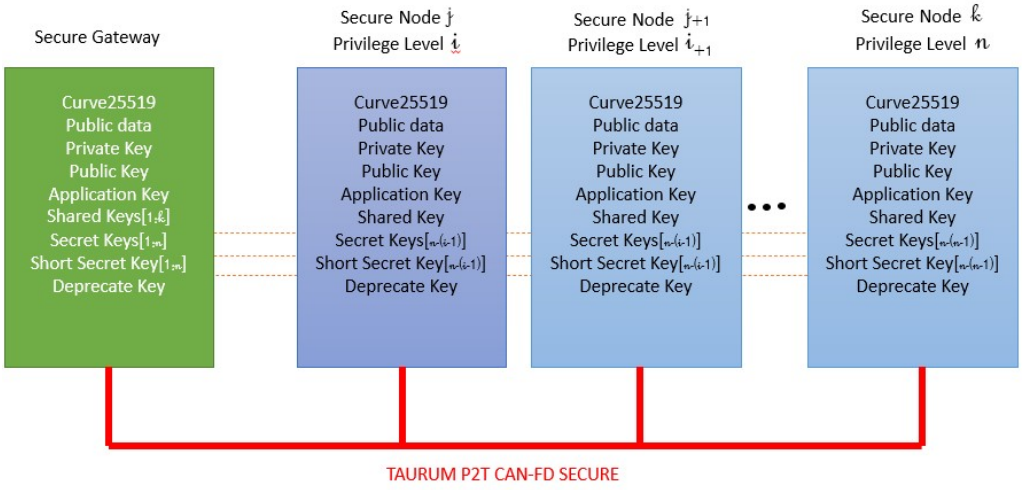


Fig. 7.8 Summary of EXT-TAURUM P2T shared secrets. Source:[4].

7.3.2 Speculative MAC calculation

The throughput is a sensitive parameter inside real-time systems, as discussed section 7.4. Security mechanisms, particularly CMAC computation, profoundly impact the system's throughput. Attackers can exploit communications peaks to generate DoS attacks. Therefore, reducing the network traffic in normal conditions is essential to have a margin when handling critical situations. To support this goal, EXT-TAURUM P2T introduces a speculative MAC computation mechanism to optimize the CPU load in connected ECUs, thus avoiding missing real-time deadlines during critical transient conditions.

To understand how this mechanism works, let us start with a quick overview of how CMAC is used in CAN communication to guarantee the integrity and authenticity of a transmitted frame. To avoid reply attacks, the frame transmitter computes a signature (CMAC digest) of the plaintext data concatenated with a rolling counter. The plaintext data, the rolling counter, and the CMAC digest are embedded in the CAN frame payload and transmitted over the CAN network (Figure 7.9). Before using data contained in a frame, the receivers must calculate the CMAC digest again and compare it with the one included in the transmitted frame. If the two digests are the same, the integrity and authenticity of the CAN message are verified, and the frame can be used; otherwise, it is discarded and considered unauthorized. The system moves in a recovery mode when a receiver often gets CAN frames with an invalid digest. The system proceeds to a recovery mode in this second situation, depending on the function connected with the transmitted frame.

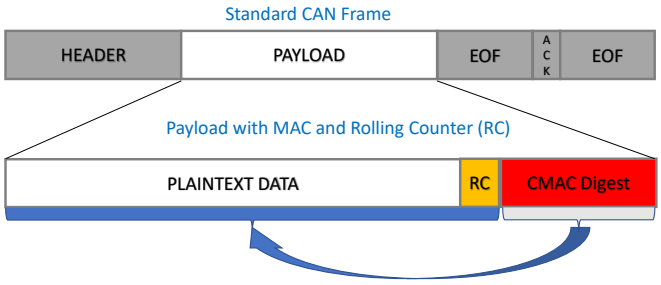


Fig. 7.9 Use of MAC in CAN frames to guarantee integrity and authenticity. Source:[4].

CAN data frames usually transport information obtained from the measurement of physical signals (e.g., temperature, pressure, rotation speed, etc.). While some of these measurements continuously change over time, other measures have slow

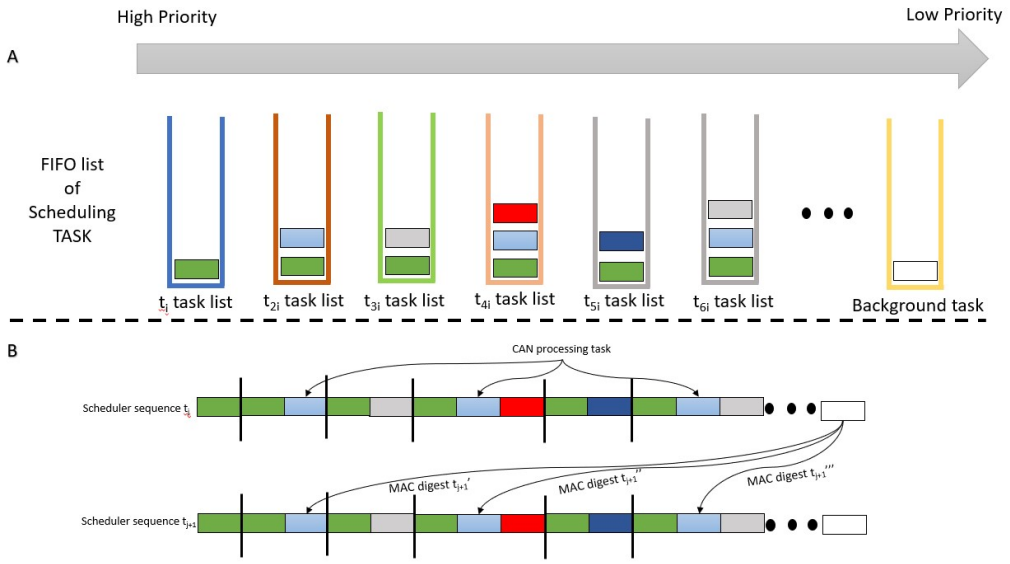


Fig. 7.10 EXT-TAURUM P2T Speculative MAC calculation implemented in generic RTOS. Source:[4].

changes and remain steady when considering short periods. Typically, steady-state signals are part of the following domains: temperature (e.g., Air Ambient temperature frame), atmosphere pressure (e.g., ambient pressure frame), voltages (e.g., battery voltage when generator's contribution is none), etc.

In this context, it is possible to predict the future data frame payload and understand if there will be a difference or not, just monitoring specific system parameters. In those cases, the rolling counter introduced to avoid reply attacks is the only change in consecutive CAN data frames. EXT-TAURUM P2T exploits this property to implement speculative MAC calculation thanks to the characteristics offered by the OSEK operating systems executed on automotive ECUs.

Figure 7.10-A represents a high-level view of how an OSEK operating system schedules tasks. Each colored rectangular is a task with its priority. Tasks at the same priority are scheduled according to a FIFO policy. When no task requires the CPU, the background task is executed. Figure 7.10-B shows the same task scheduling from a different perspective. Let us focus on tasks receiving and processing CAN data frames (light blue rectangles). Before using the information contained in a frame, these tasks must compute the CMAC digest and compare it with the one stored in the frame to perform message authentication. The speculative approach

of EXT-TAURUM P2T delegates the digest computation for all frames containing steady-state measures to a low priority task (background task), keeping just the comparison instruction between the two digests in the original task. In Figure 7.10-B, at time t_j the background task computes speculative MAC digests for steady-state frames that are used for message authentication at time t_{j+1}.

It is essential to highlight that the speculative MAC does not introduce any security threat to the system. The speculative MAC computation operates at the receiver's side following a flow summarized in Figure 7.11. CMAC digests for CAN frames that likely transmit steady-state information (steady-state frames) are computed in a background task exploiting idle CPU time and stored for later use. When a frame arrives, the receiver first compares the frame digest with the speculative digest that is already available. If the comparison succeeds, it means the frame contains steady-state information, and the speculative MAC mechanism could predict it in advance. The frame can be considered secure and used for further computations. If this check fails, either the frame is corrupted, or the contained information is not steady-state, and therefore the speculative MAC was unable to perform a correct prediction. In this case, the receiver switches back to a standard validation flow. It extracts the plaintext and rolling counter from the frame and computes the MAC digests. It then compares it with the one stored in the frame to assess its integrity and authenticity. If this comparison succeeds, the frame can be used. Otherwise, it must be discarded.

Moving MAC computation to a background task has an enormous advantage. Its operations are not under real-time constraints and do not contribute to CPU real-time utilization. Furthermore, this approach allows also to solve safety's constraints, being safety put in a strong relationship with the real-time, and all tasks outside the real-time domain are considered without any impact on safety.

Speculative MAC computation is a valuable technique to mitigate secure hardware overload peaks.

7.3.3 Hardware signature for branding system

EXT-TAURUM P2T provides a secure communication infrastructure to implement the hardware signature mechanism conceptually introduced in [100], able to avoid the hardware replacement attack described in section 5.

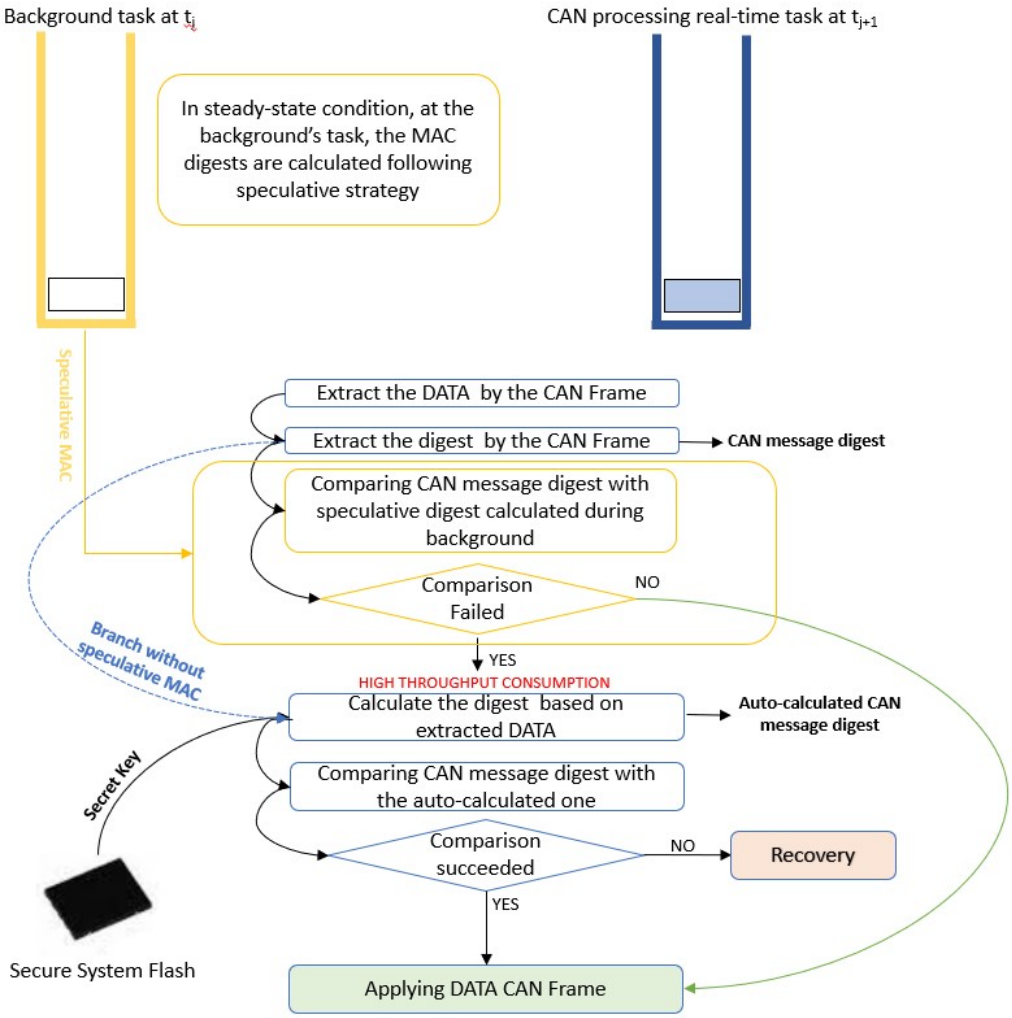


Fig. 7.11 MAC Speculative Strategy block scheme. Source:[4].

To generate a compatibility discontinuity among hardware platforms integrated into different market subdomains, every carmaker buying parts from OEM must securely store a shared secret K_{apk} into every ECU (including the EXT-TAURUM P2T SGTW). This secret is unique for every carmaker and is used to verify the origin of the ECU.

During operation, the EXT-TAURUM P2T SGTW uses the Secure CAN network to periodically initiate a distributed hardware verification protocol depicted in Figure 7.12. The verification process is local to every PL. Considering privilege level m, SGTW selects a target ECU to be verified randomly. It generates a nonce *r* and sends it over the Secure CAN network encrypted with the corresponding PL

key K_{PLm} (step 1). It then shares the same random challenge over the Secure CAN network with all other ECUs working at the same PL (step 2).

At this stage, the challenged ECU must answer the challenge by encrypting *r* using the carmaker secret key K_{apk} and sending this information back to the SGTW and all other ECUs at the same PL encrypted with the PL secret key K_{PLm}. The SGTW and all ECUs that receive the challenge response can act as verifiers, checking the correctness of the response. Suppose at least one ECU detects a violation. In that case, the EXT-TAURUM P2T key deprecation feature can be activated to isolate the complete PL subdomain in the network and initiate a recovery action to exclude non-authentic hardware to keep the system safe for a certain period before permanently invalidating the compromised module. In case of a failed response without recovery mode triggered by SGTW, SGTW is compromised too. Another way to identify a discredited SGTW is to monitor the challenged module selection. If nodes detect that a particular node has never been challenged is a symptom of a tampered network.

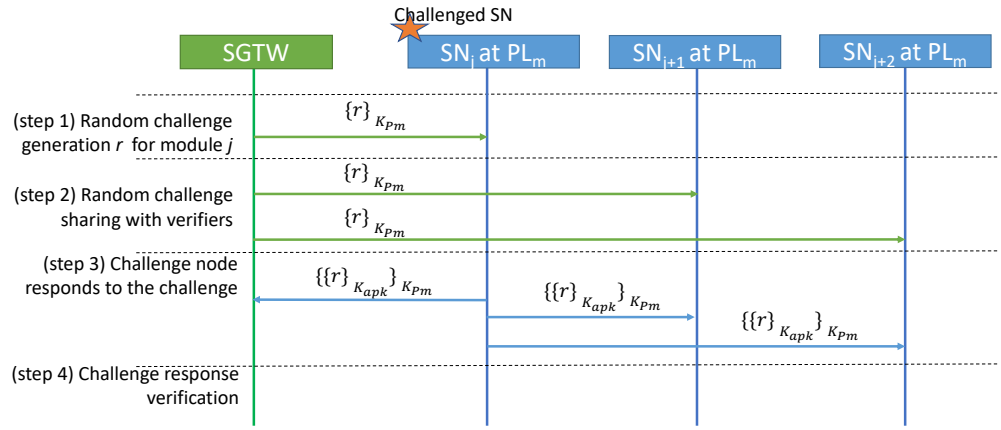


Fig. 7.12 EXT-TAURUM P2T Hardware Signature with challenge-response authentication. Source:[4].

The carmaker's secret key becomes the critical security actor in this condition. However, information leakage for a specific company does not become a threat for all companies with the same hardware platform since they all have a proper programmed secret key.

7.4 Experimental Results

The EXT-TAURUM P2T Secure CAN network concept underwent extensive evaluation through a detailed simulation of a vehicle network architecture. This simulation emulated the communication between two ECUs, represented by the SGTW and two CAbn nodes. This setup aimed to reflect the interactions typically observed within a modern vehicle's communication system.

In our experimental setup, the communication between the ECUs was facilitated by a standard CAN database (db), which defined the structure and protocol of the messages exchanged over the network. The use of a typical db CAN ensures that our simulation mirrored real-world conditions and standards, providing a robust platform for testing the EXT-TAURUM P2T system.

The centerpiece of our testing environment was the neoVI FIRE 2 Multi-Protocol Vehicle Interface, produced by Intrepidcs [107]. This device was adeptly configured to handle a CAN FD baud rate of 500Kbit/s, enabling high-speed data transmission that is critical for real-time vehicular communication. The EXT-TAURUM P2T was programmed to efficiently manage up to five payload layers (PLs), which demonstrates its capability to enhance security measures in a high-load network environment (Figure 7.13).

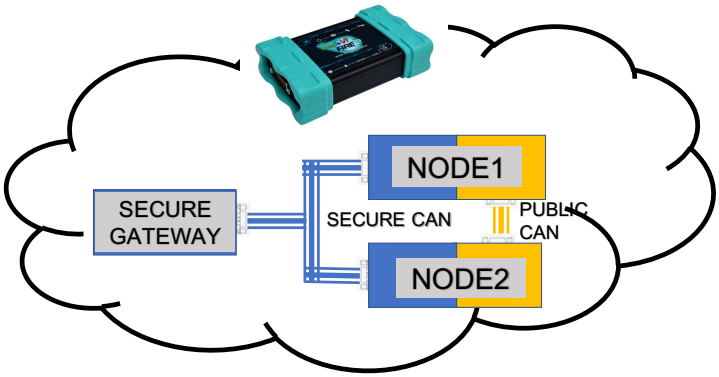


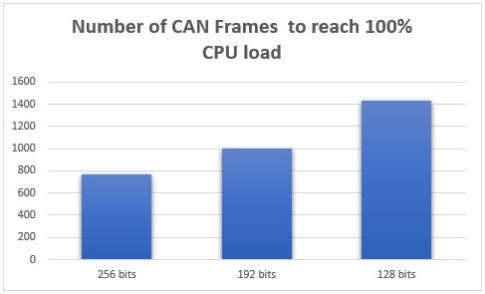
Fig. 7.13 EXT-TAURUM P2T simulation environment setup. Source:[4].

The Python programming language was utilized to develop the entire communication stack, ensuring a flexible and detailed integration of all protocols. The simulation tests provided critical insights into the feasibility and performance of the EXT-TAURUM P2T system under realistic operational conditions. These experimental findings confirm the practicality of the EXT-TAURUM P2T architecture and

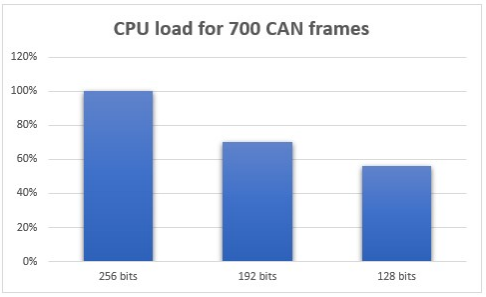
highlight areas for further development and optimization, particularly in adapting the system to diverse automotive communication environments and in scaling up to accommodate more complex network configurations.

7.4.1 Performance evaluation

As discussed in subsection 7.3.1, EXT-TAURUM P2T introduces a Short Secret Key mode set at run-time in case of need. The following experimental results are focused on determining the throughput overhead trend introduced by CMAC calculation with different key lengths. Figure 7.14a shows the maximum number of CMAC digest computations the system can sustain in dedicating all resources to this activity. At the same time, Figure 7.14b shows the saving in terms of resources changing CMAC digest data length. The figure clearly shows how reducing the CMAC digest from 256 bit to 128bit enables about 40% saving of CPU time that can be used to handle critical overloading situations.



(a) Maximum number of frames to be processed to reach 100% CPU utilization for MAC processing.



(b) CPU utilization trend keeping constant the number of processed frames for different CMAC digest's lengths.

Fig. 7.14 CPU execution time saving in shorter key mode. Source:[4].

Figure 7.15 reports results concerning the speculative MAC calculation, described in subsection 7.3.2. The target reference for this experiment is a periodic task scheduled every 25ms and processing 80 different CAN frames whose CMAC digests must be authenticated. 18 out of the 80 processed frames transmit steady-state information, and their authentication can benefit from speculative MAC calculation.

With speculative MAC disabled, the frame authentication requires around 6% of real-time CPU time in regular running.

By activating speculative MAC calculation on the 18 steady-state frames, in the hypothesis that all speculations are successful, the real-time CPU usage drops down to around 1%, demonstrating the effectiveness of this technique.

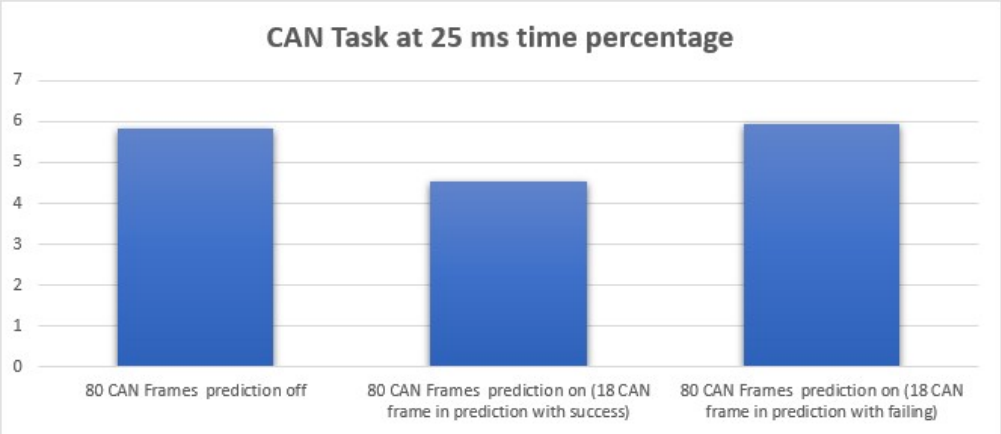


Fig. 7.15 TAURUM P2T Advanced Secure CAN network throughput trend profile based on HMAC used mode Source:[4].

Finally, in the worst-case condition of all speculations failing, a 0.1% real-time CPU usage overhead is introduced, with a negligible impact on the system.

7.4.2 Overhead evaluation

Implementing the EXT-TAURUM P2T communication stack introduces extra code. Comparing the firmware of one of our sample nodes implemented without any security feature with one implementing the EXT-TAURUM P2T communication stack, we measured a 300% code overhead. Nevertheless, in our prototype, all cryptographic operations are software implemented. In real ECUs, the use of Crypto Cores would significantly mitigate this overhead. As described before, at the very first time, the system executes the key provisioning protocol for sharing and exchanging keys to all the ECUs in the network. This process lasts no more than 50 ms for sharing the secret keys between a secure gateway and two secure nodes in our experimental implementation. This time strongly depends on the CAN baud-rate settings. A similar amount of time, less than 50ms, is also needed to update secret keys for each privilege level at the end of each rolling period. Being this a broadcast operation, this time is not influenced by the number of nodes. Time measurements

are all performed on the prototype implementation of the system. Experimental activities also proved the concept's capability on privilege separation.

Eventually, let us discuss the EXT-TAURUM P2T impact on the hardware architecture. Most of the ECUs in actual vehicles are already multi-CAN devices, often with spare channels available. They, therefore, are already able to host two CAN-buses. Thus, the EXT-TAURUM P2T architecture only requires adding the SGTW module and ensuring the Secure CAN cabling. This hardware overhead is mitigated by the lack of the IT secret key management infrastructure, with annexed security weakness described above and impact on management costs.

7.4.3 Security analysis

The proof of the security of the EXT-TAURUM P2T solution holds under the *infeasibility* hypothesis. We assume the use of state-of-the-art secure cryptographic algorithms with proper key lengths.

The keystone of EXT-TAURUM P2T is a mechanism to establish a first shared secret K_{SH}representing a root of trust for all following security mechanisms. EXT-TAURUM P2T exploits state-of-the-art Elliptic curve cryptography (ECC), a public-key cryptography schema suitable for use in environments with limited resources such as mobile devices and smart cards. In particular, EXT-TAURUM P2T exploits Curve25519, an elliptic curve that offers state-of-the-art 128 security bits and is designed for use in the Elliptic Curve Diffie-Hellman (ECDH) key agreement design scheme. This curve is one of the fastest ECC curves and more resistant to the weak number random generator. Curve25519 is built in such a way as to avoid potential attacks on implementation and avoid side-channel attacks and random number generator issues.

After establishing the first shared secret, all communications on the secure CAN network are encrypted using Advanced Encryption Standard (AES), implemented with the state-of-the-art AES256 Cipher with Block Chaining Cipher Block Chaining (CBC) modality. This guarantees confidentiality, integrity, and authentication of all messages transmitted over this channel.

Regarding messages exchanged over the public CAN network, integrity and authenticity are implemented exploiting state-of-the-art CMAC. Confidentiality on this network cannot be introduced since legislation requirements impose plaintext

transmission on this network. MAC exploits secret keys securely shared among parties using the secure CAN network. A rolling counter mechanism is used to avoid reply attacks. The introduction of the privilege level concept, EXT-TAURUM P2T, compartmentalizes the security level (i.e., CMAC key length) implemented on this channel. State-of-the-art AES256 is used at the higher levels, while lower levels can resort to reduced key lengths. Even if reduced key lengths might represent a security threat, implementing the periodic key rolling protocol guarantees a minimal timeframe to mount an attack. The key deprecation protocol ensures a secure approach to react if a secret is compromised.

MitM attacks on the network can be efficiently prevented with the above mechanisms. Moreover, the availability of a secure communication channel enables secure authentication of each hardware module in the CAN network resorting to the protocol provided in Section IV-C. According to this protocol, every ECU connected to the network embeds a secret provided by the carmaker at the plant. The protocol exploits authentication using the nonce to identify trusted modules and resorts to the security of the secure CAN network to accomplish the required exchange of messages.

All previous security mechanisms require state-of-the-art hardware blocks to securely store secret keys and perform cryptographic operations onboard each ECU connected to the CAN network. However, this is a standard requirement in the automotive domain where ECUs are equipped with dedicated Hardware Security Modules. The basic assumption is that these modules are secure against costly physical attacks such as side-channel attacks. Moreover, thanks to the key provisioning protocol introduced by EXT TAURUM-P2T, even if an attacker succeeds in performing a physical attack able to compromise a single vehicle, the effect of the attack will be limited in time to the key rolling period and limited in space to a single vehicle and not to the entire fleet.

To conclude the security analyses, EXT-TAURUM P2T can mitigate DoS attacks even if it cannot altogether remove this threat. Mitigation is introduced by reducing key lengths for cryptographic operations and speculative MAC computation. Both solutions can be exploited to reduce the system's load whenever computation and transmission peaks typical of DoS attacks arise.

