Silesian
University
of Technology

Department of fundamentals
of machinery design

Doctoral Thesis

Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept

Author: MSc. Eng. Marcin Gajdzik

Supervisor: Ph.D. D.Sc. Eng. Anna Timofiejczuk, Associate Professor

Industry supervisor: Ph.D. Eng. Wojciech Sebzda

Gliwice, 2023

This dissertation represents the culmination of several years of highly intensive effort, numerous iterations, and setbacks, all of which have enabled me to identify the vulnerabilities in the initial assumptions. These challenges have only empowered my determination to revisit the subject with even greater motivation. The scope of this work intertwines several facets of my passions, namely, the automotive industry, cybersecurity, and the practical application of artificial intelligence.

I extend my appreciation to the Dräxlmaier Company for their support. I would also like to extend my gratitude to Ph.D. Eng. Wojciech Sebzda, my industry supervisor, for his invaluable support and exemplary professionalism. I would also like to express my sincere thanks to Ph.D. Eng. Marek Sznura, who encouraged me to take up the challenge of this academic journey 4 years ago. I would also like to express my appreciation to my fellow colleague MSc. Eng. Kamil Sternal, a PhD student, for his support, dedication, and sharing expertise.

I reserve a special acknowledgment for my PhD dissertation supervisor, Ph.D. D.Sc. Eng. Anna Timofiejczuk, Associate Professor, without whose guidance, this work would not have yielded such substantial outcomes. Thank you for your continuous refinement of research results and the accomplishments achieved. My profound thanks also go to Ph.D. D.Sc. Eng. Piotr Przystałka, Associate Professor, whose invaluable support and knowledge sharing significantly enhanced the quality of the proposed solution.

Furthermore, I wish to convey my gratitude to my family, particularly my wife, for her unwavering support, patience, and valuable tips.

Marcin Gajdzik

Gliwice, September 2023

Contents

List of important abbreviations

List of important abbreviations

ABS - Antilock Brakes System

ADAS - Advanced Driver Assistance Systems

AE - Auto Encoder

AES256 – Advanced Encryption Standard 256

AI - Artificial Intelligence

BILSTM - Bidirectional Long-Short Memory

CAN - Controller Area Network

CAN FD - Controller Area Network Flexible Data

CRC - Cyclic Redundancy Check

DNN - Deep Neural Network

E2E - End-to-End Protection for CAN transmission

ECC – Elliptic Curve Cryptography

ECU - Electronic Control Unit

ESC - Electronic Stability Control

GPS – Global Positioning System

GRU - Gated Recurrent Unit

GRU-AE – Gated Recurrent Unit – Autoencoder

HMAC – key-Hash Message Authentication Code

IoT - Internet of Things

IoV - Internet of Vehicles

LED – Light-Emitting Diode

LSTM - Long Short-Term Memory

MAC – Message Authentication Code

ML – Machine Learning

NLP – Natural Language Processing

PC – Personal Computer

PKI – Public Key Infrastructure

PWM – Pulse Width Modulation

ReLu – Rectified Linear unit

RNN - recurrent Neural Network

RSA – Rivest-Shamir-Adleman

SHA2 – Secure Has Algorithm 2

TCS - Traction Control System

TW – Time Window

UDS – Unified Diagnostic services

V2I - Vehicle To Infrastructure

V2N - Vehicle To Network

V2P - Vehicle To Pedestrian

V2V - Vehicle To Vehicle

V2X - Vehicle To Everything

VRU - Vulnerable Road Users

XOR – Exclusive or

Chapter 1

Introduction

The chapter is dedicated to presenting the research background, objectives, and plan. There were also characterized the author's outlines the motivations behind embarking on the research endeavor. An overview of potential risks within the area of embedded systems in the automotive industry were discussed. The section also underscores the significance of cybersecurity in present days, particularly when considering the context of multi-data processing within vehicle technology.