7.5 Conclusion

The rapid expansion of electronic-based systems within road vehicles has significantly enhanced functionality and user experience but has concurrently introduced new security vulnerabilities into contemporary automotive designs. The EXT-TAURUM P2T Advanced Secure CAN FD Architecture emerges as a cutting-edge solution to fortify the vehicle's communication infrastructure against these emerging threats. This innovative architecture introduces several novel security features designed to safeguard vehicular communications, including:

- Periodic Secure Key Provisioning Mechanism: Utilizes the architecture's secure channel to periodically update cryptographic keys, thereby enhancing security by preventing key stagnation and reducing the risk of key compromise over time.
- Implementation of Privilege Levels of Security: This feature establishes a layered security approach by delineating between trusted and untrusted zones within the vehicle's network. It effectively segregates sensitive operations and data, minimizing the potential impact of breaches in less secure, untrusted zones.
- Dynamic Reallocation of MAC Computations: This strategy optimizes system performance by offloading MAC computations to background tasks, thereby reducing CPU load for real-time processes. This approach ensures that critical real-time functions are not hampered by security operations, maintaining optimal system responsiveness and reliability.

The features above of the EXT-TAURUM P2T architecture have been rigorously evaluated through a comprehensive experimental setup. The results of these experiments provide empirical evidence supporting the feasibility of the architecture, demonstrating its effectiveness in enhancing vehicular communication security without compromising system performance.

Furthermore, a preliminary cost evaluation concerning the potential industrial application of the EXT-TAURUM P2T architecture reveals its economic viability. The analysis suggests that the proposed security enhancements can be implemented

affordably, making it a practical option for mass production in the automotive industry. This cost-effectiveness, coupled with its demonstrated security and performance benefits, positions the EXT-TAURUM P2T as a promising solution for addressing the complex security challenges faced by modern vehicular systems.

In conclusion, the EXT-TAURUM P2T Advanced Secure CAN FD Architecture represents a significant advancement in automotive security, offering a multi-faceted approach to protect against the evolving landscape of cyber threats. Its strategic integration of advanced security mechanisms ensures robust protection of vehicular communication networks, paving the way for safer and more secure automotive technologies in the future.

Chapter 8

CAN-MM: Introducing an Out-of-Band Multiplexed Message Authentication Code (MAC) to enhance Controller Area Network (CAN) Message Authentication

8.1 CAN-MM Technology

The CAN-MM technology introduces a non-intrusive method for implementing MAC based message authentication and integrity check without reducing the payload capacity and maintaining full backward compatibility with all versions of the CAN standard. This approach is particularly pertinent for CAN 2.0 applications, as the additional payload capacity enables the development of a secure CAN network with a sufficiently large MAC digest size. Moreover, the CAN-MM technique can enhance the response time and performance of MAC digest computation across all CAN versions.

Essentially, the underlying concept of CAN-MM involves utilizing digital modulation techniques (i.e., On-Off Keying (OOK)) to multiplex the transmission of the MAC digest with the original CAN frame payload. The OOK is a simple digital modulation scheme based on Amplitude-Shift Keying (ASK) commonly used in

telecommunication [108, 109]. OOK transmits a logical one by sending a carrier wave signal, while the absence of the carrier wave represents a logical zero.

The MAC information is encoded by switching the carrier wave on and off. A logical zero is transmitted on the bus by generating the original CAN signals, while in the case of a logical one, a wave is added to the standard CAN electric signals (in both CANH and CANL). This wave acts as a carrier. Its amplitude is a configured parameter, with a value of $Vpp = 300mV$ in this study, to ensure sufficient margins when reconstructing the original signal at the receiver's side. An example of the resulting CAN-MM physical signal is shown in Figure 8.1.

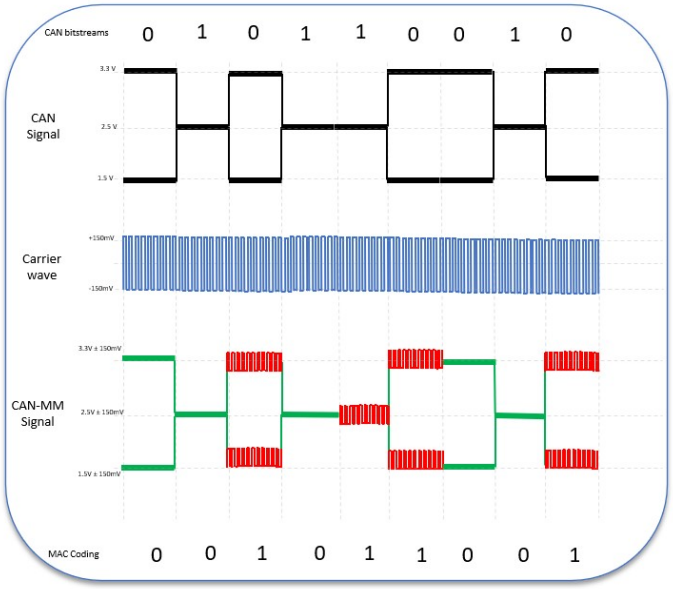


Fig. 8.1 CAN-MM physical signal

To combine the signals from the CAN frame and MAC digest, the CAN-MM system necessitates appropriate synchronization, as depicted in Figure 8.2. The Identifier Extension (IDE) bit of the CAN Control field initiates the synchronization procedure. During this procedure, a synchronization sequence of logic "1" and "0" is introduced on the MAC CODE RX line for the entire duration of the Control field. These values are modulated with the content of the Control field. Subsequently, the MAC digest is modulated onto the data payload. Finally, to enhance the reliability of the system, the CRC of the MAC digest is modulated onto the CRC slot of the payload. The CRC is a specialized checker to detect transmission errors. Multiplexing the MAC digest directly with the message ensures a strong link between

the MAC code and the corresponding message, bolstering security by minimizing vulnerabilities such as message and code separation.

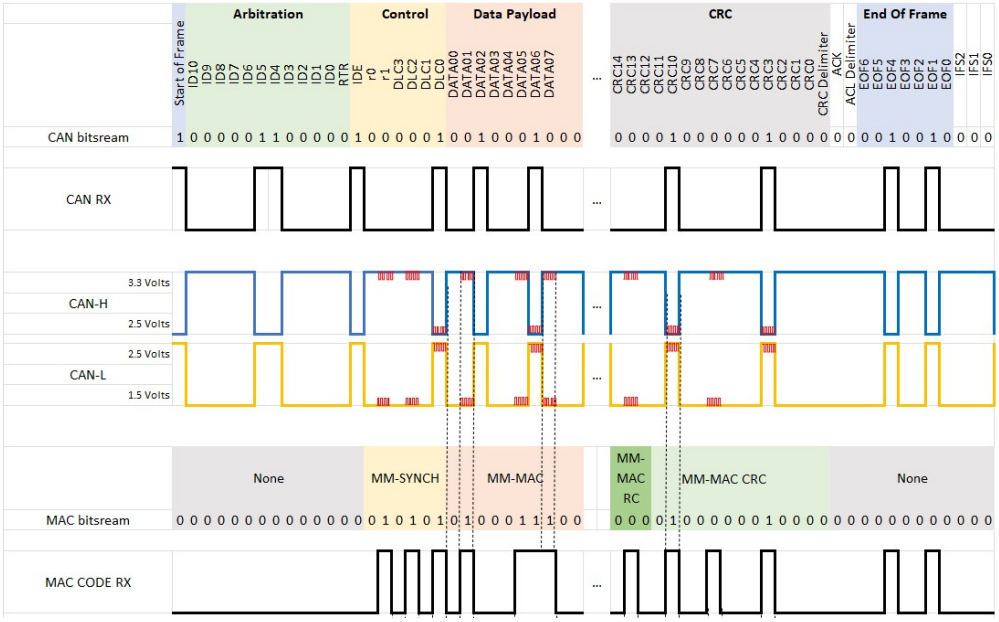


Fig. 8.2 Physical Electrical CAN-MM Scheme

The CAN-MM is not the first concept that proposes an authentication method using an out-of-band channel in the CANnetwork. Most proposed solutions are based on the CAN+ concept [110], including CANauth, LCAP[111, 112]. However, the CAN+ concept overlooks crucial aspects like EMC and disturbance handling, adversely affecting all derived solutions.

Moreover, the fundamental idea of CAN+ is to enhance throughput by exploiting the "grey zone" during the synchronization and arbitration procedures. These procedures, however, differ in the latest versions of CAN, namely CAN FD and CAN XL. This difference suggests that the CAN+ concept may not practically apply to these newer versions.

By the way, CANAuth [12] is a protocol that closely adheres to CAN specifications, tailoring its security features to suit the CAN bus environment. One of its key characteristics is that it is not designed for source authentication. Instead, authentication is tied to message IDs. Given that messages can originate from various sources, this approach makes it challenging to trace the origins of messages. This is in line with CAN's message-oriented communication structure. However,

a significant concern arises from the extensive range of CAN IDs - in the order of hundreds (11 bits) or even millions (29 bits for extended frames). The practicality of storing a unique key for each possible ID is questionable, as reported by B. Groza et al [113].

Figure 8.3 shows the comparison between the CAN FD frame structure and the CAN 2.0 frame with CAN-MM. It is evident from the figure that the CAN 2.0 frame with CAN-MM is shorter than the CAN FD while retaining the same amount of information. This reduction in frame size helps optimize the system's real-time performance and the CAN bus load of the entire vehicle network.

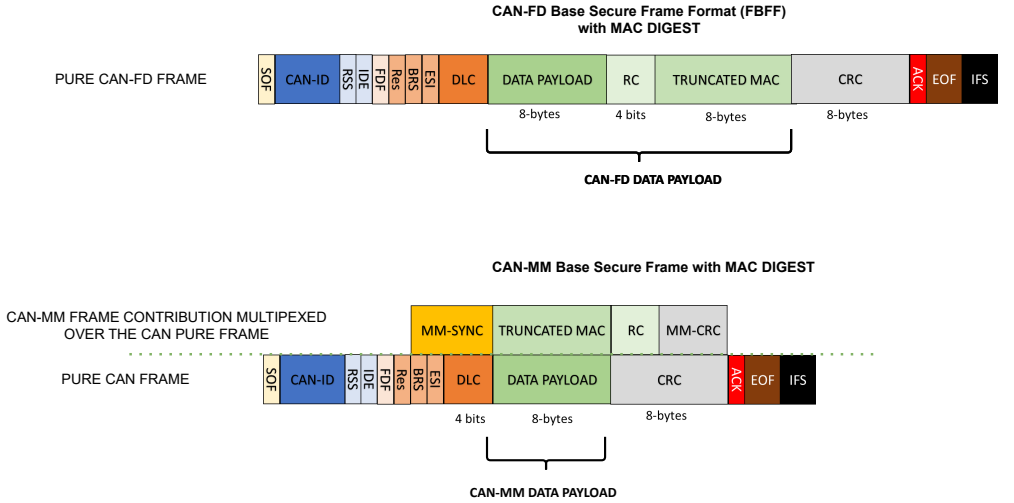


Fig. 8.3 Secure CAN-FD frame vs CAN 2.0 frame with CAN-MM

The CAN-MM architecture consists of two main blocks: a transmitter and a receiver module. The following sections describe those modules.

8.1.1 CAN-MM transmitter

Figure 8.4 presents the architecture of the CAN-MM transmitter. The blue block represents the standard CAN transmitter, while the green block includes the additional functional components required to implement the CAN-MM schema. The custom CAN-MM components are situated downstream of the standard CAN interface to ensure full electrical compatibility with existing CAN interfaces.

A multiplexer block is employed to multiplex the MAC-related information. This block includes a diverter switch [114] with two inputs, namely a carrier supplied by an internal generator and ground. The modulated CAN signal is applied to both CANH and CANL. The multiplexer is controlled by the MAC bitstream to provide a carrier as output when the corresponding MAC bit is one and no contribution when the corresponding bit of the MAC is zero. The multiplexer control line is synchronized with the CAN controller to multiplex the MAC information with the CAN payload.

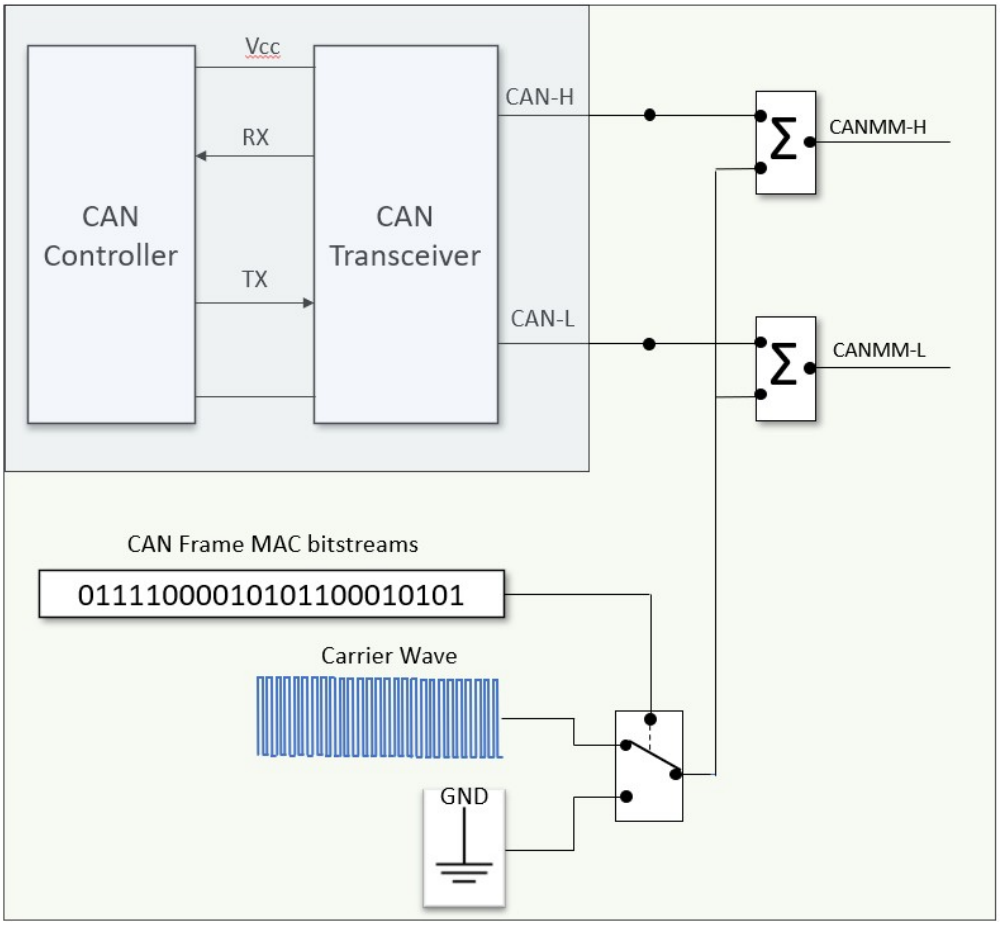


Fig. 8.4 CAN-MM Transmitter block scheme

8.1.2 CAN-MM receiver

Figure 8.5 depicts the architecture of the CAN-MM receiver. The standard CAN-MM receiver architecture is represented by the blue block in Figure 8.5, while the custom blocks added for the CAN-MM architecture are shown in green. The CAN-MM receiver includes a decoder block that is responsible for extracting the multiplexed MAC bit-stream sequence from the payload of the CAN frame. This decoder block utilizes a hybrid analog-digital electronic network to extract the correct CAN-MM contributions encapsulated in the CAN physical signal. As shown in Figure 8.5, the standard CAN receiver and the MAC decoder operate in parallel. While the transceiver processes the CAN frame, the decoder operates to reconstruct the MAC bit-stream. This allows the MPU to receive the CAN data payload and its MAC code in a shorter time window compared to existing solutions [92].

8.1.3 CAN-MM decoder

The CAN-MM decoder, shown in Figure 8.6, is the most complex block of the CAN-MM architecture. Its primary responsibility is extracting the MAC information multiplexed with the original CAN frame. The decoder is composed of four stages, which are as follows:

- *Filtering*: This stage is replicated for both CANH and CANL. It includes a band-pass filter with a center frequency *fc* at the frequency of the carrier signal.
- *Comparing*: This stage is a threshold comparator that operates on both CANH and CANL to identify the specific area where the carrier signal is present.
- *Conjunction*: This stage combines the analog data from both CAN lines into a single digital signal stream.
- *Counter*: The final stage is a logical network that identifies the area of the carrier signal in the digital domain.

These stages work together in a highly coordinated fashion to accurately extract the modulated information from the CAN channel.

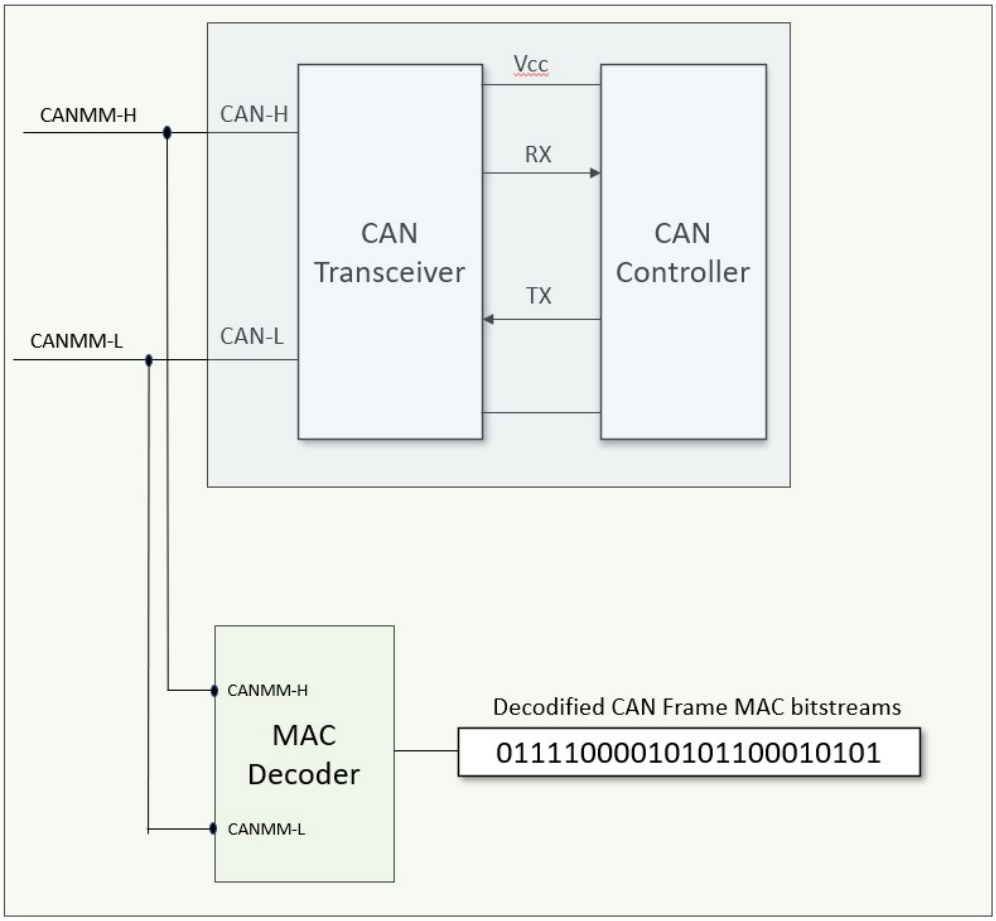


Fig. 8.5 CAN-MM Receiver block scheme

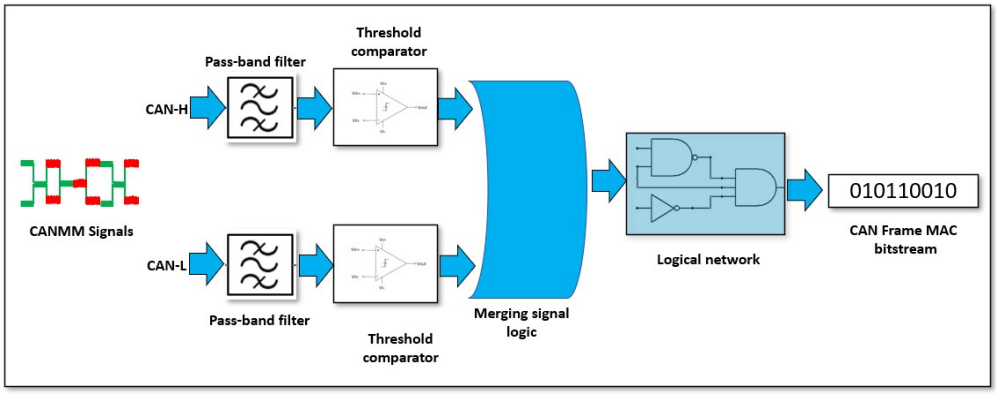


Fig. 8.6 CAN-MM MAC decoder Type-A block scheme

8.2 Validation Model

8.2.1 Experimental setup

The validation of the CAN-MM architecture considers a typical application scenario, specifically, a standard automotive CAN 2.0 network operating at a speed of 500kbps. A hybrid automotive CAN network comprising three CAN nodes was designed and simulated using the LTSpice [115] simulation environment to validate the architecture. Two nodes were CAN-MM transceivers, one serving as a transmitter and the other as a receiver. The third node was a standard CAN version 2.0 receiver. This setup enabled the validation and verification of the CAN-MM functionality and its backward compatibility with standard CAN transceivers. The complete block diagram for this configuration is presented in Figure 8.7.

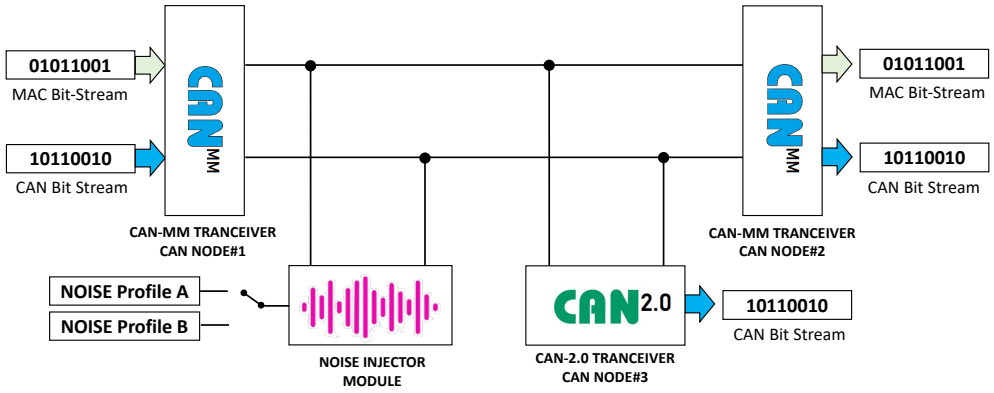


Fig. 8.7 Block scheme of the CAN-MM validation setup

8.2.2 Noise and interference analysis

CAN systems boast a robust immunity to ground noise and electromagnetic interference, thanks to differentially transmitted information, independent ground reference, usage of twisted-pair cabling, and balanced differential transceivers.

Since the CAN-MM technology is modifying the original profile of the CAN signals, evaluating it under realistic noisy environments is crucial. A validation environment simulated standard vehicle noise to assess noise and interference effects on CAN-MM technology. The noise profile is acquired using a multi-protocol

vehicle interface device connected to an actual vehicle's OBD port. The device, programmed to transmit a specific CAN frame to the ECM, captures the physical CAN signal via an oscilloscope. Direct access to the CAN bus input of the ECU is facilitated through a break-out box. The noise profile is obtained during engine idle, aligned with specifications from various research papers [116–118]. Noise signals, recorded from both CAN lines with the same phase, cover frequencies from 10kHz to 10MHz, with amplitudes between -100mV and 100mV. Signal-to-Noise Ratio (SNR) calculations involve computations on two identical carrier signals with a peak-to-peak amplitude of 300mV. The SNR for this scenario was calculated to be approximately 14.31 dB (Figure 8.8). This value provides insight into the signal's quality relative to the background noise with the current parameters.

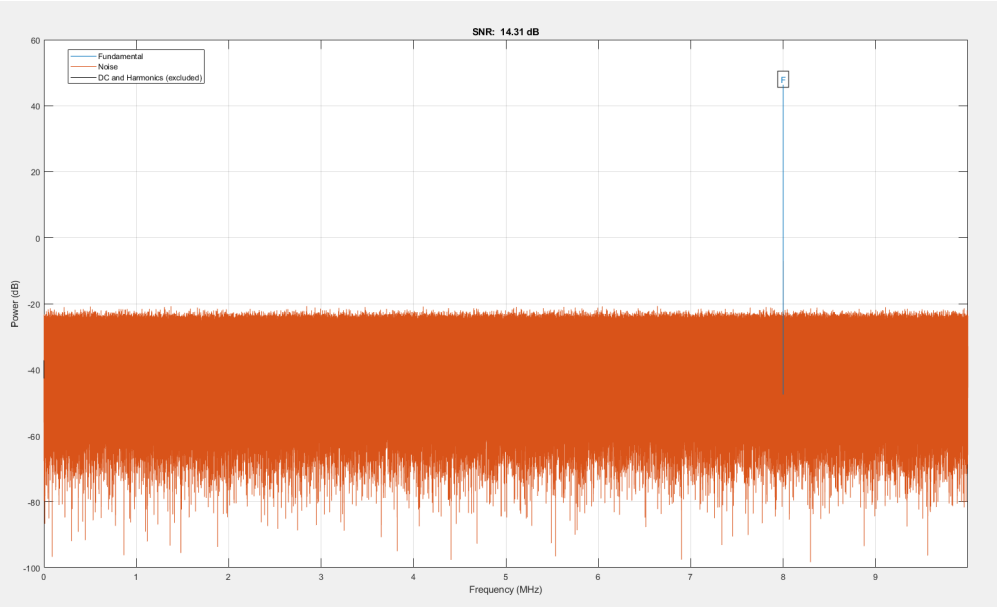


Fig. 8.8 SNR graph for real CAN recorded signals

8.2.3 SPICE Model

The SPICE simulation incorporates input signals, such as the CAN bitstream and its associated MAC, generated from Piecewise Linear (PWL) files. Supplementary signals, including noise profiles, follow the same method with their respective PWL files. Standard library parts provided by the tool are utilized for the remaining design components.