1.1 Research background

In the era of grooming automation, electromobility and increasing use of the Internet, in particular IoT (Internet of Things) and Indystry4.0 era, one of the most important priorities in the industry is to identify threats that may arise in embedded systems. Such systems are especially widespread in the automotive industry. In cars they are used during their regular operation in road traffic, gathering and processing big amount of data. Nowadays, attacks on such systems are observed increasingly. To protect the vulnerable data and ensure passengers safety, it is necessary to develop and implement approaches aiming at eliminating or at least minimizing treats of attacks.

Contemporary cars are examples of applications of technologies related to the "Industry 4.0" concept, where the focus is put on integration of modern technologies, involved in the intelligent control of an increasing number of modules that communicate with each other. All efforts are aimed at controlling all possible elements and processes in a car using electronic modules connected with each other by means of connectors known as buses. The Internet of Things, being the fundamental approach in Industry 4.0 concept, has been developing rapidly in recent years in the automotive sector. It also plays an important role. New technologies bring many conveniences and new opportunities. Unfortunately, it is also related to several potential risks such as:

- possibility of data theft
- destabilization of car (or any mechatronic device) operation
- taking control over the vehicle (or any mechatronic device).

Considering these risks, the embedded systems controlling the car can directly or indirectly affect human health and even life. The consequences of losing control can be very serious.

It is important to stress that electric cars, which are powered by batteries storing large amounts of energy, are becoming increasingly popular. Voltages are hundreds of volts. In case of these cars, it is possible to predict a scenario when through the lack of an adequate protection of the control module, the car can be used for an improper purpose. That is why it is necessary to be aware of the possibility of the attack on the car's built-in control systems and to use such safeguards which ensure safety of users. There are different kinds of attacks and in the most serious form it can immobilize the vehicle. It should be stressed that it is not possible to elaborate complete and sure protection against all forms of attacks, since new technologies bring also new forms of attacks. Dangerous situations, caused by attacks, are mostly related to taking control over selected modules such as a braking system and destabilization of a car operation.

Contemporary cars, as mechatronic systems, collect increasingly more and more data and information about their users. Examples are favorite usage settings, most frequently chosen routes or certain measurements allowing to control the driver's psychophysical condition. All this data is stored in the device memories. This data are very important for various reasons and cannot be allowed to be stolen.

A manufacturing company that implements the correct procedures following current low, should deliver such product (in terms of any mechatronic system) that is resistant to modern threats (including cyber threats). It is particularly important in the automotive industry. As it was concluded above, it is impossible to be sure that the car is always protected against every form of attacks. New types and ways of threats are constantly emerging. Therefore, what is important, is creating solutions which make it possible to protect not only against known threats but also against treats that are not known currently. The goal of the thesis was to develop procedures and guidelines, which include outlined directions for further action. It is important to be ready, in sense of being aware that new threats would appear, which we are also supposed to cope with. It seems that a right direction is the use of artificial intelligence systems implemented in cars and supervising the traffic on the vehicle's buses. It let us constantly monitor whether there are anomalies in transmissions between modules built into the vehicle. An additional motivation to conduct research on the presented topic is the development of autonomous cars, where safety issues are placed at the highest level, similarly to the aviation industry.

1.2 Research objectives

The main objective of the research included in the thesis is to identify potential threats in embedded systems used in automotive and develop solutions to prevent them. One of the main aspects of the research is to elaborate a method of low-cost encryption that minimizes a possibility of destabilization the car operation.

An important aspect of the research is to identify a possibility to implement approaches based on artificial intelligence to identify threats, which are recognized on the basis of anomalies. In the vehicle such symptoms can be considered as a potential risk to regular car operation. It is particularly important in areas where electronic systems and software have an impact on the maintenance, and technical state of mechanical parts of the car.