In this setup, the LTC2875 standard CAN transceiver (refer to Figure 8.9) is employed, as depicted in Figure 8.7. The CAN-MM added part features a High Voltage Latch-Up Proof and a Single pole double throw (SPDT) Switch. Depending on the control value, this block outputs either the carrier wave or zero, subsequently added to the CANH and CANL signals provided by LTC2875, along with the noise contributions (see Figure 8.10).

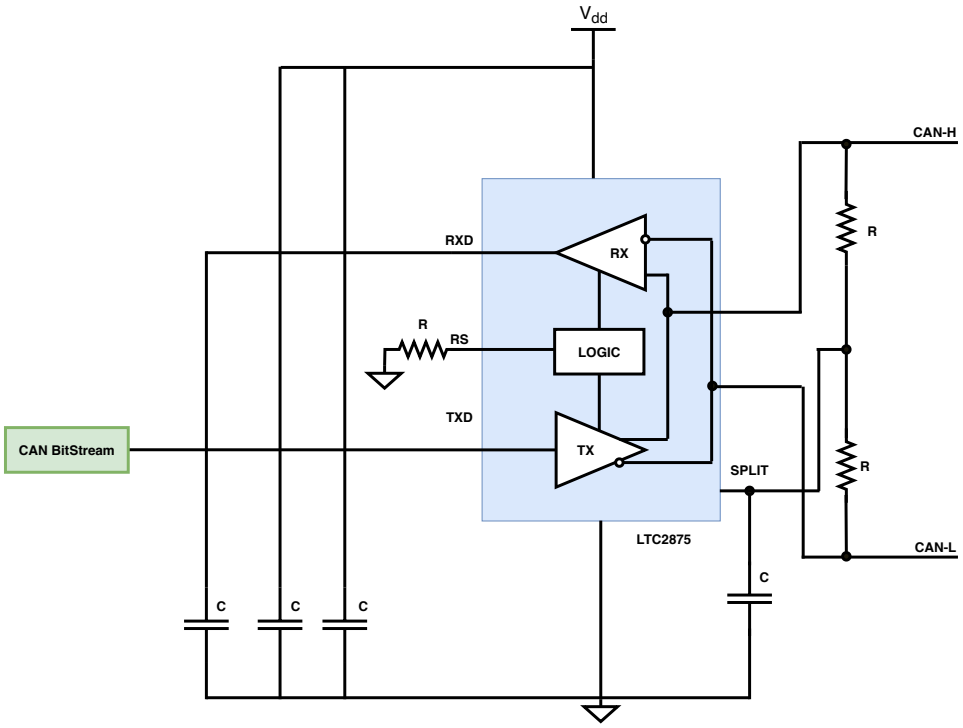


Fig. 8.9 CAN-MM Transceiver - Stage 1 - SPICE Block

Unlike the transmitter, the custom part of the CAN-MM receiver processes data in parallel to the standard transceiver (refer to Figure 8.11). The receiver includes a pass-band analog filter with a cutoff frequency set to the carrier frequency, followed by a voltage comparator with a voltage reference set to the absolute value of the noise (in this case, 100 mV). These stages form the first decode chain for CAN-MM and are identical for both CAN lines (see Figure 8.11).

In the second stage of the CAN-MM receiver, the contribution on the two CAN lines is collapsed together through a `NOR` port. Downstream of the `NOR` port is a custom logical network based on flip-flop counters, which is used to extract the MAC contribution (refer to Figure 8.12).

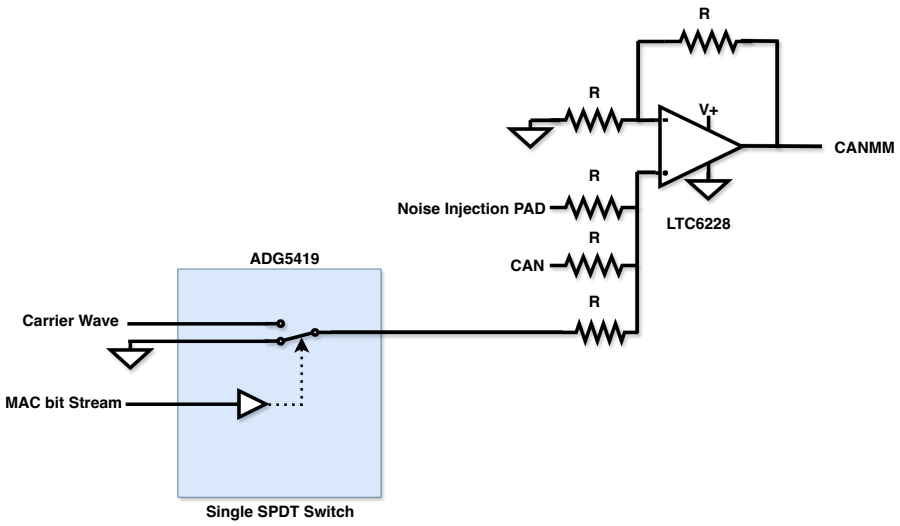


Fig. 8.10 CAN-MM Transceiver - Stage 2 - SPICE Block

8.2.4 Preliminary Hardware Implementation

A hardware prototype was created to enhance the validation of the CAN-MM technology. The prototype is specifically designed to assess the functionality of the CAN-MM transmitter. It is implemented within a compact In-Loop CAN network, as illustrated in Figure 8.13. The primary goal of this validation is to confirm the capability of a standard receiver to receive the CAN-MM conditioned signal accurately.

The experimental setup involves a laptop connected to a Neo VI Multi-Protocol Vehicle Interface, which oversees a custom hardware board designed for CAN-MM operation. This board is crucial for converting the incoming CAN signal, received through the Neo VI interface, into a CAN-MM frame. The conversion process is directed by control signals continuously managed by the Neo VI device. Additionally, the hardware board is linked to another Neo VI device via the CAN-MM bus, set up to function under the standard CAN protocol. This configuration creates a closed loop with the laptop, facilitating seamless communication.

Notably, the CAN-MM bus is deliberately designed to be open-access, enabling the intentional introduction of noise and permitting data acquisition with an oscilloscope. In the second stage of the loop-back scheme, a programmable noise source

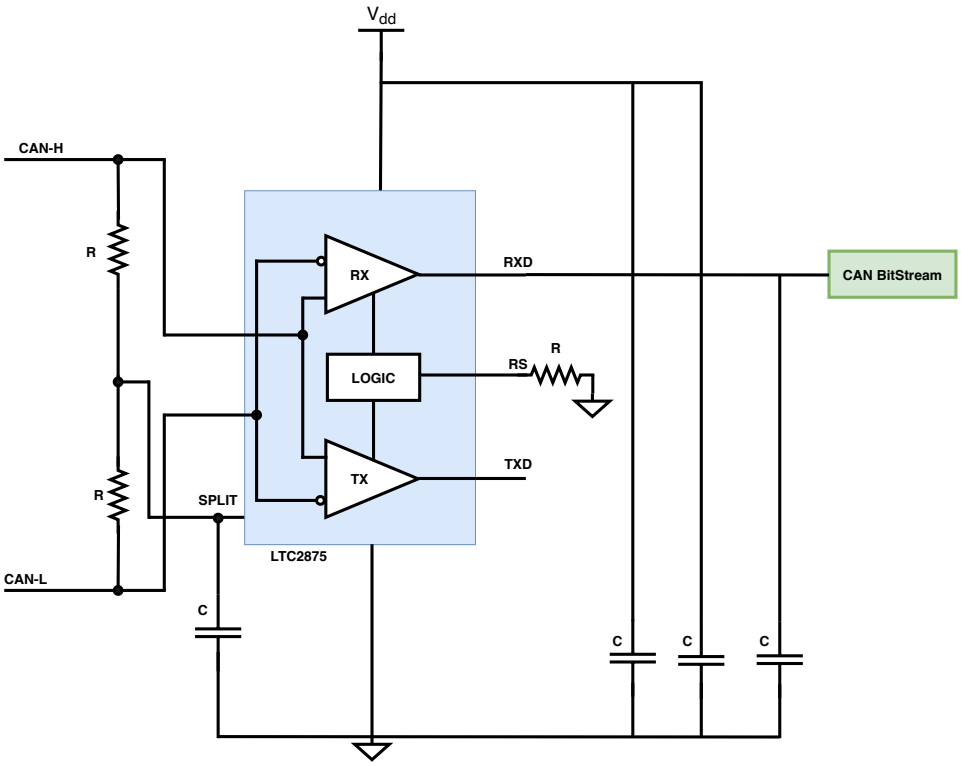


Fig. 8.11 CAN-MM Receiver - Stage 1 - SPICE Block

was also added to simulate the noise profile acquired during the idle operation of the engine, as previously used in the LT-Spice simulations.

8.3 Experimental results

The collected signal diagrams, illustrated in the following figures, show the electrical signals generated by each module depicted in Figure 8.7. The output signals generated by CAN-MM node #1 are illustrated in Figure 8.14, which depicts four subplots. The blue line in the first subplot illustrates a section of a transmitted CAN bitstream, while the second one displays the differential electrical signals. The third subplot shows the CAN-MM electrical signals that are transmitted on CANH and CANL, where MAC signal in the fourth subplot is multiplexed.

Figure 8.15 depicts the functionality of the CAN-MM receiver in node #2. It shows how the receiver manages the physical signal generated by the CAN-MM

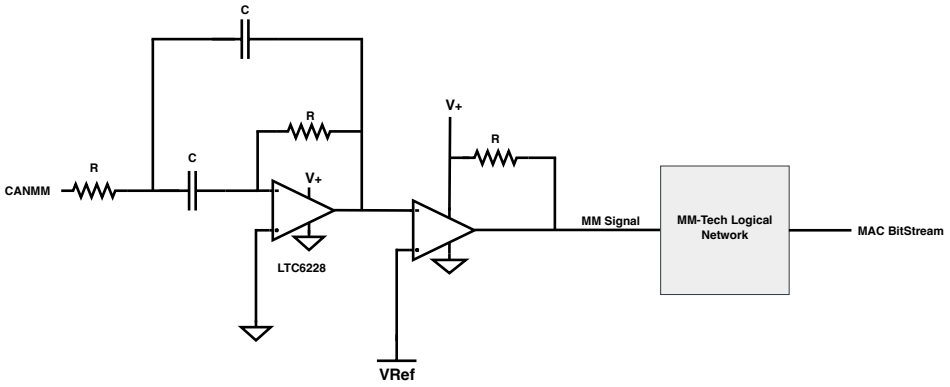


Fig. 8.12 CAN-MM Receiver - Stage 2 - SPICE Block

transmitter and transmitted on the bus. The bottom subplot displays the received CAN-MM physical signal through the CAN-MM transceiver, which is identical to the signal transmitted by node #1 in Figure 8.14. The subplot in blue colour is the MAC bitstream extrapolated by the CAN-MM decoder in node #2, and it is the corresponding MAC of the subplot in red colour.

To demonstrate the complete compatibility of CAN-MM with the standard CAN 2.0 protocol, node #3 simulates a standard CAN 2.0 transceiver. As shown in Figure 8.16, the backward compatibility is guaranteed, as the transceiver can reconstruct the correct CAN bitstream when it receives a CAN frame modulated under CAN-MM specifications. However, a standard CAN transceiver lacks the extended hardware required to demodulate the MAC bitstream, making it impossible to extract it.

To support a timewise analysis of the CAN-MM to understand the potential benefits of the parallel transmission of the MAC alongside the data payload, we computed the MAC transmission Extra Time (MET), introduced by the transmission of the MAC digest. It depends on the MAC's length in bits ($MACsize$) and the selected CAN protocol transmission time of a data bit (τ_{dbit} [76]), as shown in equation Equation 8.1.

$$MET = MACsize * \tau_{\text{dbit}} \tag{8.1}$$

Aligning with the experimental setup in [76], we computed MET using τ_{dbit}=0.00025 (ms) for the CAN FD and τ_{dbit} equal to 0.0001 (ms) for the CAN XL.

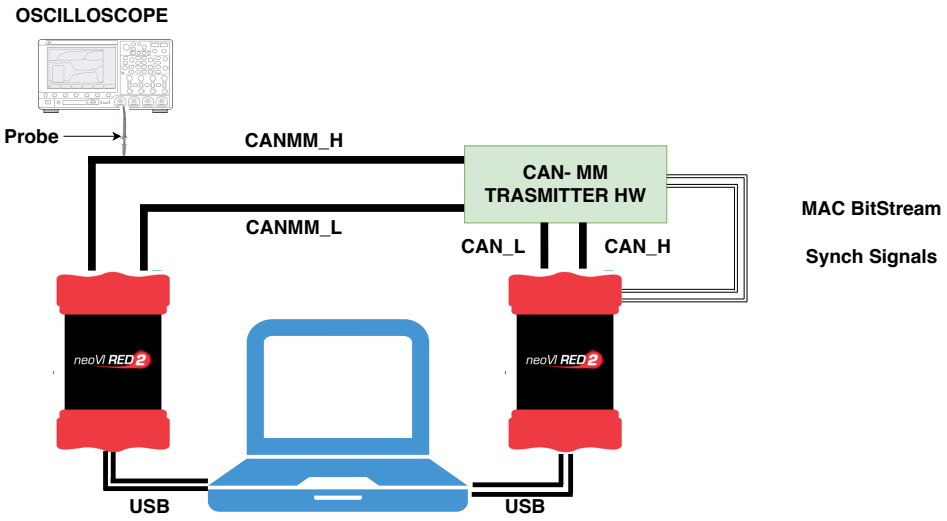


Fig. 8.13 CAN-MM Hardware Concept Scheme

In a CAN FD the MET required to transmit the 64-bit MAC digest is 16 µs, as per equation Equation 8.2

$$MET = MACsize * \tau_{\text{dbit}} = 64 * 0.00025 = 16(\mu s) \tag{8.2}$$

Adopting a more traditional baud rate on CAN FD, 500kbps, we calculate a $\tau_{\text{dbit}} = 0.002(ms)$. In this condition, the extra transmission time required by MAC appended to the payload is 128 µs (see Equation 8.3).

$$MET = MACsize * \tau_{\text{dbit}} = 64 * 0.002 = 128(\mu s) \tag{8.3}$$

Keeping the MAC's size constant, adopting the CAN XL protocol with a speed rate of 10Mbps, the MET would be reduced to 6.4 µs, which represents the best possible transmission performance by Secure Onboard Communication (SecOC) and CAN secure (CANsec), as per equation Equation 8.4, demonstrating that a broad adoption fo CAN XL would introduce faster performance.

$$MET = MACsize * \tau_{\text{dbit}} = 64 * 0.0001 = 6.4(\mu s) \tag{8.4}$$

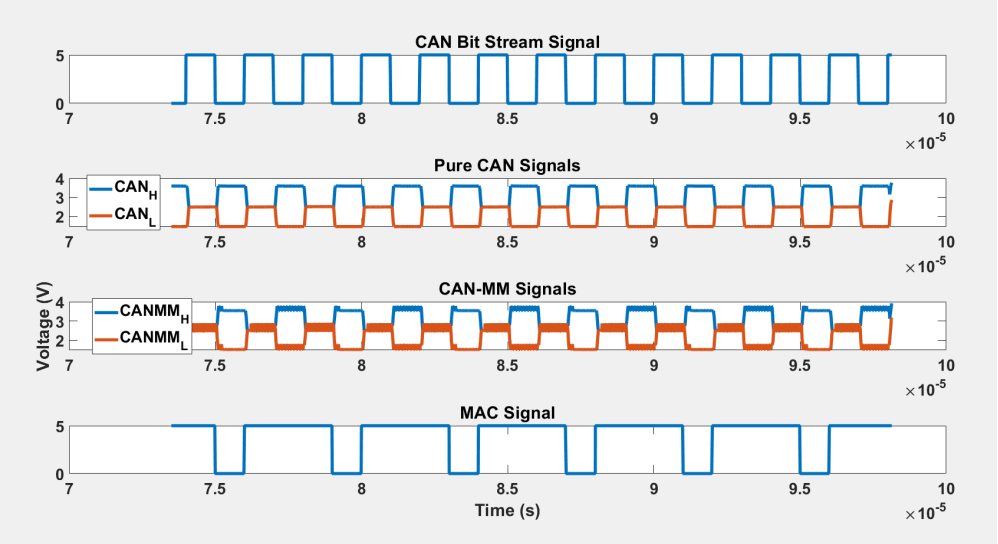


Fig. 8.14 CAN-MM transmitter output

Opting for CAN-MM instead highlights a key benefit: the negligible impact on transmission times due to MAC. This capability to maintain consistent transmission times, with or without MAC, offers a solution to the schedulability challenges discussed by Ikumapayi et al.[76].

Moreover, CAN-MM supports countermeasures on the schedulability noted by the authors of [77]. The systems described in the paper adopt Rate-monotonic scheduling (RMS), a deterministic scheduling algorithm for real-time operating systems that assign priorities to tasks based on their period; the shorter the period, the higher the priority. A pivotal aspect of RMS is its CPU utilization bound for n periodic tasks, which can be calculated using the Liu & Layland formula, Equation 8.5, where C_i is the computation time of task i, T_i is the period of task i, and U is the total CPU utilization. This formula ensures that if the total CPU utilization is below a certain threshold, all tasks can be scheduled to meet their deadlines, making RMS particularly efficient for systems with hard real-time constraints.

$$U = \sum_{i=1}^{n} \frac{C_i}{T_i} \leq n(2^{\frac{1}{n}} - 1) \tag{8.5}$$

The transmission time of the CAN and the MAC might significantly contribute to C_i, the computational load. By reducing the transmission time, CAN-MM directly

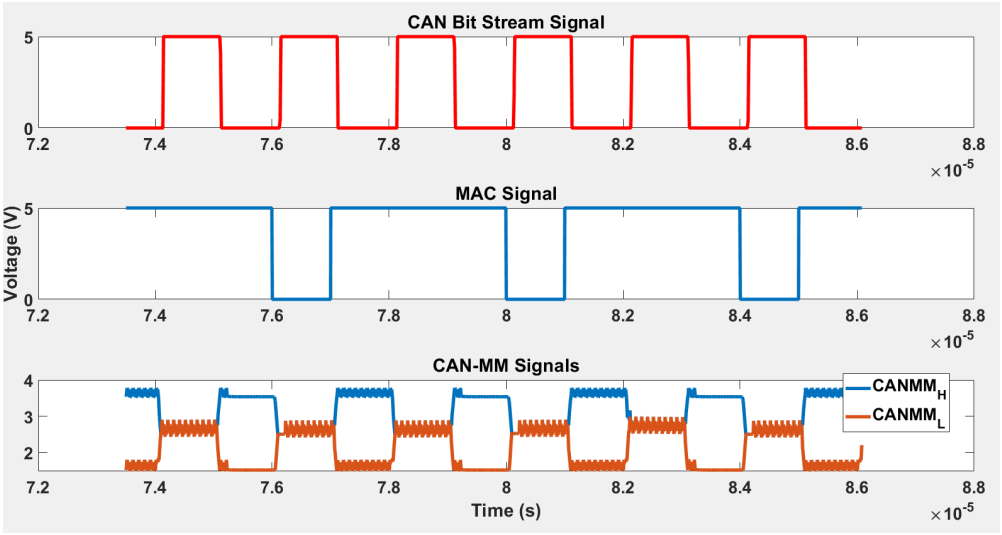


Fig. 8.15 CAN-MM receiver signals

decreases C_i and, consequently, the total CPU utilization. This reduction is crucial for enhancing resilience against certain types of attacks.

To provide a general understanding, the HSM performance metrics published by Pott [119] indicate that more than 300 clock cycles are required for MAC verification. When considering latency, the total time is approximately 5-6 µs, which parallels the time savings achieved by CAN-MM compared to CAN XL. Consequently, this denotes that CAN-MM might theoretically offer a twofold increase in the system's ability to withstand such attacks, in contrast to the conventional CAN XL framework where the MAC is appended to the payload.

The robustness of CAN-MM was further validated through measures performed on the hardware implementation introduced in subsection 8.2.4. These results complement the ones produced by the LT-SPICE simulations. The captured data in Figure 8.17 portrays the real-time CAN-MM-H bus traffic. The applied noise profile follows what has been captured from a vehicle as described in subsection 8.2.2. Within this experimental framework, the CAN-MM transmitter effectively performs the multiplexing of the MAC Bitstream, precisely the bit sequence `0000111010111110111`, over the underlying physical CAN-H signal. This multiplexing process is executed through the OOK modulation technique, closely replicating the observations obtained in the simulated environment, thus confirming the robustness of the CAN-MM system.

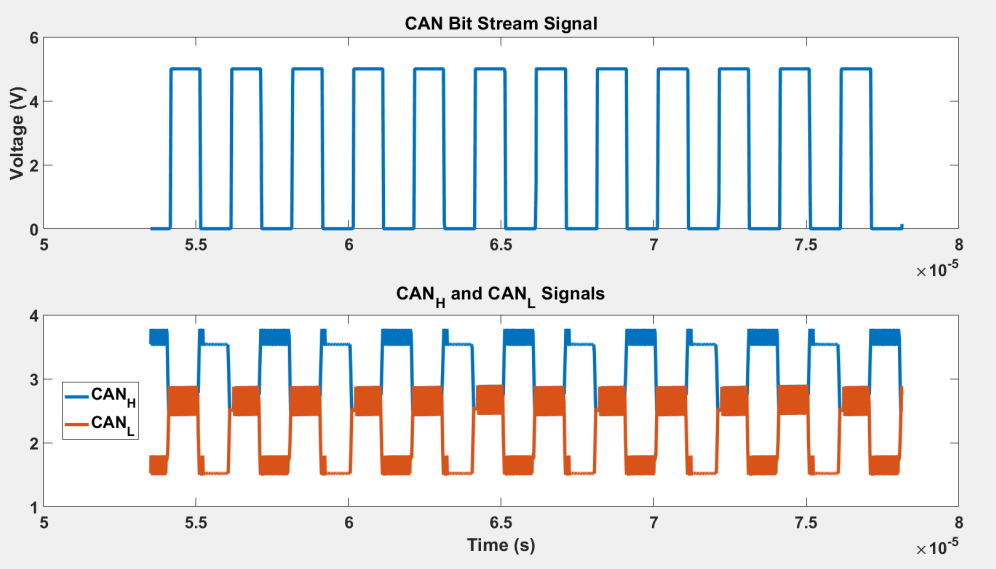


Fig. 8.16 CAN 2.0 transceiver

Moreover, the BUSMASTER [120] tool reported error-free reception of the transmitted CAN message. This confirms the backward compatibility of the CAN-MM approach with conventional hardware. The multiplexed carrier of the standard transceiver is intelligently filtered out, effectively treating it as noise in the system.

8.4 CAN-MM Type-B

section 8.3 highlights a potential limitation in the CAN-MM architecture when the carrier and noise frequencies align, manifesting sporadic failures in demodulating the MAC bit-stream. While this scenario is unlikely to occur in actual situations, considering that noise amplitudes exceeding 100mV are seldom encountered, this paper introduces an advanced CAN-MM architecture called Type-B, able to withstand scenarios where the carrier signal frequency matches the noise. CAN-MM Type-B ensures additional robustness to noise across all frequency bands without risking data corruption.

The CAN-MM Type-B physical signals scheme incorporates Carrier Phase Shift Modulation (CPSM) [121] as depicted in Figure 8.18. The CPSM carrier varies between CANH and CANL, causing a phase shift ranging from 90° to 270°. The proposed design sets the phase modulation to 90° for CANL as depicted in Figure 8.21.

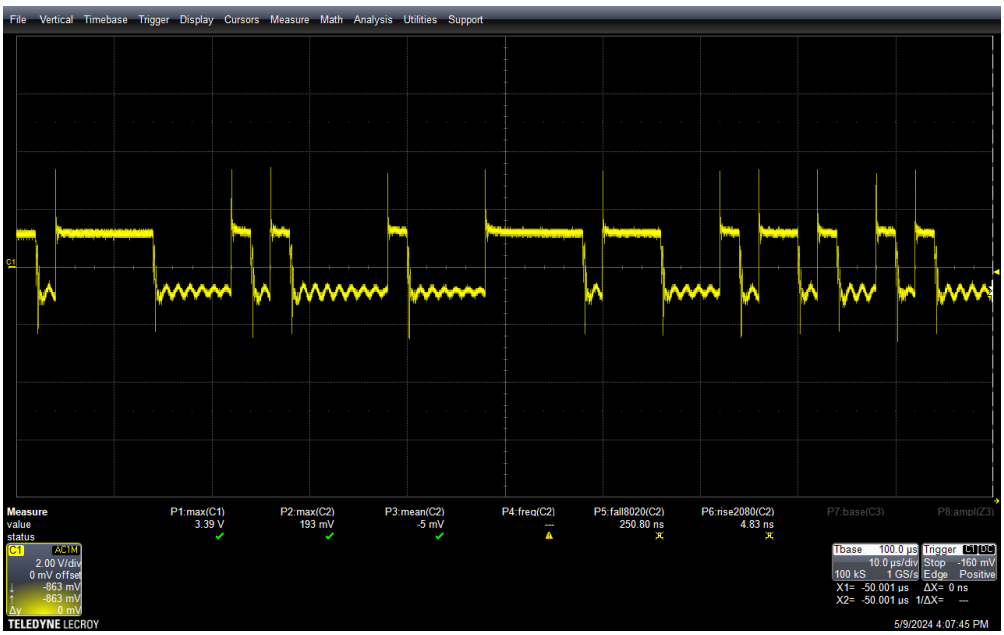


Fig. 8.17 CAN-MM-H acquired by Oscilloscope

The additional phase-shifting can result in incorrect codification, particularly if the differential voltage in the red area depicted in Figure 8.20 exceeds the 0.5V threshold. To overcome this limitation, an additional re-phaser stage represented by the orange area in the receiver reported in Figure 8.19 reverses the CPSM applied by the CAN-MM Type-B transmitter. This block is placed at the very beginning of the reception process. Once the re-phasing is completed, the standard CAN-MM receiver, which includes the standard CAN transceiver and the CAN-MM decoder, work in parallel to extract their respective data from the re-phased frame.

The additional protection to noise of CAN-MM Type-B across all frequency ranges comes with the cost of adding an upstream hardware re-phaser block to the CAN transceiver when it functions as a receiver.