1.3 Research plan

The presented work is a result of research supported by the Polish Ministry of Education and Science, Grant No.: DWD/3/33/2019, under which the following plan was adopted and implemented:

- a review of current solutions in embedded systems in automotive industry
- analysis of current threats, including cyber threats
- selection of specific embedded systems
- developing an own research/testing concept aimed at destabilizing the regular operation of systems, including attempts to completely disable regular operation and take control of the system
- preparation of test bench
- carrying out verification tests
- the development of a concept of safeguards to minimize the hazards arising from the types of risks tested
- performing verification tests after implementation of the developed safeguards
- development of a concept of the CAN bus supervisor, with using artificial intelligence methods
- preparing proposals and solutions to better protection of the vehicle's built-in systems against threats
- outline directions for further analysis and research.

Chapter 2
State-of-the-art

The chapter describes the designing process of a contemporary car vehicle. The description is based on a comparison to the past approaches. The author indicates directions of car systems development, which have morphed from mechanic to mechatronic ones. The chapter lists the potential hazards to car systems, as a not secured gaps to cyber-attack. Based on the analyzed literature the possible types of cyber-attacks are enumerated, as well as exemplary successful performed attacks on the cars are characterized. Additionally, the chapter extends its examination of the literature to explore the current security measures employed in automobiles. The author provides a discussion on the protective methods. Finally, the last section of the chapter illustrates specific applications of artificial intelligence within the automotive industry.

2.1 Mechatronic car vehicles designing

The idea of a vehicle with its own power source, able to take people or goods on board, had always been a dream that humanity has been striving for. The beginnings of self-powered machines date back to times of the first industrial revolution, when a steam-powered engine was developed, which powered the first steam locomotives. This can be considered a breakthrough in land transport, since huge amounts of goods could be transported for very long distances. Parallelly to the public land transport the automotive industry had been developing. It was especially aimed at manufacturing personnel vehicles. It gave a lot of independence in travelling at lower costs of preparing road infrastructure. The history of automotive industry dates to the end of the 19th century and the invention of the first internal combustion engine that was installed in a vehicle. These vehicles were complex mechanical structures. The operations of all basic modules responsible for driving, braking, and turning were based solely on mechanical systems.

It should be stressed that in the early 20th century, electric cars were also quite popular, especially in the United States. They had a limited range of distance, but due to their advantages such as noiseless engine operation, no exhaust fumes, and no need to start with a mechanical hand-crank, they were especially popular among women. Contrary to contemporary electric cars they were completely mechanically controlled vehicles.

2.1.1 Contemporary car vehicles

In the early phase of the development of the automotive industry, motor vehicles were controlled entirely mechanically. However, with its development, there was a gradual change involving the integration of electronics and car control, thus increasing the share of mechatronic systems in favor of mechanics. The main elements of mechatronic system are shown in Fig. 1.