An LT-Spice model was developed to validate the robustness of the CAN-MM Type-B architecture (Figure 8.21). MAC code 1 is encoded by adding a carrier with a shifting phase on CANL, allowing for greater robustness during decoding activities. However, in certain regions, the phase shifting can cause the differential voltage between these signals to exceed the 0.5V limit. Thus, as shown in Figure 8.22, the signal is shifted back before decoding, obtaining full synchronization.

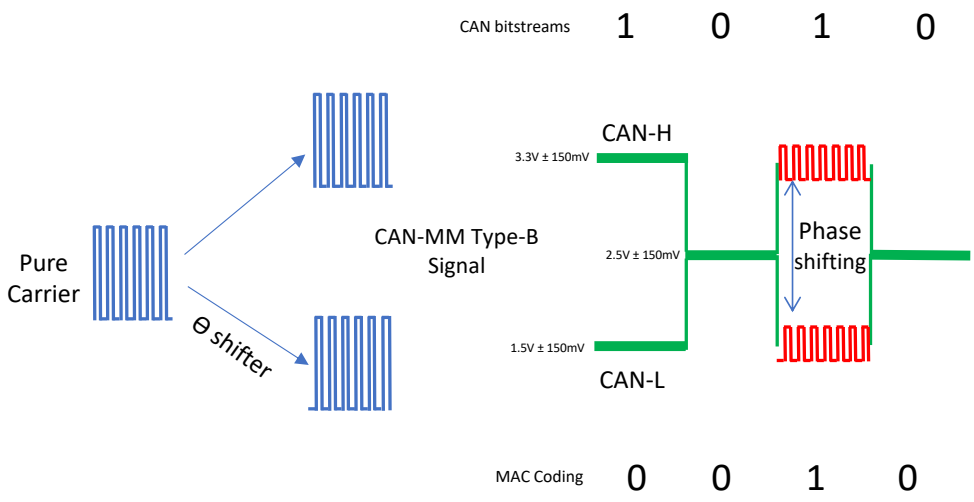


Fig. 8.18 CAN-MM Type-B physical signals scheme

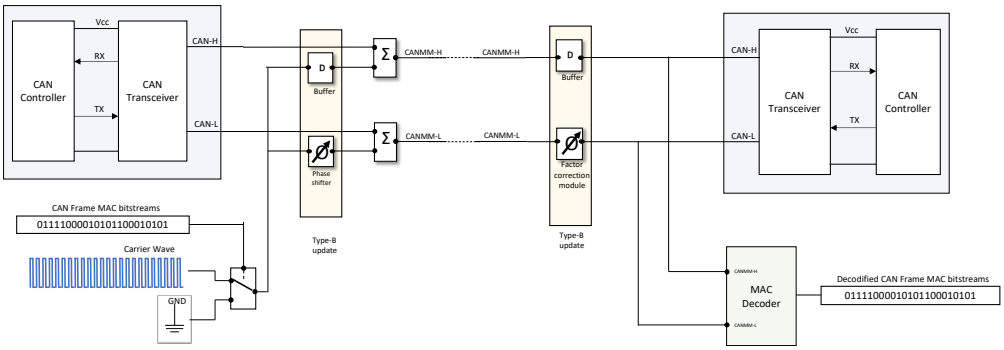


Fig. 8.19 CAN-MM Type-B Transmitter& Receiver Block scheme

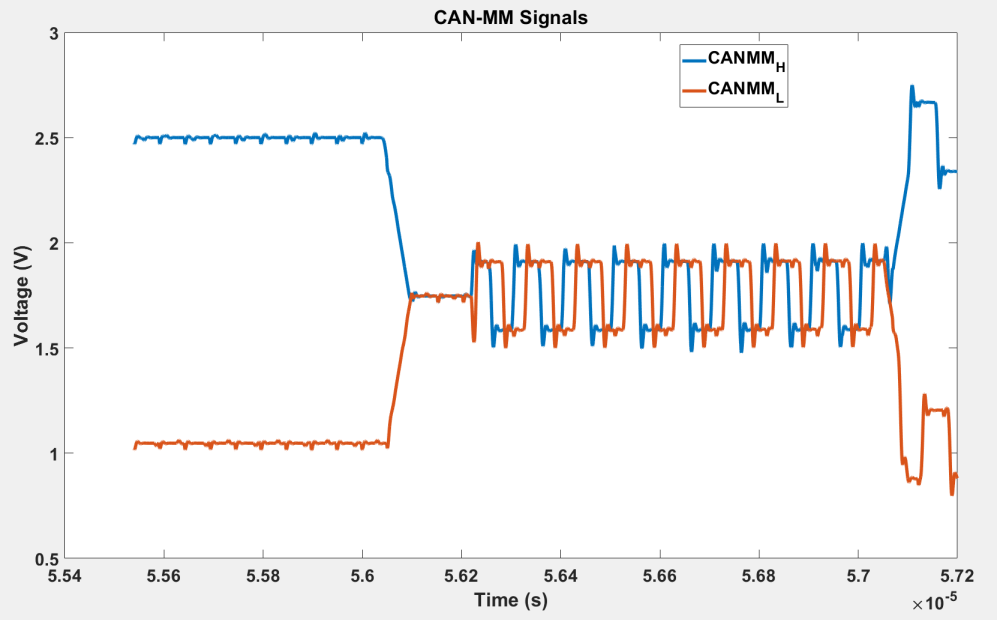


Fig. 8.21 CAN-MM Type-B Physical Signal with the shifted carrier on CAN-L

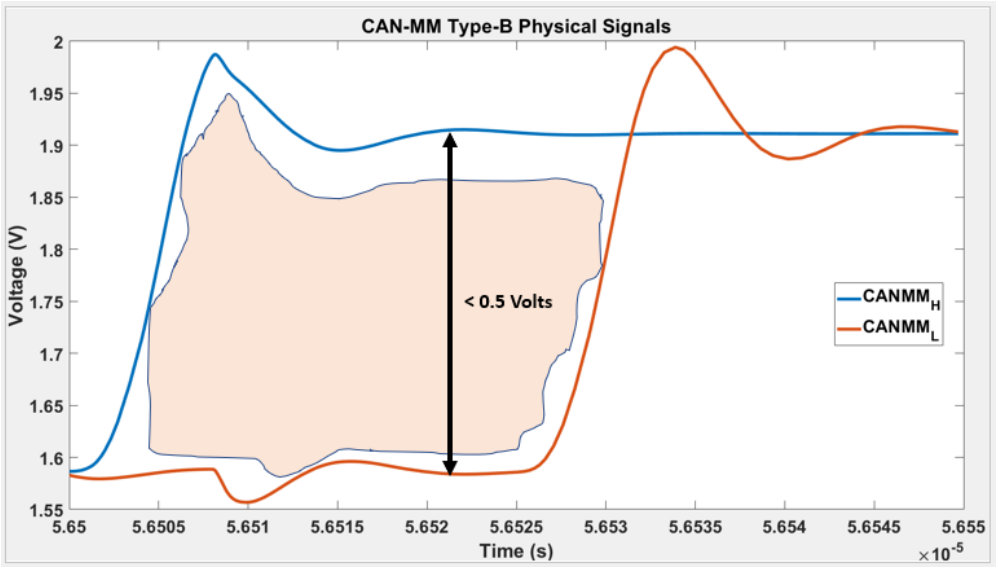


Fig. 8.20 Critical Area due to shifting phase for codification correctness

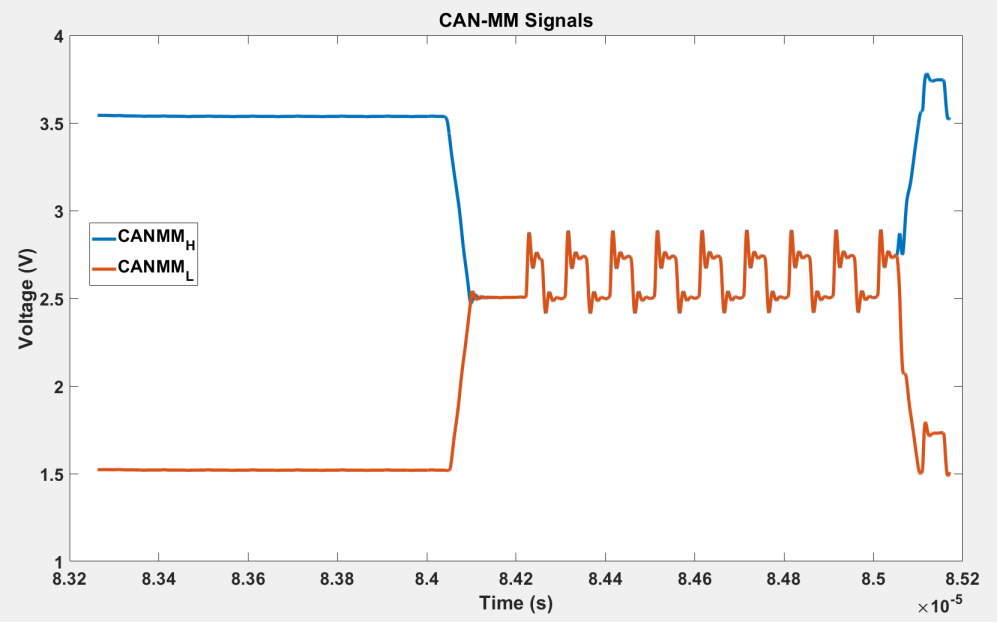


Fig. 8.22 CAN-MM Type-B filter scheme

Figure 8.23 presents a comparative comparison between CAN-MM and CAN-MM Type-B to validate the design robustness. This experiment applies a noise signal with a 140mV amplitude to the original CAN-MM architecture model. The investigation

is completed only for completeness since the resulting signal is clearly out of specification. As a result of the high noise level, the receiver could not extract the correct MAC bit-stream, and the output was a MAC bit-stream stuck to 1. However, in the case of CAN-MM Type-B, despite a noise signal with an amplitude of 200mV, the receiver correctly decoded the MAC stream.

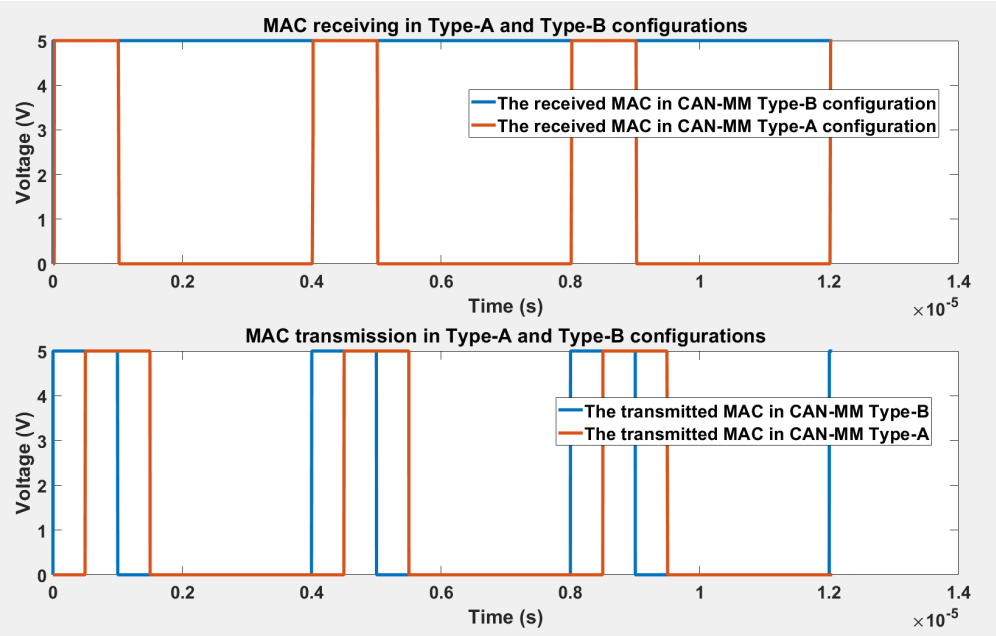


Fig. 8.23 CAN-MM Type-A vs. CAN-MM Type-B Noise capability performances

By referring to Figure 8.24, we have calculated the signal-to-noise ratio (SNR) for this scenario to be approximately 17.32 dB. This high SNR value underscores the signal's robustness, affirming its clear distinction from the surrounding background noise.

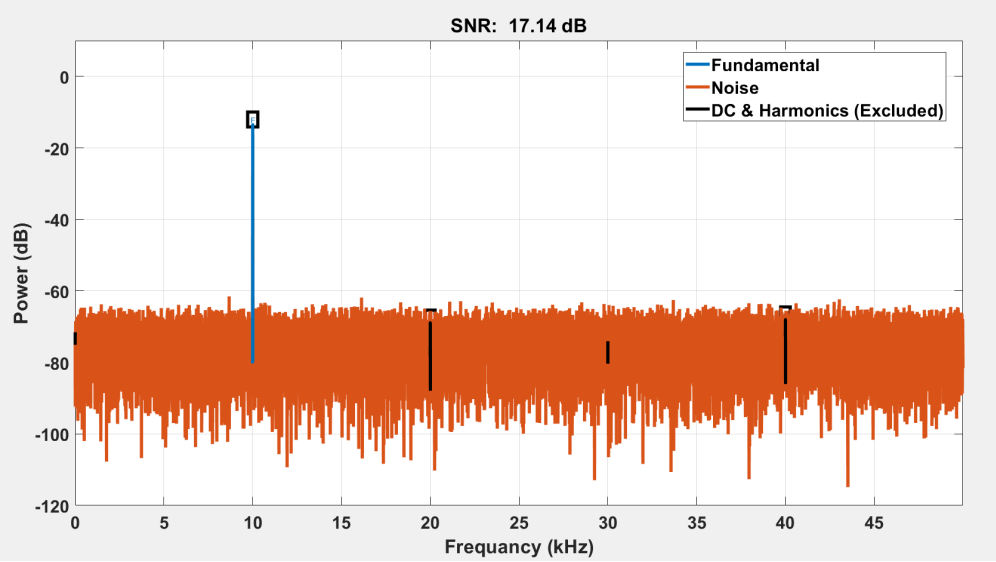


Fig. 8.24 SNR CAN-MM TypeB Graph

8.5 Security Analysis

This section delves into the security aspects of the CAN-MM architecture, particularly addressing attack models outlined in section 5.8.

The main objective of CAN-MM is to support a full CAN 2.0 vehicle network security by embedding a SecOC compatible MAC code within each payload frame, matching the same level of protection of CAN FD. Moreover, it supports security against threats such as MitM and replay attacks due to the presence of the MAC mechanism that neutralizes those types of attacks. This capability also includes the more recent Janus attack, as described by the author [74].

CAN-MM may also neutralize Cloak attacks by maintaining payload integrity, even amidst bit modifications. Leveraging the sample rate of two receivers will be more complex if the attacker also must coherently switch the modulated MAC. Such complexity will narrow the timing window where the attack is effective, as discussed in the original paper [75].

When a significant challenge arises when the system is overwhelmed by an excessive number of MACs that need to be validated [77], the validation process demands intensive cryptographic computations, potentially compromising the system's ability

to adhere to real-time deadlines. This issue becomes particularly acute with the influx of numerous fraudulent MACs. The CAN-MM system introduces enhanced security measures against those kinds of attacks.

8.6 Conclusion

This paper presented an efficient solution to mitigate security concerns within the automotive domain's fundamental communication protocol, the CAN. The proposed solution, CAN-MM, facilitates the transmission of MAC payloads in standard CAN to complement any security schemas based on it efficiently. The support of the MAC transmission also safeguards the automotive communication system against MitM and replay attacks.

The CAN-MM architecture, developed to upgrade communication hardware for upcoming security regulations, maintains compatibility with existing CAN devices, avoiding the necessity for a complete system or vehicle architecture overhaul. This hybrid networking capability offers flexibility to designers, minimizing the requirement for updating electronic components to the new generation and thereby reducing the cost of transitioning a vehicle fleet into the cyber-secure domain.

Additionally, an improved Type-B version of CAN-MM addresses potential demodulation issues without sacrificing backward compatibility. While this modified version may compromise some degree of backward compatibility, the applied modulation technology to the CAN protocol can be extended not only to version 2.0 but also to other existing versions that already incorporate the MAC.

Chapter 9

LIN-MM: Introducing an Out-of-Band Multiplexed Message Authentication Code (MAC) to Ensure Message Authentication in Local Interconnect Network Communications (LIN)

9.1 Introduction

This paper unveils a pioneering technique dubbed LIN Multiplexed MAC (LIN-MM), which ingeniously amalgamates a data digest of a LIN payload into the payload, ensuring the integration is seamless. This digest, a composite of a MAC and Message Integrity Code (MIC) as highlighted in previous research [122], serves to fortify the transmitted LIN data frames against integrity and authenticity breaches. Ingeniously crafted, LIN-MM eschews alterations to the original LIN data frame architecture, thereby guaranteeing its full backward compatibility with the conventional protocol. This approach not only preserves the integrity of the data but also streamlines the validation process of the digest by concurrently multiplexing data and their corresponding authentication codes, which significantly abbreviates the processing

duration, enhancing overall efficiency and security in data transmission within LIN networks.

9.2 LIN attack vector analysis

ECUs act as masters in a LIN network, while sensors and actuators are usually slave devices. Every LIN transaction follows the same schema. The master sends a header that includes a PID identifying a task carried out by a slave node (e.g., ask a sensor to report the measured physical quantity or command an actuator to set itself to a new target position).

LIN slaves are the primary attack vector against LIN networks due to their high vulnerability exposure. The literature reports four possible primary attacks able to compromise the security of the LIN bus [123–125].

In the *message spoofing attack*, the attacker sniffs the bus traffic to identify the proper time slot to inject a spoofed message directed to a victim node. Spoofed messages can be used to sleep a slave node, alter the SYNC field to tamper with synchronization, or inject illegitimate messages. In general, this attack aims to destroy bus communication. Technical ability is not required to mount this attack. The attacker can exploit the dominant and recessive electrical states to cause frame corruption and Denial of Service (DoS).

Similar to the spoofing attack, the *MitM* exploits an external malicious module to dissect a portion of the LIN bus. The malicious module can disconnect a victim node and a part of the LIN bus. Therefore, the attacker can hijack LIN frames from and to the disconnected LIN branch (Figure 9.1).

The *response collision attacks* happens when an illegitimate response message is transmitted together with a legitimate frame. According to the specifications, if a node detects a collision, it asserts an error bit and stops transmitting, waiting for the next transmission slot. A collision is detected when, during transmission, the electrical level observed on the bus is not coherent with the transmitted logical level. Checking the electrical level of the bus during transmission is possible thanks to the electrical implementation of the LIN transceiver (Figure 9.2).

The attacker can either send a false header playing as a master node or wait for the legitimate master frame and manipulate the message [124]. The goal is to trigger

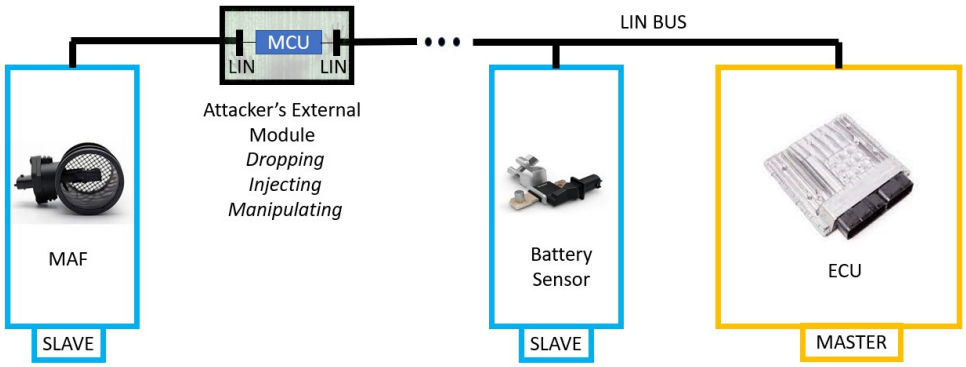


Fig. 9.1 LINMitM Attack Scheme. Source:[5].

an unexpected response colliding with the legitimate one. The legitimate slave node drops the transmission while the attacker can send an illegitimate response frame to the master node. The master node considers the attacker's message legit when the checksum code is correct.

The *header collision attack* is similar to the response collision attack, but the attack vector is now a master header frame instead of a slave response frame. The attacker injects an illegitimate header on the LIN bus to provoke collision with an allowed header. Again, in case of collision, the master stops transmitting, and the attacker can inject a malicious frame that can redirect a request to a different slave. In this way, the attacker can tamper with the sequence of responses of the LIN network and even isolate a victim node. This attack can slide down a vehicle's windows, lock or unlock the car, or lock steering wheels while vehicles are travelling along the road.

The main difficulty of injecting an incorrect response on the LIN network lies in exploiting physical access to the LIN bus. Direct access through external modules, as shown in Figure 9.1 provides complete control of the bus. However, it is possible to gain partial LIN access through the CAN network. Usually, the master LIN nodes are connected to the CAN bus [126]. An attacker can reach the LINbus through the CAN On-Board Diagnostic (OBD) port mounted in a vehicle cabin, using recent hacking techniques [127, 128].

To avoid the response and header collision attacks, Takahashi et al. [124] suggest that a slave node sends out an abnormal signal, which would overwrite a false message sent by an attacker if it detects that the bus value does not match its

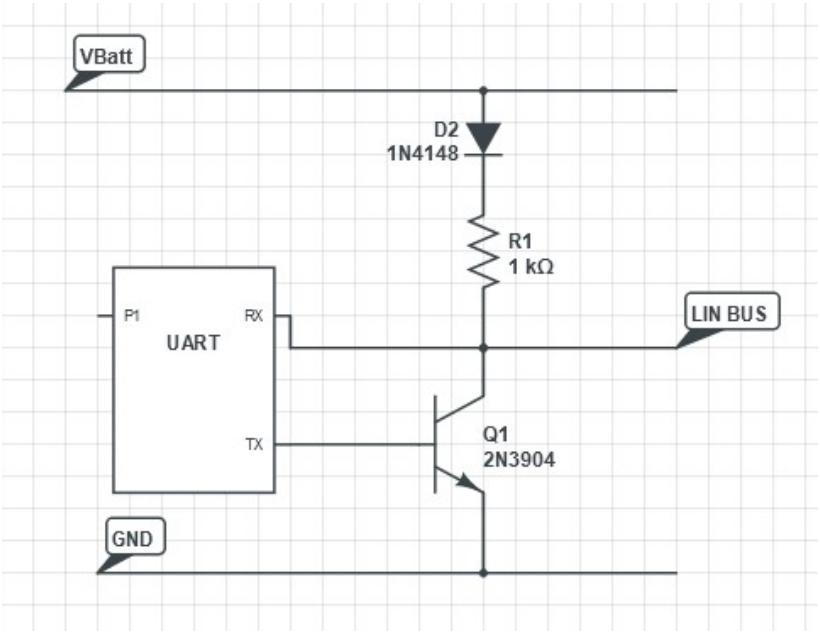


Fig. 9.2 LINTransceiver Scheme. Source:[5].

response. The solution is limited because the slave communicates when the master releases the appropriate time slot, so the countermeasure is not immediate. Additional suggestions include incorporating MAC and assigning essential data to the first byte of transmission, as the first byte is more difficult to corrupt. The main limitation is that the MAC code erodes the frame data payload. The LIN protocol has a maximum data payload of 8 bytes. By NIST's guidelines [68], a robust MAC code cannot be less than 64 bits, which is precisely the entire LIN payload length. The current mitigation is to reduce the MAC digest to 4 bytes providing protection that does not meet the automotive security standards.
To the best of our knowledge, the LIN attacks described above are all possible LIN exploits that literature reports in automotive research.

9.3 LIN-MM

Multiplexed Message Authentication Code for Local Interconnect Network (LIN-MM) is a new solution to introduce message authentication code compliant with NIST's guidelines [68] in a standard LIN network without reducing the LIN payload size. LIN-MM is not intrusive and ensures full back compatibility with standard

LIN devices. Moreover, LIN-MM eliminates the MAC transmission latency by transmitting it concurrently with the data payload. To the best of our knowledge, this is the first study on security applied to LIN networks.

LIN-MM applies signal modulation to multiplex the MAC bitstream with the electrical signal of the LIN frame (Figure 9.3). In particular, LIN-MM exploits On-Off Keying (OOK) [108], one of the most straightforward digital modulation schemes, to transform the MAC bitstream into an electrical signal. OOK uses a carrier signal; it turns the carrier "On" when transmitting a logic '1' and turns it "Off" when transmitting a logic '0'. The modulated carrier is added to the original LIN electrical signal to multiplex the MAC bitstream with the LIN bitstream. The full 8-byte payload of a LIN response is available to implement advanced features using LIN-MM.

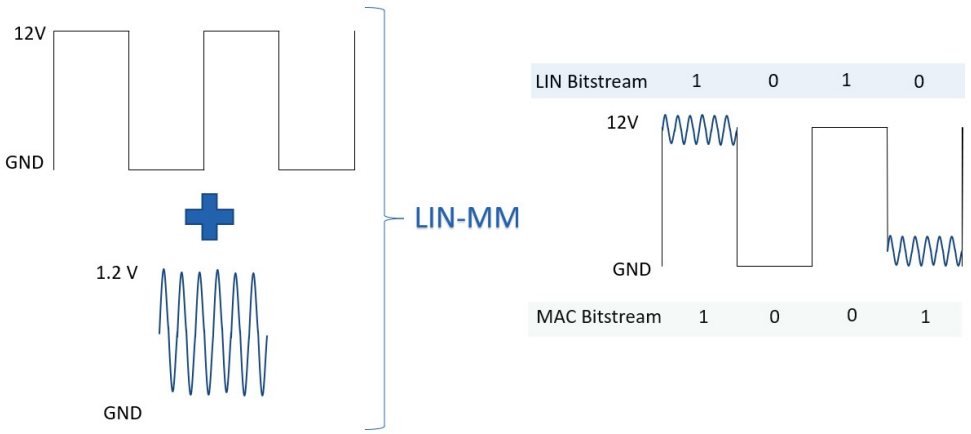


Fig. 9.3 LIN-MM Physical Electrical Signal. Source:[5].

In its current implementation, LIN-MM is limited to the slave responses. The 8-byte payload of a slave response is enough to carry the information of a 64-bit MAC code compliant with NIST recommendations. Even if the same technique can be applied to the master header frames, the limited length only allows multiplexing short and less secure codes.

9.3.1 LIN-MM Slave Architecture

As illustrated in Figure 9.4, the LIN-MM Slave pairs a standard LINtransceiver with a custom LIN-MM carrier generator. This component generates a modulated carrier

signal based on the MAC bitstream. The original LINsignal and the carrier signal are added to create the LIN-MM electrical signal.

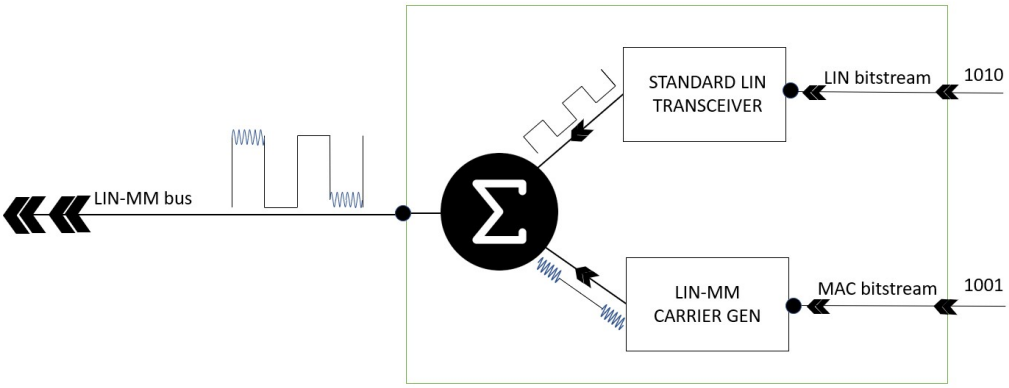


Fig. 9.4 LIN-MM Slave Block-Scheme in trasmission. Source:[5].

The LIN-MM carrier generator is composed of a multiplexer accepting two inputs: the carrier provided by a dedicated signal generator and GND (Figure 9.5). The MAC bitstream controls the multiplexer commutation. It switches the multiplexer to the carrier signal when the corresponding MAC bit is '1'; it changes to GND otherwise. The standard LIN transceiver and the LIN-MM carrier generator are synchronized properly to multiplex the two signals.

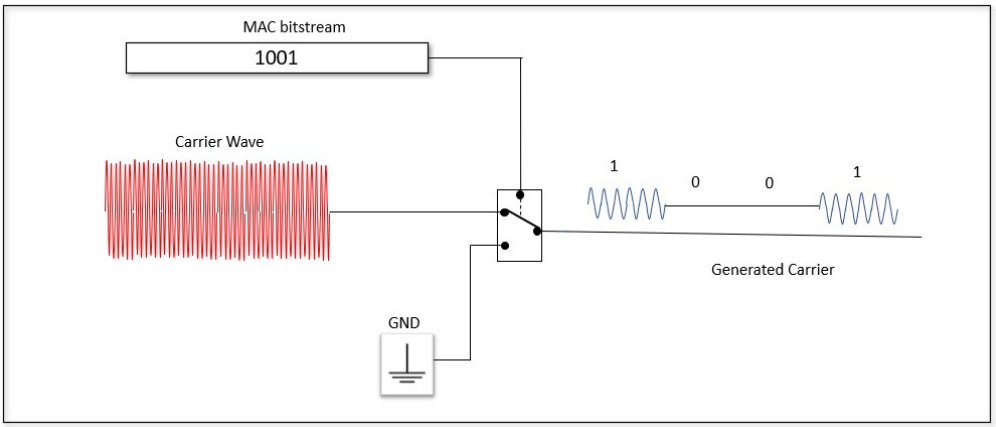


Fig. 9.5 LIN-MM Carrier Generator Block-Scheme

The carrier frequency (f_c) must be selected to enable its isolation from the LIN signal through filtering, even in case of noise. The proposed implementation exploits

a 100 kHz sinusoidal signal that can be easily separated from the 20 kbit/s LIN signal. The carrier frequency is synchronous with the pure LIN signal, and both share the same sample time windows. Considering $V_{batt} = 12V$, the carrier amplitude is set to 1.2V to keep the generated signal within the LIN electrical specifications (section 9.3).

9.3.2 LIN-MM Master

Figure 9.6 shows the architecture of the LIN-MM Master composed of two main blocks: a standard LIN transceiver and a demodulation block. The standard LIN transceiver processes the LIN-MM signal. The MAC multiplexed signal is noise canceled by the internal transceiver filters. The demodulation block is introduced to demodulate and reconstruct the MAC bitstream from the physically received signal.

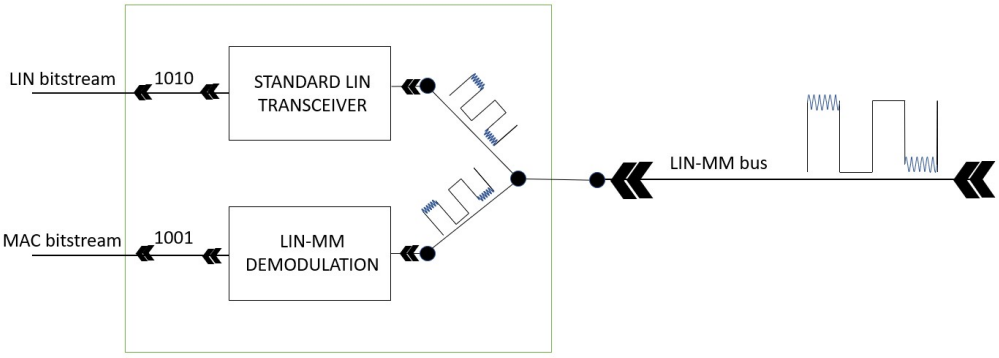


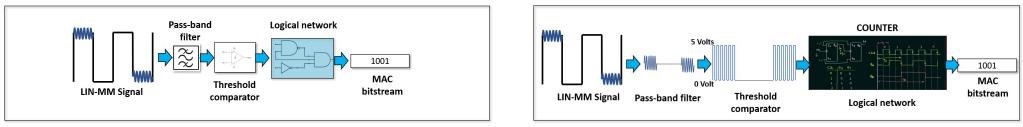
Fig. 9.6 LIN-MM Master Block-Scheme in receiving. Source:[5].

The LIN-MM demodulation block comprises three subsystems (Figure 9.7a). Figure 9.7 shows the effect of these subsystems on the processed signal.

A pass-band filter with a center frequency f_c at the carrier's frequency isolates the carrier's contribution from the rest of the signal. With $f_c = 100kHz$ the filter is designed with a bandwidth $BW = 50kHz$ corresponding to a low-pass frequency $f_l = 75kHz$ and a high-pass frequency $f_h = 125kHz$.

A threshold comparator transforms the analog sinusoidal carrier into a signal in the digital domain with a bit transmission rate equal to the carrier frequency.

Finally, a digital network reconstructs the MAC bitstream. It acts as a digital counter synchronized with the LIN bit signal. The counter is reset at the beginning of each LIN period (i.e., LINbit transmission period) and counts the number of digital pulses generated by the comparator. At the end of the LINperiod, a MAC logic '0' is reconstructed if the counter detected less than three pulses, a logic '1' otherwise. This approach allows for reliable MAC bitstream reconstruction, with a robust resilience to noise that may generate spurious spikes. With this schema, the MAC bitstream can be reconstructed with a delay of a single LIN period.



(a) LIN-MM Demodulation Block pipeline (b) LIN-MM Demodulation Block Signal Profile

Fig. 9.7 LIN-MM Demodulation Block Scheme. Source:[5].

9.4 Experimental results

An LTSpice [115] prototype implementation of a LIN-MM architecture composed of a Master and a Slave node was implemented to prove the feasibility of the proposed schema and therefore validate and verify the LIN-MM functionality. Figure 9.8 shows a high-level block scheme of the prototype architecture. The master node sends a LIN header frame to the slave node that replies with a LIN response message. The response message encapsulates a 64-bit MAC digest for authenticating the transmitted data. The system works with a 19.2k bit/s baud rate. The entire architecture is implemented with a standard LIN transceiver.

9.4.1 Functional validation

Figure 9.9 provides a functional validation of the proposed architecture showing the LIN-MM Response Frame, produced by the LIN slave node (Figure 9.8). The first signal (red) shows the physical, electrical signal on the LIN bus. The second signal (blue) shows the MAC bitstream encapsulated in the LIN-MM signal.

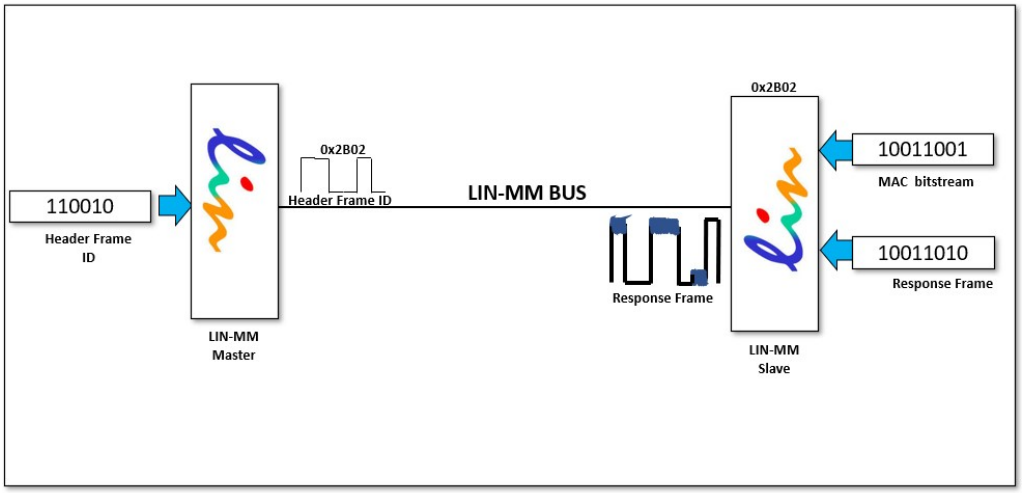


Fig. 9.8 LIN-MM Spice Model Block Scheme. Source:[5].

As expected, the LIN-MM physical signal shows the presence of the carrier in correspondence to MAC bits at logic '1'. In contrast, no carrier is present in correspondence of MAC bits at logic '0'.

Figure 9.10 shows the MAC bitstream propagation time. The blue signal is the MAC bitstream generated by the LIN-MM slave, while the red line is the MAC bitstream reconstructed by the LIN-MM Master. The MAC bitstream propagation latency time is 52us, limited to one LIN period sample.

9.4.2 Overhead evaluation

To deploy LIN-MM, it necessitates the integration of an extra plug-in module into all nodes that necessitate secure LIN communication. When comparing the conventional LIN transceiver hardware to that of LIN-MM, there's an anticipated cost increase of about 2% per unit. This estimate is derived from the baseline cost of a standard LIN transceiver, factoring in the expenses associated with the supplementary discrete components needed for the LIN-MM's modulation and demodulation functionalities. Such a cost increment is deemed acceptable, especially when the only other alternative for achieving a similar level of security involves switching to the CAN protocol, which would entail significantly higher expenses. Within the LIN-MM framework, the master node is tailored solely for demodulation, whereas the slave nodes are equipped with modulation capabilities. Although specific data on power

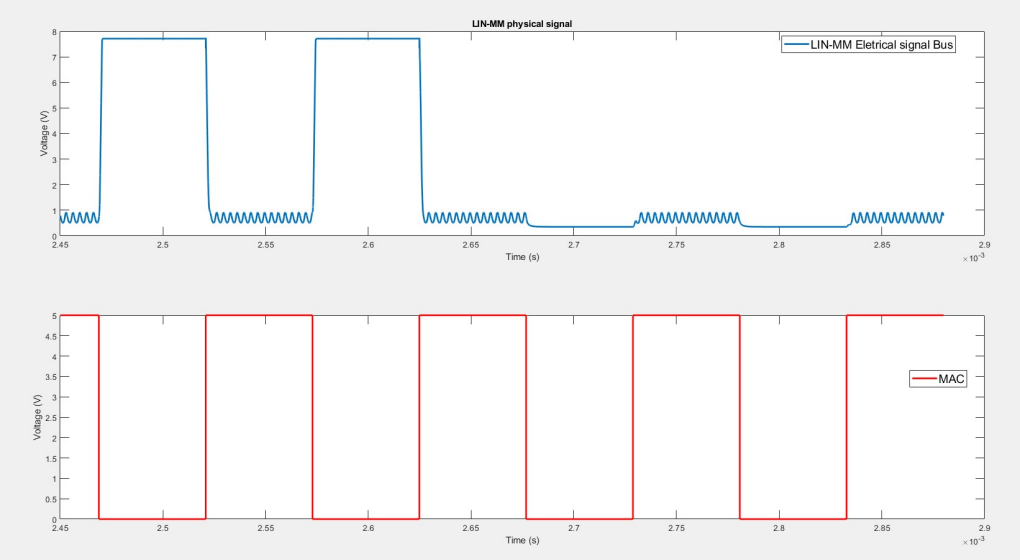


Fig. 9.9 LIN-MM Response Frame. Source:[5].

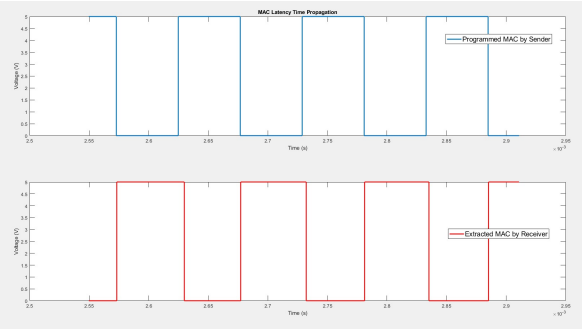


Fig. 9.10 MAC bitstream time propagation. Source:[5].

consumption are absent, the additional power requirement is considered minimal due to the utilization of a few low-power components for the modulator and demodulator construction.

The LIN-MM receiver is capable of capturing the entire MAC bit stream merely 50 microseconds post-receiving the LIN payload, demonstrating exceptionally brief latency periods. This represents a notable enhancement in performance over the current, less secure methods that incorporate a 32-bit MAC code within the payload, which typically experience latency times around 190 milliseconds.

Furthermore, the influence of LIN-MM on hardware and vehicular architecture is significant. LIN-MM is fully compatible with existing hardware and supports

operation within a hybrid network. This flexibility allows for the strategic upgrading of critical asset nodes to LIN-MM while maintaining non-critical nodes on the conventional hardware setup.

In summary, the empirical evidence corroborates the anticipated outcomes. The LIN-MM paradigm successfully introduces the direct multiplexing of the MAC code at the LIN physical signal layer. This accomplishment is pivotal in affirming the enhanced security level that LIN-MM offers over the traditional LIN network.

9.4.3 Security analysis

The keystone of LIN-MM is a mechanism to multiplex at the electrical level a MAC digest with a standard LINsignal.

The proof of the security of the LIN-MM solution holds under the infeasibility hypothesis. We assume the use of state-of-the-art secure cryptographic algorithms with proper key lengths.

Employing a state-of-the-art automotive hardware control module, LIN-MM can be implemented to work with a state-of-the-art Cipher-based Message Authentication Code (CMAC) based on the Advanced Encryption Standard 128-bit Cipher (AES128) with Block Chaining (CBC) modality. The introduction of the MAC code guarantees integrity and authentication on LINcommunication with significant mitigation of the attacks introduced in section 9.2. CMAC-128bits with a truncated digest to 8 bytes guarantees a considerable security level increment. Sixty-four bits are the minimum digest's length for considering the MAC code as secure. Today, solutions embedding a 32-bit digest in the LINdata payload cannot guarantee this level of security.

By guaranteeing integrity and authenticity of LINresponse frames, LIN-MM ensures resiliency from the attacks that exploit the response frame as a vector, i.e., Spoofing, Man in the Middle (MitM), and Response collision attacks.

On the contrary, LIN-MM is not a viable security mechanism for those attacks that use the header frame as a vector, i.e., Header collision attacks. The primary constraint, in this case, is that the header frame is not large enough to multiplex a robust MAC code. Moreover, the LIN-MM is ineffective as a countermeasure for *Denail of Service (DoS)* attacks.

The LIN-MM architecture requires sharing a secret key between the master and the slave nodes. Storing this secret key is not a significant issue, given that all LINnodes are based on microcontrollers. In this context, the key management infrastructure becomes an important issue that must be considered before deploying this solution at a commercial level.

9.4.4 Noise analysis

During the LT-Spice simulation phase, we conducted targeted experiments to assess the protocol's noise resilience. With a constant battery voltage (VBatt) set at 13.5 volts, our findings indicated a noise tolerance reduction to approximately 9%. In the most challenging scenario examined, electrical noise was measured at 2.7% of the LIN noise band capacity. Given the absence of specific LIN vehicle noise models or direct in-vehicle noise data, we adapted an existing CAN network noise model for our experimental setup. The results from these evaluations bolster our confidence in the LIN-MM architecture's viability within actual automotive settings. Despite the observed decrease in noise tolerance attributable to the modulation component, the system is anticipated to operate effectively within acceptable noise tolerance margins.

9.5 Conclusion

LIN-MM represents a strategic enhancement aimed at modernizing the conventional LIN hardware utilized within the automotive sector. This initiative is in response to the emerging security regulations and requirements, with a keen emphasis on minimizing associated costs. Notably, LIN-MM is designed to be backward compatible with current LIN devices, enabling it to function within a hybrid network that accommodates both traditional LIN and LIN-MM devices. This adaptability makes LIN-MM a highly versatile solution, significantly lowering the financial burden associated with updating the existing vehicle fleet to comply with new cyber-security standards. The security assessment conducted demonstrates a marked enhancement in the security posture of the LIN network, particularly against the initial three categories of attacks outlined in section 9.2. However, it is acknowledged that vulnerabilities to Header collision attacks persist, as they are not directly mitigated by the

current LIN-MM framework. Efforts are currently underway to refine the LIN-MM architecture, with a provisional update named (Type-B) focused on bolstering the integrity of the LIN Header Frame, thereby addressing this identified weakness and further strengthening the network's resistance to such exploits.

Chapter 10

PSP Framework: Introducing a Novel Risk Assessment Approach Aligned with ISO/SAE-21434

10.1 Introduction

In chapter 2, we delved into the automotive industry's complex challenges, focusing on the stringent cybersecurity regulatory landscape and the emergence of new automotive technologies, particularly in the context of the green transition. The European Community's ambitious "Fit for 55" initiative [129], aimed at promoting (Zero-Emissions Vehicles (ZEVs)), marks a significant shift towards environmental sustainability by seeking to reduce carbon emissions and redefine automotive manufacturing and regulatory practices.

Alongside environmental efforts, the industry is also grappling with compliance challenges posed by the UNR-155, which places a significant burden on Original Equipment Manufacturers (OEM) to ensure that every component within the supply chain meets strict European regulatory standards. This is crucial for certification bodies tasked with enforcing these regulations. In response, the International Organization for Standardization (ISO) introduced the ISO/SAE 21434:2021 Road Vehicles - Cybersecurity Engineering Standard [130], providing a comprehensive framework for managing cybersecurity risks in the automotive sector.

This chapter examines the ISO/SAE 21434 standard, particularly its (Threat Analysis and Risk Assessment (TARA)) section. Our analysis highlights the vulnerabilities and limitations of the standard's risk assessment models, pointing out scenarios where these models may not accurately assess risks due to misalignment in index directions. Such issues cast doubt on the reliability of these methodologies for effectively quantifying and mitigating cybersecurity threats.

Our goal is to conduct a thorough critique and propose an enhanced approach that addresses these shortcomings and aligns closely with the rigorous demands of the ISO/SAE 21434:2021 standard. We offer a refined model that ensures more precise, reliable, and actionable outcomes from the TARA process. This chapter aims to bridge the gap between the theoretical foundations of cybersecurity standards and their practical implementation in the automotive industry. By advocating for a strong cybersecurity framework, we contribute to developing a resilient automotive sector capable of adapting to rapid technological advancements and ensuring future vehicles' safety, security, and environmental sustainability.

10.2 ISO/SAE-21434 STANDARD

In August 2021, the ISO/SAE-21434 was released, the first standard focused on cybersecurity for road vehicles. It was designed to support and ensure security throughout the ECU supply chain, specifically to help original OEMs comply with the UN R155 regulation. Figure 10.1 displays all the standards for developing the ISO/SAE-21434 standard. It is worth noting that many of the standards used in its creation are not solely related to the automotive industry, particularly those related to cybersecurity.

The development process of ISO/SAE is deeply rooted in the V-model, a cornerstone in software development practices. This model is also a fundamental part of the ISO-26262 [131] standard and the Automotive SPICE framework [132]. The process begins with the formulation of a TARA model, encompassing four key process activities: the identification of assets, the identification of threat scenarios, the rating of impact, and the analysis of attack paths. These activities are designed to be recursive, capable of being revisited at any stage of the development cycle, and are methodically implemented as outlined in Deliverable D2 of the HEAVENS project [133]. TARA becomes particularly crucial during production stages, especially when

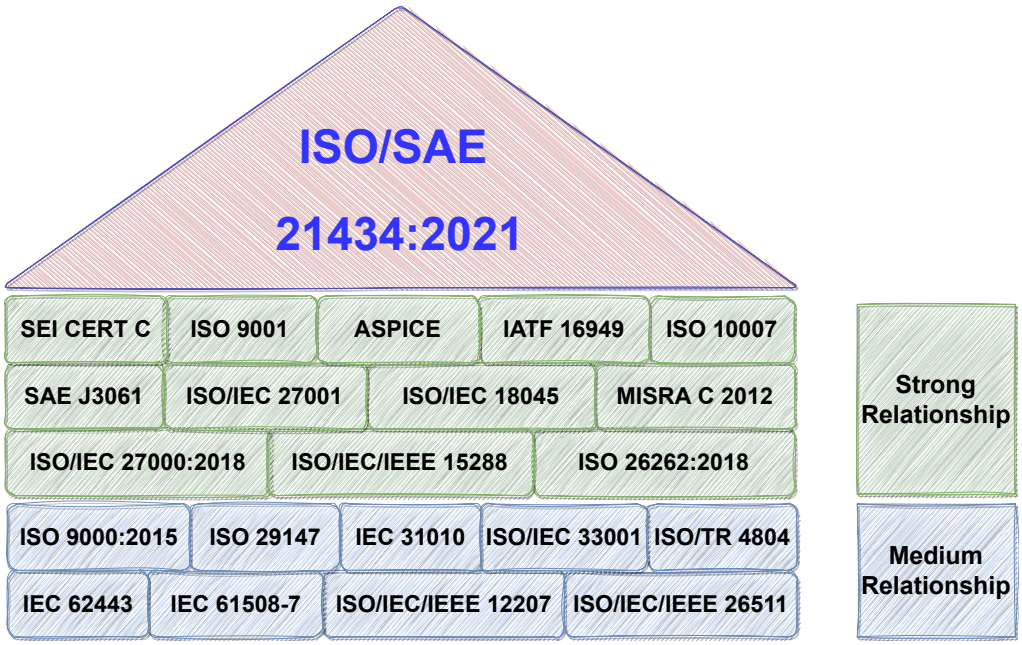


Fig. 10.1 Standards contribution list to ISO/SAE-21434. Source:[6].

vulnerabilities are identified in the field. Figure 10.2 showcases the integration of TARA across different phases of development..

In contrast to standards such as ISO-26262, ISO/SAE-21434 introduces predefined models with static weights as specified in Clause 15 of the standard (refer to Figure 10.3), which restricts the adaptability of the model to the specific needs of the automotive network domain. This rigidity in the model configuration stands as a constraint in the development of TARA, potentially resulting in outcomes that may not accurately reflect the real-world scenario.

The potential for inaccurate outcomes in analysis can be attributed to the emphasis on IT security over product security by other security standards. While the TARA model of ISO/SAE-21434 excels in areas closely associated with IT infrastructure, it necessitates enhancements in other sectors. Given the increasing complexity and diversity in vehicle architecture, the challenge lies in the static model's inability to address the nuances across all domains adequately. Figure 10.4 illustrates a simplified vehicle architecture, highlighting various functional domains and ECUs. However, not every domain is equally vulnerable to the same types of attacks. Upstream's reports [134] categorize attacks into three main types: long-range, short-range,

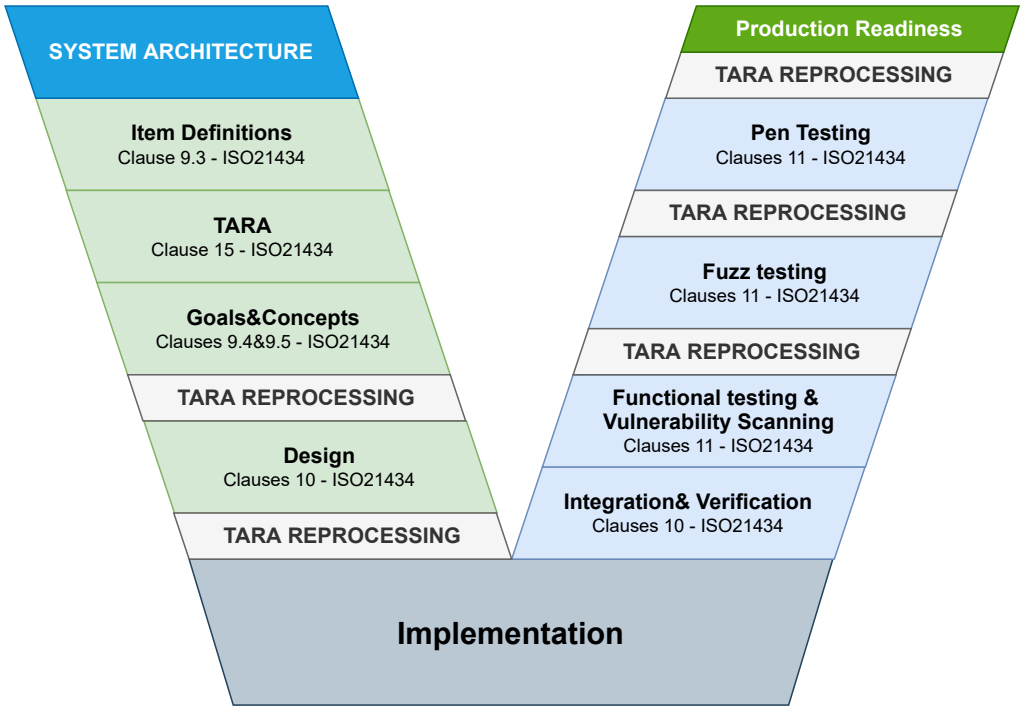


Fig. 10.2 ISO/SAE-21434 Development Life Cycle. Source:[6].

and physical access, while also acknowledging that potential attackers can differ significantly in their profiles, objectives, resources, and motivations [135].

The ISO/SAE-21434 standard sets forth threat feasibility models designed to unify threat modeling practices across different users, projects, applications, and organizations. These models are pivotal for fostering a uniform approach to threat modeling. Specifically, the standard outlines three models for assessing attack feasibility: those based on attack potential, the Common Vulnerability Scoring System (CVSS), and attack vectors. It categorizes attackers into various groups, such as Insiders (e.g., service or maintenance staff), Outsiders (e.g., black-hat hackers), Rational individuals (e.g., car owners), Malicious entities (e.g., criminals), Active agents (e.g., conventional thieves), Passive observers (e.g., competitors), and Local actors (e.g., the vehicle owner) [136].

Nonetheless, the application of a static Enterprise IT TARA model within the automotive industry's complex and varied landscape can yield unproductive outcomes. This issue becomes particularly pronounced in the context of developing TARA for an Engine ECU in compliance with ISO-21434. It underscores the limitations of all

Elapsed time		Specialist expertise		Knowledge of the item or component		Window of opportunity		Equipment	
Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value	Enumerate	Value
≤1 day	0	Layman	0	Public	0	Unlimited	0	Standard	0
≤1 week	1	Proficient	3	Restricted	3	Easy	1	Specialized	4
≤1 month	4	Expert	6	Confidential	7	Moderate	4	Bespoke	7
≤6 months	17	Multiple experts	8	Strictly confidential	11	Difficult/ none	10	Multiple bespoke	9
>6 months	19								

Fig. 10.3 Attack Potential weights model extracted by ISO/SAE-21434. Source:[6].

three models in accurately determining attack feasibility rates, revealing significant discrepancies in their effectiveness across different scenarios.

When the prescribed models from ISO/SAE-21434 were employed, the evaluation yielded a significantly elevated score for the possibility of remote attacks while undervaluing the threat from physical attacks, as exemplified in Figure 10.5. This assessment framework, however, may not align well with the realities of automotive safety-critical, hard real-time powertrain devices where physical attacks are neither uncommon nor overly complicated. In these contexts, the primary mode of communication is through the CAN bus, with external interfacing facilitated by the OBD port, which is readily accessible from the vehicle's cabin. Specifically, the potential for attacks on the CAN bus, especially targeting the powertrain subnet domain, tends to be predominantly physical [137]. The feasibility of executing remote attacks on ECUs that lack Firmware Over-The-Air (FOTA) capabilities is rare and presents substantial challenges. Typically, perpetrators of powertrain attacks fit the Insider or Rational Local profiles, characterized by unrestricted time and device access. Thus, the risk assessment scores generated by the ISO-21434 standard for powertrain scenarios can be misleading, as evidenced by various studies pointing out the deficiencies or inaccuracies in the TARA outcomes produced under the ISO-21434 framework [138, 139].

Moreover, the Cybersecurity Assurance Level (CAL) is defined based on attack vectors, including Physical, Local, Adjacent, and Network, as depicted in Figure 10.6. ISO-21434 establishes four cybersecurity target levels, from the most stringent, CAL4, to the least, CAL1, analogous to the Automotive Safety Integrity Level (ASIL) levels in ISO-26262. The powertrain sector, responsible for real-time operations critical to safety, is susceptible to DoS attacks [140] primarily through

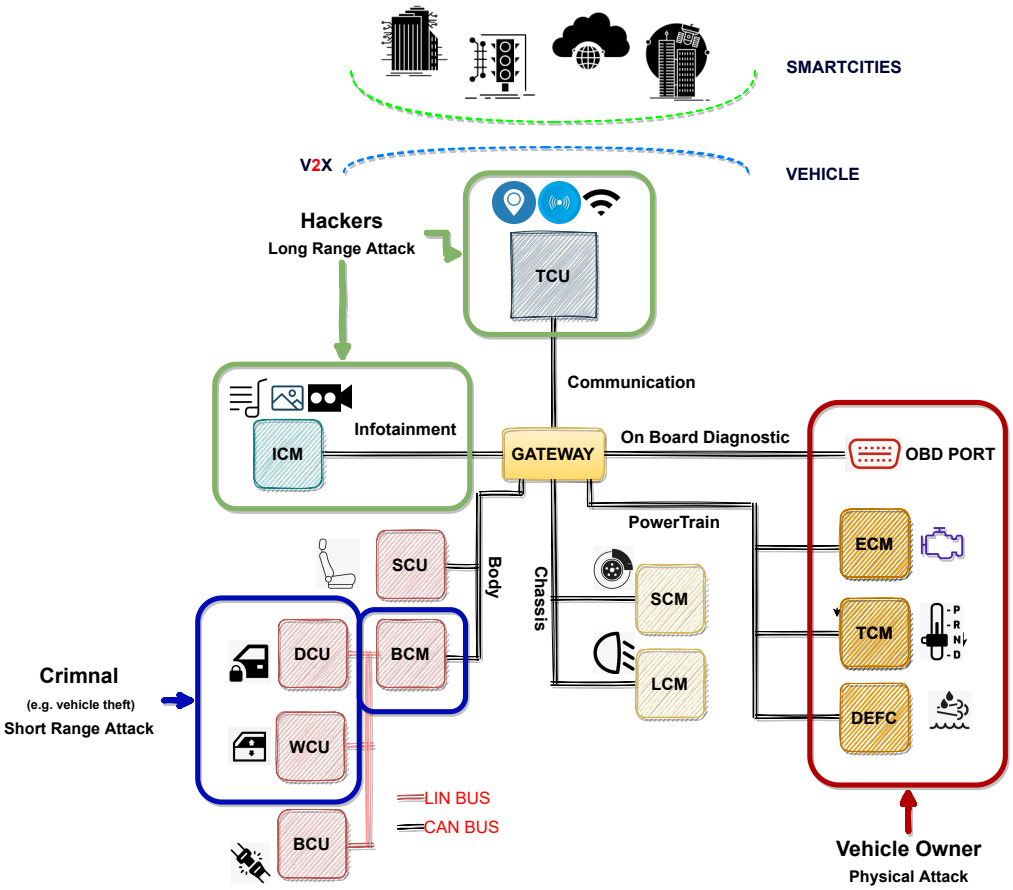


Fig. 10.4 The figure highlights in green the ECUs with a suitable rate for Long-range Attack, in blue the Short-range Attack while the red confines the Physical Attack ECUs

physical means. It's important to note that such attacks are not considered a significant concern beyond a CAL2 security status, indicating a moderate to low-security focus. This reflects the ISO-21434 standard's classification of physical attack threats up to CAL2, as illustrated in Figure 10.6.

Consequently, numerous industrial technical forums have called for a revision of the TARA model as implemented by ISO/SAE-21434. While various papers offer solutions or enhancements, the inherent complexity, heterogeneity, and vulnerability to Man At The End (MATE) attacks [141] of the system mean that no single solution can comprehensively address the entire spectrum of potential attack surfaces and attacker profiles with adequate precision. This highlights a critical challenge in achieving a universally applicable and accurate threat assessment within the automotive cybersecurity domain.

Attack feasibility rating	Criteria
High	**Network:** Potential attack path is bound to network stack without any limitation. EXAMPLE 1 Cellular network connection making the ECU directly connected and accessible on the internet.
Medium	**Adjacent:** Potential attack path is bound to network stack; however, the connection is limited physically or logically. EXAMPLE 2 Bluetooth interface, virtual private network connection.
Low	**Local:** Potential attack path is not bound to network stack and threat agents require direct access to the item for realizing the attack path. EXAMPLE 3 Universal serial bus mass storage device, memory card.
Very low	**Physical:** Threat agents require physical access to realize the attack path.

Fig. 10.5 Attack vector-based approach extracted by ISO/SAE-21434. Source:[6].

		Attack vector[b]			
		Physical	**Local**	**Adjacent**	**Network**
Impact	Severe	CAL2	CAL3	CAL4	CAL4
	Major	CAL1	CAL2	CAL3	CAL4
	Moderate	CAL1	CAL1	CAL2	CAL3
	Negligible	---[a]	---[a]	---[a]	---[a]

[a] See [PM-06-08].

[b] Attack vector is a static parameter of attack feasibility.

Fig. 10.6 CAL determination based on impact and attack vector parameters table extracted by ISO/SAE-21434. Source:[6].

10.3 PSP Dynamic TARA Model for Road Vehicle Purpose

As highlighted in Section 10.2, the Road Vehicle sector is characterized by its extensive diversity, encompassing various domains, sub-domains, attack surfaces, attack vectors, and profiles of attackers. Consequently, static security assessment models can yield inaccurate outcomes under certain conditions. This scenario poses a significant risk to the automotive industry, as firms allocate substantial resources towards ensuring their offerings are secure, not only to comply with legal mandates but also to augment product value. Nevertheless, the reliance on unreliable

assessment models may lead to the misallocation of resources, with firms potentially focusing on less critical areas.

Our goal is to circumvent such scenarios by introducing a non-intrusive, adaptive framework known as PSP, which is an acronym derived from the initials of its creators. This framework is designed to support analysts in evaluating the likelihood of attacks.

The PSP framework operates through a dual approach. Initially, it employs dynamic models that adhere to the guidelines of the ISO-21434 standard, adjusting weights dynamically to assess various conditions accurately. Following this, it facilitates the development of a bespoke runtime model that estimates the potential financial implications of attacks.

Furthermore, the PSP framework incorporates Natural Language Processing (Natural Language Processing (NLP)) techniques to refine its attack feasibility evaluation model. While Machine Learning and Deep Learning [142] have found application in several automotive sectors, including IDS [143] and Manufacturing [144], the application of NLP within the road vehicle domain remains limited [145, 146]. Our proposed methodology leverages NLP for conducting sentiment analysis on social media data for specific attack types, such as Insider, Rationale, and Local attacks, as detailed in Section 10.2. Through the application of NLP, the PSP framework can automatically generate updated weight tables in alignment with ISO-21434 standards, thereby enhancing the accuracy of analyses across all circumstances. This enables security teams to more accurately gauge the severity of MATE (Man-At-The-End) attacks, which have been identified in existing studies as challenging to evaluate [147].

The workflow of the PSP framework is depicted in Figure 10.7, highlighting the steps involved from initial input to the generation of updated attack feasibility tables. Initially, the PSP framework utilizes Twitter APIs [148] to gather data. Inputs such as the type of target application (for example, cars, trucks, agriculture machinery), the geographical region (such as Europe, North America, etc.), and the category of the application (like sports cars, vans, industrial, domestic, etc.) are fed into the system (as shown in Figure 10.7, block 1). At the onset, a predefined list of relevant hashtags (e.g., #dpfdelete, #egrremoval, #egrdelete, #egroff, #dieselpower, #chiptuning) is

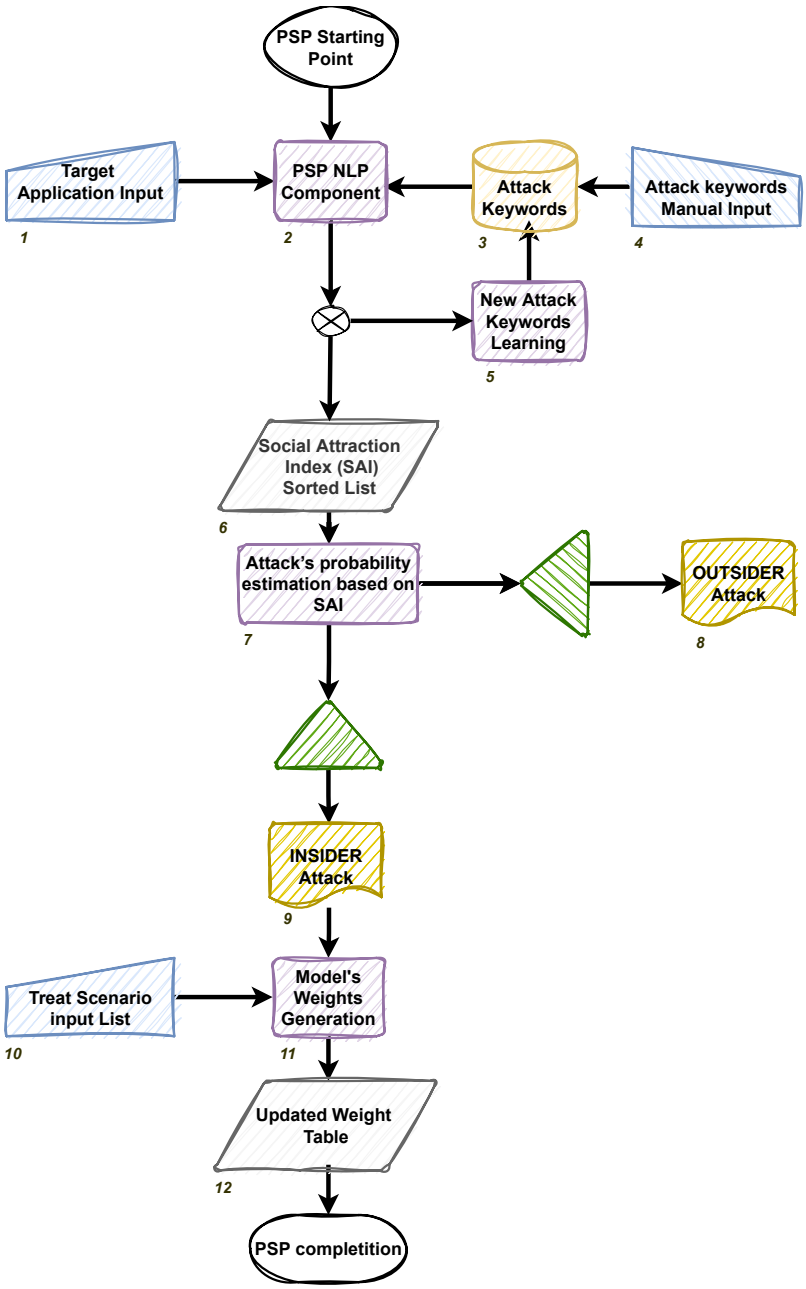


Fig. 10.7 PSP Work-Flow Scheme. Source:[6].

used to populate the keyword attack database, as indicated in Figure 10.7, blocks 3 and 4.

This information then undergoes analysis by the PSP's NLP component (Figure 10.7, block 2), which generates a ranked Social Attraction Index (Social Attrac-

tion Index (SAI)) list. The ranking is determined by analyzing Twitter posts for the specified target and keywords, focusing on the posts' view counts, interaction levels, and overall popularity to calculate each entry's estimated attack probability (demonstrated in Figure 10.7, blocks 6 and 7).

During the SAI computation, an auto-learning component within the NLP system is activated to integrate new keywords into the database for subsequent analyses, ensuring comprehensive and accurate findings by preventing keyword shortages (this process is outlined in Figure 10.7, block 5).

Subsequently, the SAI list entries are categorized into either insider or outsider attacks. Insider attacks are those acknowledged and permitted by the owner, even if executed by third parties (such as untrusted services or racing workshops), whereas outsider attacks are unauthorized third-party actions of which the owner is unaware (like criminal activities, theft, or black hat hacking). Given that social media typically highlights insider threats, adjusting the model's standard weight values for outsider threats is deemed unnecessary.

The PSP framework primarily addresses insider threats, which are specific to products, notably in the realms of road vehicles and IoT. These insider attacks, being distinct from traditional IT domain threats, necessitate greater expertise for effective management.

At this juncture, the PSP framework combines the insider attack list with a set of threat scenarios identified by the product security team to create new ISO-21434 compliant attack feasibility tables, incorporating revised weight values (as seen in Figure 10.7, block 12).

According to the ISO-21434 standard, attack vectors are assigned fixed weight values in the model (illustrated in Figure 10.5). For outsider threats, the PSP framework maintains these standard weights, as depicted in Figure 10.8-A. However, for insider threats, it modifies the weights based on corrective factors derived from the SAI (noted in block 7 of Figure 10.7), potentially altering the prioritization of attack vectors (as illustrated in Figure 10.8-B).

To demonstrate the capabilities of the PSP framework, we will examine a potential threat scenario involving Engine Control Module (ECM) reprogramming. While this type of attack has a low feasibility rating according to ISO-21434 weights due to its physical attack vector (Figure 10.5) [149], according to [134], it has a high oc-

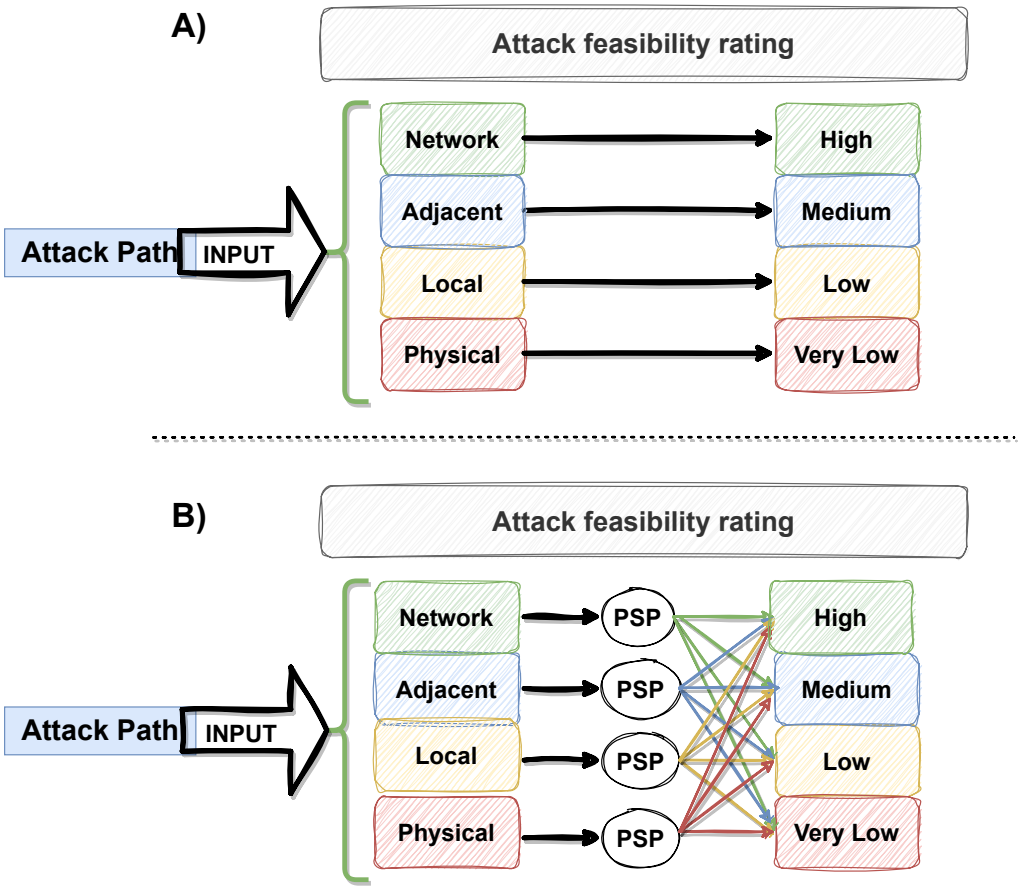


Fig. 10.8 The figure **A)** shows the attack feasibility weights, defined by ISO-21434, for outsider threats **B)** On the contrary, the insider threats get attack feasibility weights tuned by PSP framwork. Source:[6].

currence rate preferably based on physical attacks. By utilizing the PSP framework, we were able to update the standard attack feasibility value table, resulting in a more accurate assessment of the threat (Figure 10.9-B).

It's worth noting that the social sentiment analysis time window plays a crucial role in the PSP framework's analysis. For instance, Figures 10.8-B and 10.8-C show different attack feasibility ratings for the same threat scenario in the insider attack domain. This is because the PSP platform considers all Twitter posts in the former, while it only focuses on recent posts from 2021 onwards in the latter. The trend inversion highlighted by PSP began last year and is confirmed by the Upstream global automotive cybersecurity report. As a result, reprogramming via a physical attack is no longer mainstream, and attackers are more likely to opt for a local attack

via OBD. While this demonstrates PSP's ability to detect current threats, it also highlights the attackers' improved techniques for bypassing secure mechanisms using local attacks.

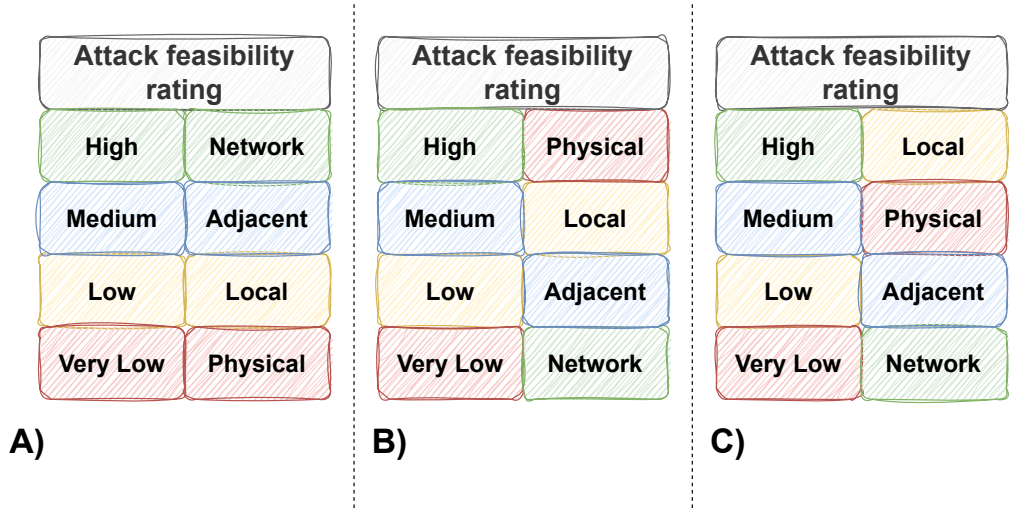


Fig. 10.9 The figure **A)** show the original G.9 table titled Attack vector-based approach provided in ISO-21434 document. Figure **B)** revised the G.9 table applying the PSP model corrections for ECM reprogramming as a Threat Scenario. The final figure, **C)**, always shows a revised G.9 table by PSP model built on the same database but limiting the data since 2022. Source:[6].

The enhancement of attack feasibility models, as per the ISO-21434 standards, represents just one facet of the PSP framework. Additionally, it innovates by devising an attack feasibility model rooted in a financial index, premised on the assumption that vehicle owners orchestrate all internal tampering or reprogramming breaches, albeit illegally, for personal gain.

Insider attacks have burgeoned into a profitable niche, with the widespread adoption in the aftermarket tuning sector—encompassing ECU reprogramming, external control units, and emission defeat devices—indicating a substantial market. These modifications are typically motivated by desires to reduce operational costs or enhance performance, with industrial vehicles generally aiming for the former and passenger vehicles and light trucks the latter. The feasibility of an insider attack correlates directly with its market demand; if the execution costs align with market willingness, the attack's likelihood increases, whereas sparse occurrences suggest a misalignment with market demand.

The PSP framework excels in mapping, classifying, and ranking insider attacks, capitalizing on market visibility. This method proves particularly effective in evaluating critical elements marked by high unpredictability and volatile market trends, as facilitated by MATE. Social tags streamline the collection of new data, enabling rapid trend identification. Figure 10.10 delineates the PSP action flow.

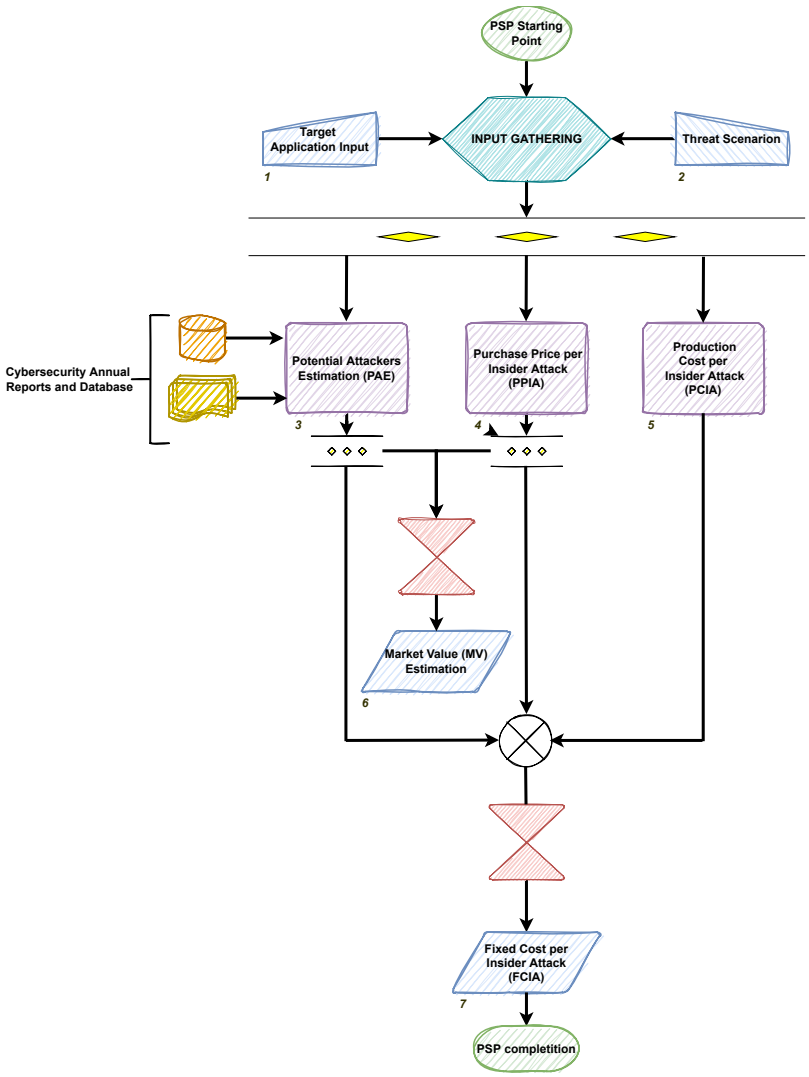


Fig. 10.10 Financial attack feasibility PSP Work-Flow Scheme. Source:[6].

The PSP framework is used to determine the market value (MV) of a potential insider attack by computing each threat scenario through equation Equation 10.1. MV is the initial measure of the size and profitability of an attack. The equation takes into account two factors: PAE (Figure 10.10, block 1) estimates the number

of potential attackers, while *PPIA* (Figure 10.10, block 2) represents the maximum purchase price a vehicle owner would be willing to pay for an insider attack. To estimate *PPIA*, the framework utilizes NLP and text mining techniques to cluster adversary devices or services found online based on their prices. The *PAE* value is determined by Equation 10.2, which relies on past year's vehicle sales (VS) trend reports. In non-monopolistic markets, VS is replaced with market share (MS). The framework also considers the percentage of potential attackers (PEA), which is determined by analyzing vehicle cybersecurity annual reports. The search parameters can be customized based on vehicle, application, years, period, historical trend, and region.

$$MV = PAE \cdot PPIA \tag{10.1}$$

$$PAE = \begin{cases} VS \cdot PEA, & \text{for monopolistic markets} \\ MS \cdot PEA, & \text{for non-monopolistic markets} \end{cases} \tag{10.2}$$

The MV index helps us determine whether an attack falls within the intended scope. To increase our confidence level in estimating the feasibility of an attack, it is crucial to calculate the break-even point (BEP) using mathematical methods [150]. The BEP is the point at which the cost of producing an asset, in this case, an insider attack, is equal to its purchase price. Insider attacks are profitable in the blue area (shown in Figure 10.11), where their feasibility rate ranges from medium to high. Conversely, attacks in the red zone are not profitable, as their revenue is lower than their costs.

In Equation 10.3, a formula is presented for calculating the BEP. This formula uses a numerator that represents the fixed cost (FC) and a denominator that represents the difference between the purchase price per unit (PPU) and the variable cost per unit (VCU). The VCU considers the manufacturing cost, such as installing a defeat device in the case of an insider attack. In the scenario discussed in this paper, the PPU is defined as *PPIA* in Equation 10.1, the highest price an attacker would be willing to pay.

Since it is unlikely that a single attacker would be able to conduct a global physical attack, the revenue per unit expressed in the denominator is divided by the number of attackers (n), which is equivalent to multiplying the fixed cost (FC) by n.

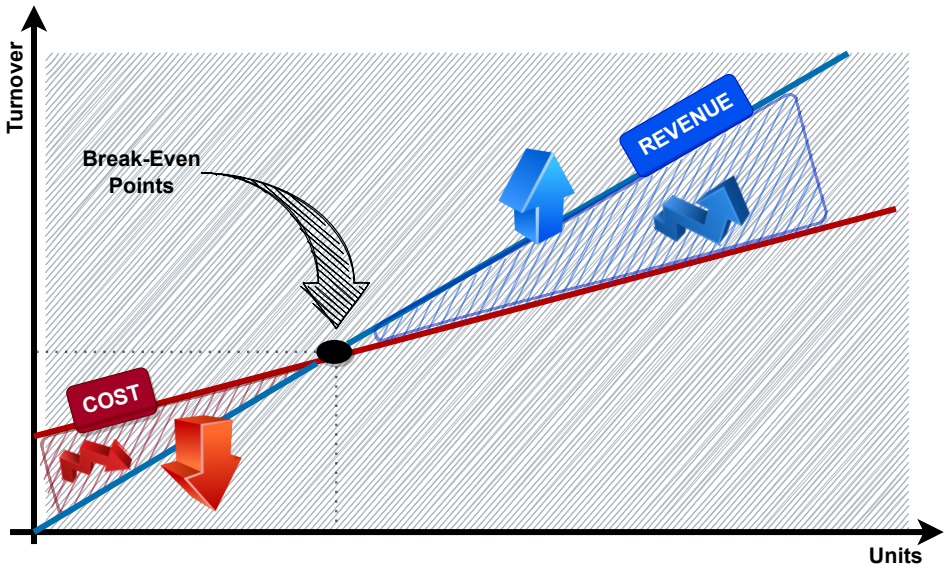


Fig. 10.11 The figure shows a standard BEP diagram. In our study, it is important to understand where the zone is profitable for the attackers. Source:[6].

$$BEP = \frac{FC}{\frac{(PPIA-VCU)}{n}} = \frac{FC \cdot n}{(PPIA - VCU)} \tag{10.3}$$

As demonstrated in Equation 10.4, the value of FC is determined by considering the total number of hours required to organize the research and development activities for the adversary ($FTEH$). The hourly cost (ch) is based on a standard salary for black hat hackers. The final factor involves calculating the depreciation of Capital Expenditures (CAPEX) items on a straight-line basis (SLD), which includes various development tools, electronic instruments, and specialized hardware and software, primarily laboratory instrumentation such as Analyzers, Tracers, Debuggers, and Oscilloscopes.

$$FC = (FTEH \cdot ch) + SLD \tag{10.4}$$

The information provided by the break-even point is helpful for enhancing product security. The PSP framework utilizes the inverse function (Equation 10.5) where FC is an unknown term, and the BEP value is equivalent to the PAE. In this

way, the framework allows for calculating the total investment required to develop an insider attack.

$$FC = \frac{BEP \cdot (PPIA - VCU)}{n} \tag{10.5}$$

10.4 Experimental Results

10.4.1 Dynamic Weight Model

To assess the accuracy of the PSP framework, we examine its application to a common security threat in the automotive industry involving the use of defeat devices. These devices are engineered to tamper with an analog sensor signal. In this type of attack, the attacker first analyzes the sensor signal profile to pinpoint vulnerabilities. They then create an algorithm to alter and control the physical sensor signal. This algorithm is programmed into a configurable device, known as a defeat device, which is capable of implementing the desired modifications to the sensor signal. These devices are commercially available and are installed on the target system to execute the intended manipulations. Such manipulations might include increasing the vehicle's power or reducing maintenance costs. Defeat devices are widely marketed and often heavily promoted on social media platforms, leading to high public exposure.

In this analysis (Figure 10.12), the CVSS score—a standardized framework for rating the severity of security vulnerabilities—is applied to a specific threat under two distinct weighting regimes. Initially, when assessed with the standard weights set by ISO-21434, the threat receives a "Very Low" feasibility rating, indicating minimal risk. This standard assessment relies on traditional parameters that may not fully capture the dynamic nature of modern cyber threats.

However, when reassessed using the PSP Framework's dynamic weights, which incorporate the threat's traction on social media, the feasibility rating is adjusted to "Medium." This adjustment, achieved by tuning the Opportunity parameter from 10 to 0, indicates a more significant potential impact. The recalibration reflects the increased attention and potential exploitation due to the threat's visibility and public

Fig. 10.12 CVSS score comparison between ISO standard weight and PSP dynamic weight applied to the same threat. Source:[6].

discussion. As the threat garners more attention on social media, it becomes more likely to be exploited, necessitating a higher risk rating.

This contrast underscores the limitations of static weight systems in adapting to the rapidly evolving nature of cyber threats. Static systems often fail to account for external factors, such as media exposure, that can quickly alter a threat's severity. By recalibrating the risk assessment based on current data, the PSP Framework ensures that CVSS scores reflect a more accurate measure of the threat's real-time implications. This approach is particularly crucial in sectors where threat landscapes evolve swiftly, such as cybersecurity, finance, and critical infrastructure, ensuring that risk management strategies remain agile and informed.

The PSP Framework's strategy emphasizes that, given the high visibility of this threat, a higher risk rating is warranted. This underlines the platform's effectiveness in providing a more precise and adaptable approach to cybersecurity risk evaluation for certain types of attacks. By incorporating real-time data and social media trends, the PSP Framework enhances the accuracy and relevance of risk assessments, enabling organizations to respond more effectively to emerging threats.

10.4.2 PSP feasibility attack based on financial

To evaluate the financial viability of calculating the attack index, we used the search term "excavator, Europe" within the PSP framework. This input initiated the generation of a summary focused on insider attacks involving excavators. As illustrated in Figure 10.13, the SAI graph highlights the deactivation of the Diesel Particulate Filter (DPF) as the most severe insider threat, assigning it the highest score. The PSP framework computes these scores by analyzing and correlating SAI data with a post outline that tracks metrics such as views, occurrences, and interactions. For this analysis, we aimed to establish the financial threshold for the most significant threat, which is DPF removal. The framework thus determines the point at which an attack becomes economically viable.

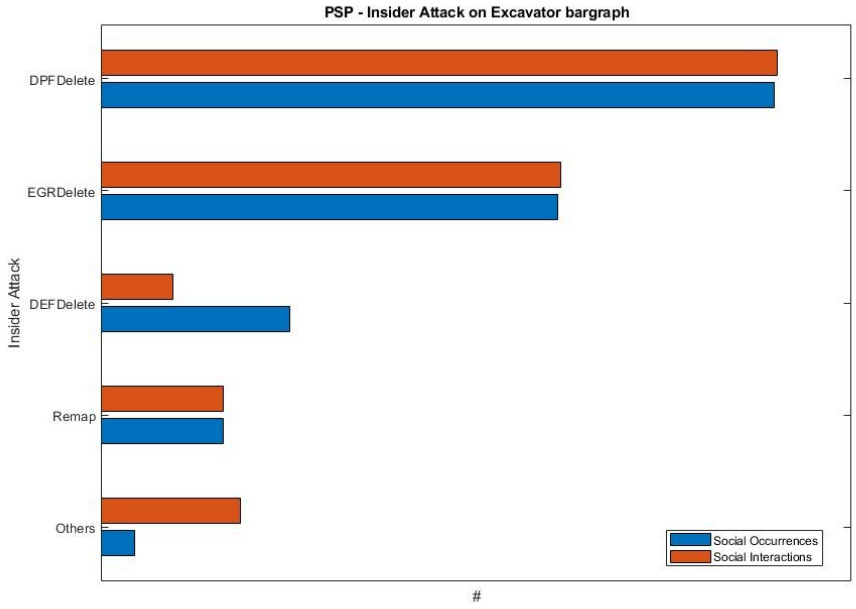


Fig. 10.13 PSP draft result about Excavator Insider Attack gotten by SAI. Source:[6].

The estimated market value (MV) for the DPF tampering attack in Europe is 506,160 EUR per year (as referenced in Equation 10.6). This figure is based on sales data from the previous year and refers to DPF tampering incidents on European soil excavators. The NLP method determines that a defeat device's average cost is 360 EUR after network screening. Text mining on cybersecurity reports provides the

number of potential attackers, which is 1,406 for a major company based on the Upstream annual report.

$$\begin{aligned} MV &= PAE \cdot PPIA \\ &= 1,406 \cdot 360\, EUR \approx 506,160\, EUR \end{aligned} \tag{10.6}$$

Simultaneously, the PSP platform returned an approximate value of 145,286 EUR for FC as indicated in Equation 10.7. This calculation considers the difference of 310 EUR between $PPIA$ and VCU, provided by the PSP platform's NLP search. It assumes three potential competitors for the attack (as estimated by the same NLP search).

$$\begin{aligned} FC &= \frac{BEP \cdot (PPIA - VCU)}{n} \\ &= \frac{1,406 \cdot 310}{3} \approx 145,286\,\text{EUR} \end{aligned} \tag{10.7}$$

The value of FC reflects the investment required for an attacker to execute an insider attack successfully. The higher the FC, the less feasible the attack becomes, significantly when the cost outweighs the potential revenue. In light of this example, the development team should create a secure anti-tampering DPF architecture to ensure product security that can withstand an adversary's investment of up to 145,286 EUR without being compromised in term of financial analysis. Investing more than 145,286 EUR to develop a defeat controller to override the DPF system does not guarantee a return on the investment or any revenue.

This illustrates how the FC index computed by the PSP platform can serve as a new attack feasibility index integrated into the general ISO-21434 models discussed earlier, fine-tuning market demand to better reflect the attack trend.

10.5 Conclusion

In conclusion, the PSP framework stands out as a pioneering tool that harnesses social media sentiment analysis to dynamically generate weight models, crucial

for decision-making within the automotive industry. This paper has highlighted the evolution from static risk assessment models, such as those outlined in ISO-21434, towards a more dynamic, runtime model environment. This shift allows for continuous monitoring of internal risks and mitigates uncertainty across all areas of the automotive sector, ensuring adaptability and suitability for diverse vehicle domains.

The framework's integration of risk feasibility models across various automotive domains ensures a consistent and reliable performance level, proving indispensable in this sector. The utilization of real-time data enhances the accuracy and practical relevance of security assessments, a significant advancement over purely theoretical models.

The preliminary concept of the PSP framework, developed using Twitter APIs, has already demonstrated satisfactory results in terms of model quality. However, significant efforts are necessary to operationalize the framework fully and automate the validation process. Enhancements are also required to improve the automation of new keyword updates and bolster attacker keyword strategies against poisoning.

Looking ahead, the planned expansion to encompass a broader array of social media platforms promises a richer dataset for analysis, potentially transforming the framework into a more comprehensive tool for capturing consumer sentiment and trends. Furthermore, the development of an anti-poisoning mechanism is essential for enhancing the framework's robustness by safeguarding against data manipulation and ensuring data integrity. This mechanism will further solidify the PSP framework's reliability.

These developments and strategic enhancements underline the PSP framework's potential to revolutionize how the automotive industry leverages social media data for strategic decision-making. By continuously adapting to technological advancements and broadening its capabilities, the PSP framework is poised to deliver refined, secure, and data-driven solutions, driving greater innovation and efficiency in the automotive sector.

Chapter 11

Final Conclusion

11.1 Research Journey

Navigating through a maze, this research journey uncovered fresh challenges and insights into the interplay between cybersecurity and automotive technologies. It was a personal and academic expedition that challenged my assumptions and expanded my intellectual curiosity.

The genesis of the research was a fundamental yet profound inquiry: how can we safeguard tomorrow's vehicles from cyber threats? The question became a multifaceted exploration of technology, policy, and human factors. The research inquiry and methodology were continually refined, guided by a pursuit of clarity and rigour. It required a comprehensive understanding of cybersecurity principles and automotive technologies and a willingness to explore new territories.

The journey encountered various challenges, each providing a valuable lesson in resilience and adaptability. Technical obstacles, such as simulating cyber attacks on automotive systems, and methodological dilemmas, such as balancing depth with breadth, were just a few examples. However, the journey also had moments of uncertainty where unexpected discoveries illuminated new avenues of inquiry and broadened the research's scope.

Upon reflection, the dynamic nature of the cybersecurity and automotive domains has become apparent. The pace of technological innovation and the evolving tactics of cyber adversaries present a challenging target for researchers and practitioners.

This research exemplifies the need for agility, foresight, and a collaborative approach to address these challenges.

11.2 Summary of Research Contributions

The core of this thesis revolves around significant strides made in enhancing cybersecurity within the automotive domain. These contributions address pressing security challenges and lay a foundation for future advancements in vehicle technology and cyber defense mechanisms. Here, we encapsulate the pivotal research contributions outlined throughout the study.

Novel Vehicle Architectures for Enhanced Security: The first significant contribution of this research is the development of novel vehicle architectures designed to elevate the standard of cybersecurity in automotive systems. Considering modern vehicles' intricate and interconnected nature, the investigation proposed a comprehensive strategy that integrates security into every aspect of vehicle design. Its holistic consideration of hardware and software characterizes these architecture components, ensuring comprehensive protection against cyber threats.

Key features of this novel architecture include the implementation of secure boot mechanisms, HSMs for cryptographic operations, and advanced IDS tailored for vehicular networks. Through implementing a multi-layered defence strategy, this architecture provides a comprehensive framework for protecting vehicles against sophisticated attacks, including those that exploit V2V and V2I communications.

Advanced Secure CAN and LIN Protocol: A critical aspect of automotive cybersecurity addressed in this thesis is the security of vehicular communication protocols, notably the CAN and LIN. The research introduced innovative methods to secure these protocols, which are fundamental to the operation of modern vehicles but have been historically vulnerable to cyber attacks.

The thesis presented a novel encryption method for the CAN protocol that significantly reduces the computational overhead typically associated with cryptographic processes. This method leverages out-of-band encryption to ensure data integrity and authenticity without compromising the performance of vehicular networks. Similarly, the research outlined a secure communication scheme incorporating encryption and authentication measures for the LINprotocol. This scheme offers a unique solution

for enhancing LIN-based communications' security without requiring extensive modifications to vehicle designs.

Framework for Attack Feasibility Analysis Using Social Media: Another significant contribution of this thesis is creating a framework to evaluate the possibility of cyber-attacks on vehicles by analyzing sentiment data from social media. This approach represents a novel application of sentiment analysis techniques, using data from platforms like Twitter to gauge public sentiment towards automotive security issues.

By analyzing social media discussions, the framework identifies potential vulnerabilities and emerging threats based on the public's perception and knowledge of cybersecurity in the automotive sector. This predictive model enables automotive manufacturers and cybersecurity professionals to address the most significant feasibility attacks and threats. Furthermore, this framework fully complies with the ISO 21434 standard on automotive cybersecurity management, ensuring its relevance and applicability to current industry practices.

11.3 Practical Implications and Applications

The practical implications of the research presented in this thesis are profound, particularly in the automotive industry where it addresses the cybersecurity challenges unique to vehicular systems. Until now, the reliance on cybersecurity techniques derived from the broader information technology domain has left certain vehicular threats unaddressed. This section of the thesis examines how the contributions of the study offer targeted solutions that bridge this gap, improving the security of automotive systems against domain-specific threats.

The research offers tailored cybersecurity measures for automotive systems that represent a significant departure from conventional IT-centric cybersecurity approaches. By focusing on the unique operational and architectural characteristics of automotive systems, these contributions provide a security framework that addresses the specific vulnerabilities and threat vectors prevalent in vehicular environments.

For example, the introduction of out-of-bound encryption methods for the **CAN protocol** considers the limited computational resources and real-time requirements of automotive systems, offering an efficient yet robust security solution. Similarly,

the secure communication scheme for the **LIN protocol** demonstrates a deep understanding of the automotive domain, providing security enhancements without necessitating major changes to existing vehicle architectures.

The practical application of these research contributions extends to current and future automotive designs. Vehicle manufacturers can integrate the proposed novel vehicle architectures and communication protocols into new vehicle designs to ensure high cybersecurity from the outset. Furthermore, the modular nature of these solutions allows for their implementation in existing vehicles through software updates and retrofitting, providing a means to enhance the security of the current automotive fleet.

Implementing these cybersecurity measures will protect vehicles against cyber threats and boost consumer confidence in automotive technology, a critical factor as the industry moves towards more connected and autonomous vehicles.

The alignment of this research with the **ISO 21434 standard** and its contributions to advancing cybersecurity practices in the automotive industry have significant policy and standardization implications. By demonstrating the effectiveness of domain-specific security measures, this study provides a solid foundation for developing industry-wide cybersecurity standards tailored to the automotive domain.

Regulatory bodies and standardization organizations can leverage the insights and methodologies presented in this thesis to refine and extend existing cybersecurity guidelines, ensuring they adequately cover the unique aspects of vehicular systems. Collaboration between academia, industry, and regulators is essential for establishing a coherent and effective cybersecurity framework for the automotive sector.

The practical applications of this research are not limited to vehicle manufacturers and cybersecurity professionals; they offer valuable insights for academic institutions and research organizations focused on automotive cybersecurity. The methodologies and findings presented can serve as a benchmark for future studies, encouraging further innovation and exploration in this essential field.

The comprehensive approach to addressing automotive-specific cybersecurity challenges outlined in this thesis highlights the importance of domain-specific research and development efforts. As the automotive industry continues to evolve, the relevance of these contributions will only increase, providing a roadmap for securing the next generation of automotive technologies.

The significance of this research lies in the fact that current automotive cybersecurity techniques, primarily derived from the information technology area, fall short of fully addressing the specific threats of the automotive domain. By developing cybersecurity solutions with an inherent understanding of automotive operational and threat landscapes, this thesis bridges the critical gap between generic IT security measures and the specific needs of automotive cybersecurity.

The research offers a new paradigm for automotive cybersecurity that is both effective and specifically tailored to the unique challenges of the domain. As vehicles become increasingly connected and autonomous, the adoption of these domain-specific cybersecurity measures will be crucial in safeguarding against current and emerging threats, ensuring the safety and security of automotive systems now and into the future.

11.4 Future Research Directions

The findings from this thesis lay a solid groundwork for advancing cybersecurity within the automotive domain, mainly through the innovative use of social media for attack feasibility analysis. A key direction for future research is the expansion and enhancement of this framework, aiming to develop an open-source platform that can execute vulnerability management monitoring in compliance with the ISO 21434 specification. This section outlines potential avenues for future exploration to realize this goal, addressing technical, methodological, and practical aspects.

11.4.1 Development of an Open-Source Platform for Vulnerability Management

A primary objective for future research is creating an open-source platform that integrates the principles of the proposed framework for attack feasibility analysis. This platform would serve as a comprehensive tool for automotive cybersecurity professionals, enabling real-time monitoring of potential vulnerabilities and cyber threats as discussed in social media and other digital forums. Key features of this platform could include:

- **Automated Sentiment Analysis:** Leveraging advanced natural language processing (NLP) algorithms to automatically detect and interpret sentiment in social media data, identifying potential threats and vulnerabilities discussed within the public domain.
- **Real-Time Threat Intelligence:** Providing real-time updates on emerging threats by analyzing vast data streams from various social media platforms, forums, and other online sources relevant to automotive cybersecurity.
- **Integration with ISO 21434 Processes:** Ensuring that the platform's functionality aligns with the vulnerability management and monitoring requirements specified by ISO 21434, facilitating compliance and enhancing cybersecurity risk management efforts within automotive organizations.

11.4.2 Enhancing Data Analysis Capabilities

Future research should focus on enhancing the data analysis capabilities of the proposed framework to handle the vast and diverse datasets inherent to social media. This involves developing more sophisticated algorithms that can accurately identify and categorize cybersecurity-related discussions, distinguishing between genuine threats and benign conversations. Improvements in this area could include:

- **Advanced Machine Learning Models:** Using machine learning models capable of understanding context, sarcasm, and technical jargon specific to the automotive cybersecurity domain to improve threat detection accuracy.
- **Cross-Platform Analysis:** Developing methodologies for integrating data from multiple social media platforms and online forums, providing a comprehensive view of the cybersecurity landscape concerning the automotive industry.

11.4.3 Addressing Privacy and Ethical Considerations

As this research direction involves the analysis of publicly available social media data, future studies must also address the privacy and ethical considerations associated with this approach. This includes:

- **Data Anonymization:** Implementing robust data anonymization techniques ensures that individual privacy is respected while conducting sentiment analysis and threat detection.
- **Ethical Guidelines:** Developing ethical guidelines for collecting, analyzing, and using social media data in cybersecurity threat assessment to ensure responsible research and monitoring activities.

11.4.4 Collaboration and Community Involvement

The development of an open-source platform for vulnerability management monitoring underscores the importance of collaboration and community involvement. Future research efforts should prioritize:

- **Engagement with the Open-Source Community:** Encouraging contributions from the global open-source community to enhance the platform's capabilities, foster innovation, and ensure adaptability to growing cybersecurity threats.
- **Collaboration with Industry and Academia:** Establishing partnerships with automotive manufacturers, cybersecurity firms, and academic institutions to validate the platform's effectiveness, gather feedback, and incorporate industry-specific insights into its development.

The future research directions outlined above aim to build on the foundational work presented in this thesis, focusing on developing an open-source platform for automotive cybersecurity vulnerability management. Enhancing the framework's capabilities to analyze attack feasibility through social media will help strengthen cybersecurity strategies in the automotive industry, following ISO 21434 standards. The realization of these goals will require a multidisciplinary approach, combining expertise in cybersecurity, data science, software development, and automotive engineering to create a powerful tool for safeguarding against cyber threats in the automotive domain.

11.5 Concluding Reflections

As we conclude this voyage of exploration, discovery, and innovation, we must reflect on the significant implications of our findings and the road ahead. The intersection of automotive technologies and cybersecurity poses a technical challenge and a societal necessity that requires immediate and sustained attention. Even as the vehicles of tomorrow promise unprecedented levels of convenience, autonomy, and connectivity, they also pose significant risks if they are not protected against the growing digital age threats.

Through a rigorous analysis of modern automotive systems and experimentation with novel mitigation measures, the research presented in this thesis has provided valuable insights into the complex landscape of cyber threats and the intricate vulnerabilities embedded in such systems. However, the work presented here is only a stepping stone towards a more secure and resilient automotive future.

It is not solely the responsibility of researchers to safeguard our vehicles but rather a collective effort that requires the active participation of industry stakeholders, policymakers, and the global cybersecurity community. The automotive industry must prioritize integrating robust cybersecurity measures from the earliest stages of vehicle design, ensuring that security is a foundational principle and not an afterthought.

To shape the future of automotive cybersecurity, policymakers play a critical role in developing comprehensive regulatory frameworks and standards that can guide the industry towards adopting best practices in cybersecurity. By fostering international collaboration, we can address the global nature of cyber threats, creating a unified front against adversaries who know no borders.

Moreover, the findings of this research underscore the importance of raising awareness and educating all stakeholders, including consumers, about the role of cybersecurity in protecting their digital and physical environments. Cybersecurity is not only a technical issue but also a human one. By promoting a security culture and enhancing vehicle users' cybersecurity literacy, we can empower individuals to take an active role in safeguarding their safety, privacy, and trust.

The landscape of automotive cybersecurity will continue to evolve, shaped by technological advances, societal norms, and the changing tactics of cyber adversaries. Emerging technologies such as artificial intelligence, machine learning, and

blockchain offer promising avenues for enhancing the security and resilience of automotive systems. However, they also present new challenges and ethical considerations that must be carefully navigated.

In this rapidly changing environment, the need for ongoing research, innovation, and collaboration has never been more critical. As researchers, we must remain vigilant, adaptive, and committed to advancing our understanding of cybersecurity in the automotive domain. Our efforts today have the potential to protect not only the vehicles of today but also shape the future of transportation in ways that prioritize security, privacy, and trust.

In summary, this research has been an enriching learning, challenge, and contribution journey. It has highlighted the pivotal role of cybersecurity in the automotive domain and the collective responsibility we share in advancing this crucial field. With determination, creativity, and collaboration, let us move forward, inspired by the knowledge that our efforts will contribute to a safer and more secure automotive future for all.

References

[1] Ai-generated image. Generated by artificial intelligence, 2024. No specific author or publication date.

[2] Dumarey Softronix. Vcu by dumarey softronix, 2024. Control Systems You Control.

[3] Franco Oberti, Ernesto Sanchez, Alessandro Savino, Filippo Parisi, and Stefano Di Carlo. Mitigation of automotive control modules hardware replacement-based attacks through hardware signature. In *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, pages 13–14, 2021.

[4] Franco Oberti, Alessandro Savino, Ernesto Sanchez, Filippo Parisi, and Stefano Di Carlo. Ext-taurum p2t: An extended secure can-fd architecture for road vehicles. *IEEE Transactions on Device and Materials Reliability*, 22(2):98–110, 2022.

[5] Franco Oberti, Ernesto Sanchez, Alessandro Savino, Filippo Parisi, Mirco Brero, and Stefano Di Carlo. Lin-mm: Multiplexed message authentication code for local interconnect network message authentication in road vehicles. In *2022 IEEE 28th International Symposium on On-Line Testing and Robust System Design (IOLTS)*, pages 1–7, 2022.

[6] Franco Oberti, Ernesto Sanchez, Alessandro Savino, Filippo Parisi, and Stefano Di Carlo. Psp framework: A novel risk assessment method in compliance with iso/sae-21434. In *2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, pages 60–67, 2023.

[7] Cybersecurity Research Group. Annual report on api-related cybersecurity incidents. *International Journal of API Security*, 2022. Reports a 380

[8] Researchers from University of Oxford and Armasuisse S+T. Brokenwire: A new technique for disrupting electric vehicle charging. *Journal of Cybersecurity and Mobility*, 8:101–115, April 2022. Details of a new attack technique that could disrupt EV charging at scale.

[9] The electric vehicles (smart charge points) regulations. https://www.legislation.gov.uk, June 2021. Regulations require cybersecurity measures in EV charging stations in the UK.

[10] Office of the National Cyber Director. Cybersecurity executive forum on electric vehicles and electric vehicle charging infrastructure, October 2022. Discussion on cybersecurity issues in EVs with industry and government leaders.

[11] A. Johnson. Analysis of relay attacks within vehicle communication systems. *Journal of Automotive Security*, 12:34–47, 2019.

[12] B. Smith. Emerging threats in automotive security: A comprehensive review. *Security Journal*, 33:88–102, 2020.

[13] C. Brown and Others. The use of obd in vehicle hacking. *Journal of Vehicle Security*, 14:200–215, 2021.

[14] D. Lee and E. Kim. Countermeasures against signal jamming and relay attacks in modern vehicles. *International Journal of Vehicle Safety*, 15:159–176, 2022.

[15] NIST Vulnerability Database. Cve-2022-37418 detail, 2022.

[16] Tabor's Investigation. Car thieves using fake jbl speakers to steal vehicles in just minutes, 2023.

[17] National Insurance Crime Bureau (NICB). Over 745,000 stolen vehicles reported so far in 2022, 2022.

[18] OWASP. Broken object level authorization (bola). https://www.owasp.org/www-project-api-security/.

[19] OWASP. Broken authentication. https://www.owasp.org/www-project-api-security/.

[20] OWASP. Broken object property level authorization (bopla). https://www.owasp.org/www-project-api-security/.

[21] OWASP. Unrestricted resource consumption. https://www.owasp.org/www-project-api-security/.

[22] OWASP. Broken function level authorization (bfla). https://www.owasp.org/www-project-api-security/.

[23] OWASP. Business logic flaw. https://www.owasp.org/www-project-api-security/.

[24] OWASP. Server-side request forgery (ssrf). https://www.owasp.org/www-project-api-security/.

[25] OWASP. Security misconfigurations. https://www.owasp.org/www-project-api-security/.

[26] OWASP. Improper assets management. https://www.owasp.org/www-project-api-security/.

[27] OWASP. Unsafe consumption of apis. https://www.owasp.org/www-project-api-security/.

[28] eurones. Gridlock as hackers order hundreds of taxis to same place in moscow.

[29] Bitsight. Critical vulnerabilities discovered in popular automotive gps tracking device (micodus mv720).

[30] S. Hamdare, O. Kaiwartya, M. Aljaidi, M. Jugran, Y. Cao, S. Kumar, M. Mahmud, D. Brown, and J. Lloret. Cybersecurity risk analysis of electric vehicles charging stations. *Sensors*, 23:6716, 2023.

[31] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. Demo: End-to-end wireless disruption of ccs ev charging. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, CCS '22, page 3515–3517, New York, NY, USA, 2022. Association for Computing Machinery.

[32] J. Johnson and T. Berg. Electric vehicle charger cybersecurity vulnerabilities. Encyclopedia, Year. Available online: https://encyclopedia.pub/entry/23684 (accessed on 08 January 2024).

[33] Albert Levi, Erhan Çetintas, Murat Aydos, Cetin Koc, and Mehmet Çağlayan. Relay attacks on bluetooth authentication and solutions. pages 278–288, 10 2004.

[34] Subir Halder, Amrita Ghosal, and Mauro Conti. Secure over-the-air software updates in connected vehicles: A survey. *Computer Networks*, 178:107343, 2020.

[35] Irdin Pekaric, Clemens Sauerwein, Stefan Haselwanter, and Michael Felderer. A taxonomy of attack mechanisms in the automotive domain. *Computer Standards Interfaces*, 78:103539, 2021.

[36] T.M. Corporation. Capec-1000: Mechanisms of attack, 2019. Last accessed on September 1, 2019.

[37] J. Reilly, S. Martin, M. Payer, and A.M. Bayen. Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cybersecurity. *Transportation Research Part B: Methodological*, 91:366–382, 2016.

[38] C. Yan, W. Xu, and J. Liu. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. In *DEF CON 24*, 2016.

[39] F. Sommer, J. Dürrwang, and R. Kriesten. Survey and classification of automotive security attacks. *Information*, 10(4):148, 2019.

[40] V.L.L. Thing and J. Wu. Autonomous vehicle security: A taxonomy of attacks and defences. In *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, page 164–170, 2016.

[41] B. Kitchenham, O.P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. Systematic literature reviews in software engineering–a systematic literature review. *Inf Softw Technol*, 51(1):7–15, 2009.

[42] M. Morana and S. Nusbaum. Input validation vulnerabilities, encoded attack vectors and mitigations, 2008.

[43] AUTOSAR GbR. Technical overview. Technical report, 2008.

[44] J. Andress. *The basics of information security: understanding the fundamentals of infosec in theory and practice*. Syngress, 2014.

[45] R. Piggin and H. Boyes. Safety and security-a story of interdependence. 2015.

[46] S. Parkinson, P. Ward, K. Wilson, and J. Miller. Cyber threats facing autonomous and connected vehicles: future challenges. *IEEE Trans. Intell. Transp. Syst.*, 18(11):2898–2915, 2017.

[47] NPR. 'rifle' sniffs out vulnerability in bluetooth devices. All Things Considered, Apr 2005.

[48] J. Petit and S.E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Trans. Intell. Transp. Syst.*, 16(2):546–556, 2014.

[49] V.H. La and A.R. Cavalli. Security attacks and solutions in vehicular ad hoc networks: a survey. *International journal on AdHoc networking systems (IJANS)*, 4(2):1–20, 2014.

[50] Computer standards & interfaces. *Computer Standards & Interfaces*, 78:103539, 2021.

[51] Nist national vulnerability database - cvss. https://nvd.nist.gov/vuln-metrics/cvss. Accessed on [insert access date].

[52] Cve details - cvss score distribution. https://www.cvedetails.com/cvss-score-distribution.php. Accessed on [insert access date].

[53] Accenture. Cybercrime could cost companies us $5.2 trillion over next five years, according to new research from accenture. URL: https://newsroom.accenture.com/news/cybercrime-could-cost-companies-us-5-2-trillion-over-next-five-years-according-to-new-research-from-accenture.htm, 2024. Accessed on January 24, 2024.

[54] BlackBerry Blog. Black basta: Rebrand of conti or something new? https://blogs.blackberry.com/en/2022/05/black-basta-rebrand-of-conti-or-something-new, 2022. Accessed on [insert access date].

[55] Check Point Research. Black basta and the unnoticed delivery. https://research.checkpoint.com/2022/black-basta-and-the-unnoticed-delivery/, 2022. Accessed on [insert access date].

[56] Upstream Security. Global automotive cybersecurity report. https://upstream.auto/reports/global-automotive-cybersecurity-report/, Year of Publication (if available). Accessed on [insert access date].

[57] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and Ian Jennions. Evaluation of can bus security challenges. *Sensors*, 20(8):2364, 2020.

[58] Amos Albert et al. Comparison of event-triggered and time-triggered concepts with regard to distributed control systems. *Embedded world*, 2004:235–252, 2004.

[59] EVITA Project. E-safety vehicle intrusion protected applications. https://evita-project.org/, 2008. Accessed: 2024-06-23.

[60] International Organization for Standardization. Iso 11898-2:2016 road vehicles — controller area network (can) — part 2: High-speed medium access unit, 2016.

[61] International Organization for Standardization. Iso 11898-3:2006 road vehicles — controller area network (can) — part 3: Low-speed, fault-tolerant, medium-dependent interfaceg, 2006.

[62] International Organization for Standardization. Iso/tc 22/sc 31 data communication, 2022.

[63] EPA-U.S. Environmental Protection Agency. Vehicle emissions on-board diagnostics (obd), 2009.

[64] UNECE. Transport - vehicle regulations, wltp task force on on-board-diagnostic (obd), 2012.

[65] Muhammad Umar Farooq, Muhammad Waseem, Anjum Khairi, and Sadia Mazhar. A critical analysis on the security concerns of internet of things (iot). *International Journal of Computer Applications*, 111(7), 2015.

[66] H. Khali, R. Mehdi, and A. Araar. A system-level architecture for hash message authentication code. In *2005 12th IEEE International Conference on Electronics, Circuits and Systems*, pages 1–4, 2005.

[67] Srdjan Čapkun, Mario Čagalj, Ramkumar Rengaswamy, Ilias Tsigkogiannis, Jean-Pierre Hubaux, and Mani Srivastava. Integrity codes: Message integrity protection and authentication over insecure channels. *IEEE Transactions on Dependable and Secure Computing*, 5(4):208–223, 2008.

[68] NIST. Recommendation for block cipher modes of operation: The cmac mode for authentication, 2016.

[69] M. Marchetti and D. Stabili. Anomaly detection of can bus messages through analysis of id sequences. In *2017 IEEE Intelligent Vehicles Symposium (IV)*, pages 1577–1583, 2017.

[70] Yang Xiao, Hsiao-Hwa Chen, Bo Sun, Ruhai Wang, and Sakshi Sethi. Mac security and security overhead analysis in the ieee 802.15. 4 wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*, 2006:1–12, 2006.

[71] R. B. Gmbh. Iso 11898-1:2015 road vehicles — controller area network (can) — part 1: Data link layer and physical signalling, 2015.

[72] András Gazdag, Csongor Ferenczi, and Levente Buttyán. Development of a man-in-the-middle attack device for the can bus. In *Proceedings of the 1st Conference on Information Technology and Data Science*, pages 115–130, November 2021.

[73] Pakinam Noureldeen, Marianne A. Azer, Ahmed Refaat, and Mahmoud Alam. Replay attack on lightweight CAN authentication protocol. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pages 600–606, 2017.

[74] Ken Tindell. The janus attack, 2024. Accessed: 2024.

[75] Li Yue, Zheming Li, Tingting Yin, and Chao Zhang. Cancloak: Deceiving two ecus with one frame. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021*, volume 2021, 02 2021.

[76] Omolade Ikumapayi, Habeeb Olufowobi, Jeremy Daily, Tingting Hu, Ivan Cibrario Bertolotti, and Gedare Bloom. CANASTA: Controller area network authentication schedulability timing analysis. *IEEE Transactions on Vehicular Technology*, 72(8):10024–10036, 2023.

[77] Vipin Kumar Kukkala, Sudeep Pasricha, and Thomas Bradley. Sedan: Security-aware design of time-critical automotive networks. *IEEE Transactions on Vehicular Technology*, 69(8):9017–9030, 2020.

[78] Miltos D. Grammatikakis, Nikos Mouzakitis, Lefteris Kypraios, and Nikos Papatheodorou. Dos detection on in-vehicle networks evaluation on an experimental embedded system platform. In Sergio Saponara and Alessandro De Gloria, editors, *Applications in Electronics Pervading Industry, Environment and Society*, pages 262–272, Cham, 2022. Springer International Publishing.

[79] Gedare Bloom. Weepingcan: A stealthy can bus-off attack. In *Workshop on Automotive and Autonomous Vehicle Security (AutoSec) 2021*, 02 2021.

[80] Tobias Ziermann, Stefan Wildermann, and Jurgen Teich. Can+: A new backward-compatible controller area network (can) protocol with up to 16× higher data rates. In *2009 Design, Automation & Test in Europe Conference & Exhibition*, pages 1088–1093, 2009.

[81] Anthony Van Herrewege, Dave Singelee, and Ingrid Verbauwhede. Canauth-a simple, backward compatible broadcast authentication protocol for can bus. In *ECRYPT workshop on Lightweight Cryptography*, volume 2011, page 20. ECRYPT, 2011.

[82] Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede. LiBrA-CAN: Lightweight broadcast authentication for controller area networks. *ACM Trans. Embed. Comput. Syst.*, 16(3), apr 2017.

[83] Ahmed Hazem and HA Fahmy. Lcap-a lightweight can authentication protocol for securing in-vehicle networks. In *10th escar Embedded Security in Cars Conference, Berlin, Germany*, volume 6, page 172, 2012.

[84] Jackson Schmandt, Alan T. Sherman, and Nilanjan Banerjee. Mini-mac: Raising the bar for vehicular security with a lightweight message authentication protocol. *Vehicular Communications*, 9:188–196, 2017.

[85] Jianing Luo, Chang-Ming Wu, and Ming-Hour Yang. A can-bus lightweight authentication scheme. *Sensors*, 21:7069, 10 2021.

[86] J. Heitz, S. M. Murphy, and R. S. Wilder. The AES-CMAC Algorithm. RFC 4493, June 2006. Accessed: 2024.

[87] Orlando Esparza, Wilhelm Leichtfried, and Fernando González. Transitioning applications from CAN 2.0 to CAN FD. In *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, page Page numbers, 2015.

[88] Mert D. Pesé, Jay W. Schauer, Junhui Li, and Kang G. Shin. S2-can: Sufficiently secure controller area network. In *Proceedings of the 37th Annual Computer Security Applications Conference*, ACSAC '21, pages 425–438, New York, NY, USA, 2021. Association for Computing Machinery.

[89] Andreea-Ina Radu and Flavio D. Garcia. Leia: A lightweight authentication protocol for can. In Ioannis Askoxylakis, Sotiris Ioannidis, Sokratis Katsikas, and Catherine Meadows, editors, *Computer Security – ESORICS 2016*, pages 283–300, Cham, 2016. Springer International Publishing.

[90] Takeshi Sugashima, Dennis Oka, and Camille Vuillaume. Approaches for secure and efficient in-vehicle key management. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, 9(1):100–106, 04 2016.

[91] Alan J. Michaels, Venkata Sai Srikar Palukuru, Michael J. Fletcher, Chris Henshaw, Steven Williams, Thomas Krauss, James Lawlis, and John J. Moore. Can bus message authentication via co-channel rf watermark. *IEEE Transactions on Vehicular Technology*, 71(4):3670–3686, 2022.

[92] C. Lin and A. Sangiovanni-Vincentelli. Cyber-security for the controller area network (can) communication protocol. In *2012 International Conference on Cyber Security*, pages 1–7, 2012.

[93] N. Nalla Anandakumar, Mohammad S. Hashmi, and Somitra Kumar Sanadhya. Design and analysis of fpga-based pufs with enhanced performance for hardware-oriented security. *J. Emerg. Technol. Comput. Syst.*, 18(4), oct 2022.

[94] H. Kang, Y. Hori, and A. Satoh. Performance evaluation of the first commercial puf-embedded rfid. In *The 1st IEEE Global Conference on Consumer Electronics 2012*, pages 5–8, 2012.

[95] R. Soga and H. Kang. Physical unclonable function using carbon resistor. In *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)*, pages 559–561, 2020.

[96] M. Yasin, J. J. Rajendran, O. Sinanoglu, and R. Karri. On improving the security of logic locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 35(9):1411–1424, 2016.

[97] K. Juretus and I. Savidis. Increased output corruption and structural attack resilience for sat attack secure logic locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 40(1):38–51, 2021.

[98] T. Thangam, G. Gayathri, and T. Madhubala. A novel logic locking technique for hardware security. In *2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE)*, pages 1–7, 2017.

[99] T. Nguyen, B. M. Cheon, and J. W. Jeon. Can fd performance analysis for ecu re-programming using the canoe. In *The 18th IEEE International Symposium on Consumer Electronics (ISCE 2014)*, pages 1–4, 2014.

[100] Franco Oberti, Ernesto Sanchez, Alessandro Savino, Filippo Parisi, and Stefano Di Carlo. Mitigation of automotive control modules hardware replacement-based attacks through hardware signature. In *2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S)*, pages 13–14, 2021.

[101] ISO - International Organization for Standardization. Iso 17356-2 road vehicles — open interface for embedded automotive applications — part 2: Osek/vdx specifications for binding os, com and nm, 2005.

[102] Florian Kluge, Chenglong Yu, Jörg Mische, Sascha Uhrig, and Theo Ungerer. Implementing autosar scheduling and resource management on an embedded smt processor. In *Proceedings of th 12th International Workshop on Software and Compilers for Embedded Systems*, pages 33–42, 2009.

[103] M. S. U. Alam, S. Iqbal, M. Zulkernine, and C. Liem. Securing vehicle ecu communications and stored data. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pages 1–6, 2019.

[104] Network Working Group. The aes-cbc cipher algorithm and its use with ipsec, 2021.

[105] Neal Koblitz, Alfred Menezes, and Scott Vanstone. Guide to elliptic curve cryptography, 2004.

[106] Daniel J. Bernstein. Curve25519: New diffie-hellman speed records. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006*, pages 207–228, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[107] Intrepid Control Systems, Inc. neovi fire 2 user guide, 2021.

[108] Marco Forzati. Phase modulation techniques for on-off keying transmission. In *Proceedings of 2007 9th International Conference on Transparent Optical Networks, ICTON 2007*, volume 1, pages 24–29, 08 2007.

[109] Saleh Faruque. *Amplitude Shift Keying (ASK)*, pages 45–55. springer, 01 2017.

[110] Tobias Ziermann, Stefan Wildermann, and Jurgen Teich. Can+: A new backward-compatible controller area network (can) protocol with up to 16× higher data rates. In *2009 Design, Automation & Test in Europe Conference & Exhibition*, pages 1088–1093, 2009.

[111] Bogdan Groza, Stefan Murvay, Anthony van Herrewege, and Ingrid Verbauwhede. Libra-can: A lightweight broadcast authentication protocol for controller area networks. In Josef Pieprzyk, Ahmad-Reza Sadeghi, and Mark Manulis, editors, *Cryptology and Network Security*, pages 185–200, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[112] Pakinam Noureldeen, Marianne A. Azer, Ahmed Refaat, and Mahmoud Alam. Replay attack on lightweight can authentication protocol. In *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pages 600–606, 2017.

[113] Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, and Ingrid Verbauwhede. Libra-can: Lightweight broadcast authentication for controller area networks. *ACM Trans. Embed. Comput. Syst.*, 16(3), apr 2017.

[114] Daniel J. Rogers, Tim C. Green, and Richard W. Silversides. A low-wear onload tap changer diverter switch for frequent voltage control on distribution networks. *IEEE Transactions on Power Delivery*, 29(2):860–869, 2014.

[115] LTSpice.

[116] Miyuki Mizoguchi, Hiroyuki Mori, Noboru Maeda, Hiroki Keino, Takashi Yasuda, and Hideki Goto. Alternative technique to estimate the immunity performance for in-vehicle ethernet. In *2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, volume 01, pages 703–705, 2016.

[117] Dong Zhang, Shaokun Zhang, Tao Fan, and Xuhui Wen. Modeling and estimation for conducted common-mode interference of a motor drive system used in electric vehicle. In *2018 21st International Conference on Electrical Machines and Systems (ICEMS)*, pages 831–835, 2018.

[118] Zhai Li, Dong Shouquan, Zhang Chengning, and Wang Zhifu. Study on electromagnetic interference restraining of electric vehicle charging system. In *2011 4th International Conference on Power Electronics Systems and Applications*, pages 1–4, 2011.

[119] Claudius Pott, Philipp Jungklass, David Jacek Csejka, Thomas Eisenbarth, and Marco Siebert. Firmware security module. *Journal of Hardware and Systems Security*, 5(2):103–113, 2021.

[120] Robert Bosch Engineering and Business Solutions and ETAS GmbH. BUSMASTER: An Open Source Software Tool for Simulation, Analysis, and Testing of Data Bus Systems. https://rbei-etas.github.io/busmaster/, 2024. Accessed: 2024-03-11.

[121] Shivang Agrawal and R. S. Kanchan. Carrier phase shift modulation for reducing the common mode voltage in a two-level three-phase inverter. In *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, pages 1067–1072, 2018.

[122] RFC. Internet security glossary, version 2, 2007.

[123] Felipe Paez and Hector Kaschel. Towards a robust computer security layer for the lin bus. In *2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA)*, pages 1–8, 2021.

[124] Junko Takahashi, Yosuke Aragane, Toshiyuki Miyazawa, Hitoshi Fuji, Hirofumi Yamashita, Keita Hayakawa, Shintarou Ukai, and Hiroshi Hayakawa. Automotive attacks and countermeasures on lin-bus. *Journal of Information Processing*, 25:220–228, 02 2017.

[125] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, and Prakash Ranganathan. Cybersecurity challenges in vehicular communications. *Vehicular Communications*, 23:100214, 2020.

[126] Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, and Richard R. Brooks. Chapter 6 - security and data privacy of modern automobiles. In Mashrur Chowdhury, Amy Apon, and Kakan Dey, editors, *Data Analytics for Intelligent Transportation Systems*, pages 131–163. Elsevier, 2017.

[127] Alfonso Martínez-Cruz, Kelsey A. Ramírez-Gutiérrez, Claudia Feregrino-Uribe, and Alicia Morales-Reyes. Security on in-vehicle communication protocols: Issues, challenges, and future research directions. *Computer Communications*, 180:1–20, 2021.

[128] HACKADAY. Embed with elliot: Lin is for hackers, 2022.

[129] European Counsil. Fit for 55, 2023.

[130] International Organization for Standardization. Iso/sae 21434:2021 road vehicles — cybersecurity engineering, 2021.

[131] International Organization for Standardization. So 26262-1:2018road vehicles — functional safety, 2018.

[132] Quality Management in the Automotive Industry. Automotive spice, 2015.

[133] Aljoscha Lautenbach, Magnus Almgren, and Tomas Olovsson. Proposing heavens 2.0 – an automotive risk assessment model. In *Proceedings of the 5th ACM Computer Science in Cars Symposium*, CSCS '21, New York, NY, USA, 2021. Association for Computing Machinery.

[134] Upstream. Global automotive cybersecurity report, 2023.

[135] Marko Wolf. *Attackers and Attacks in the Automotive Domain*, pages 77–89. Vieweg+Teubner, Wiesbaden, 2009.

[136] Vinh LA. Security attacks and solutions in vehicular ad hoc networks: A survey. *International Journal on AdHoc Networking Systems (IJANS)*, Volume 4:1–20, 04 2014.

[137] Mehmet Bozdal, Mohammad Samie, Sohaib Aslam, and I.K. Jennions. Evaluation of can bus security challenges. *Sensors*, 20:16–17, 04 2020.

[138] Simon Greiner, Maike Massierer, Claudia Loderhose, Bernd Lutz, Frederic Stumpf, and Franziska Wiemer. A supplier's perspective on threat analysis and risk assessment according to iso/sae 21434. In *20th escar Europe - The World's Leading Automotive Cyber Security Conference (15. - 16.11.2022)*. 2022.

[139] Sergej Japs, Frank Kargl, Harald Anacker, and Roman Dumitrescu. Why make it hard? - usage of aggregated statistical data for risk assessment of damage scenarios in the context of iso/sae 21434. *Procedia CIRP*, 109:293–298, 01 2022.

[140] Yousik Lee and Samuel Woo. Can signal extinction-based dos attack on in-vehicle network. *Security and Communication Networks*, 2022:1–10, 09 2022.

[141] Adnan Akhunzada, Mehdi Sookhak, Nor Badrul Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, and Muhammad Khurram Khan. Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48:44–57, 2015.

[142] Nevrus Kaja. *Artificial intelligence and cybersecurity: Building an automotive cybersecurity framework using machine learning algorithms*. PhD thesis, 2019.

[143] Elies Gherbi. *Machine learning for intrusion detection systems in autonomous transportation*. PhD thesis, 07 2021.

[144] Andre Luckow, Ken Kennedy, Marcin Ziolkowski, Emil Djerekarov, Matthew Cook, Edward Duffy, Michael Schleiss, Bennie Vorster, Edwin Weill, Ankit Kulshrestha, and Melissa C Smith. Artificial intelligence and deep learning applications for automotive manufacturing. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 3144–3152, 2018.

[145] Luca Bertoglio, Valentina Penso, and Cosimo Senni Guidotti Magnani. Machine learning and artificial intelligence boosting automotive threat intelligence. 2022.

[146] Jun Zhao, Qiben Yan, Jianxin Li, Minglai Shao, Zuti He, and Bo Li. Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security*, 95:101867, 2020.

[147] Adnan Akhunzada, Mehdi Sookhak, Nor Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, and Khurram Khan. Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48, 11 2014.

[148] Twitter, Inc. Twitter API, 2023.

[149] Shiho Kim. *Automotive cyber security : introduction, challenges, and standardization*. Springer, Cham, Switzerland, 1st ed. 2020. edition, 2020.

[150] Naning Fatmawatie. Implementation of break event point analysis and margin of safety in profit planning. *Idarotuna : Journal of Administrative Science*, 2:132–146, 12 2021.