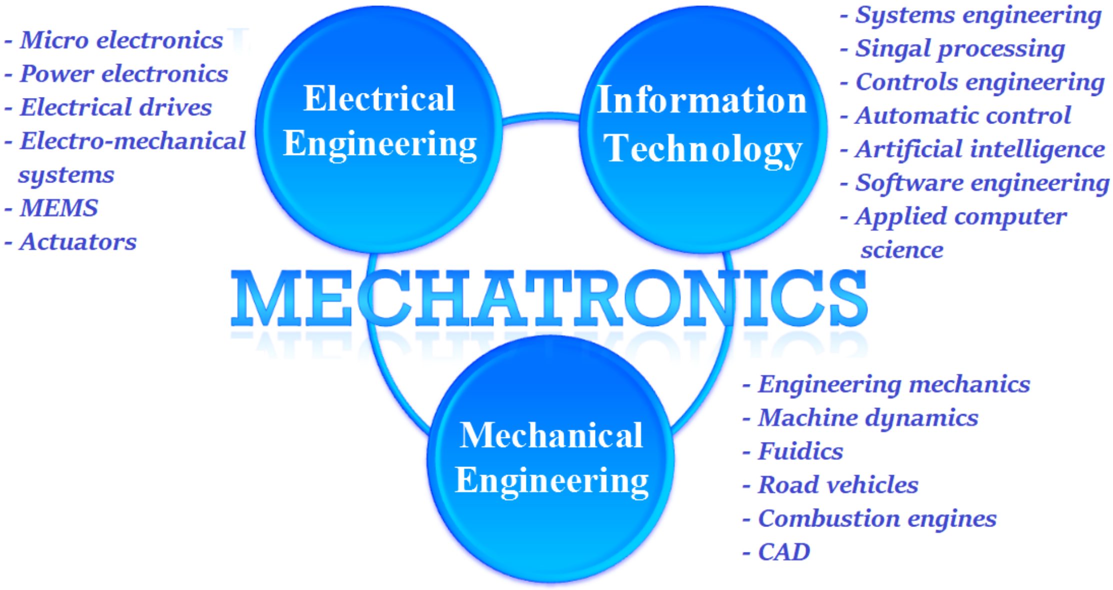


Fig. 1 Integration of mechatronic system

(The course of studies in Mechatronics, 2023)

This gradually introduced change, from mechanic to mechatronic systems, was driven by the higher and higher requirements related to better performance, greater comfort, and safety as well as optimization of fuel consumption. Thus, typically mechanical elements were gradually replaced with electronically controlled ones. The main functionalities and fundamental elements of a contemporary car are shown in Fig. 2 and Fig. 3.

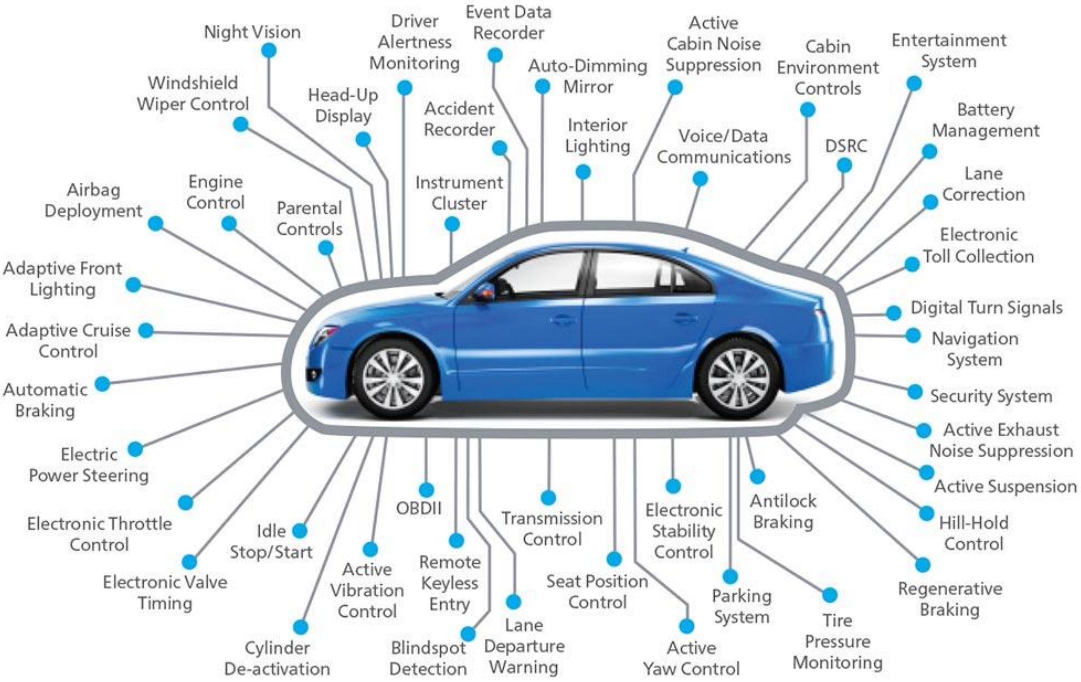


Fig. 2 Main functionalities of contemporary cars

(Asfa, 2023)

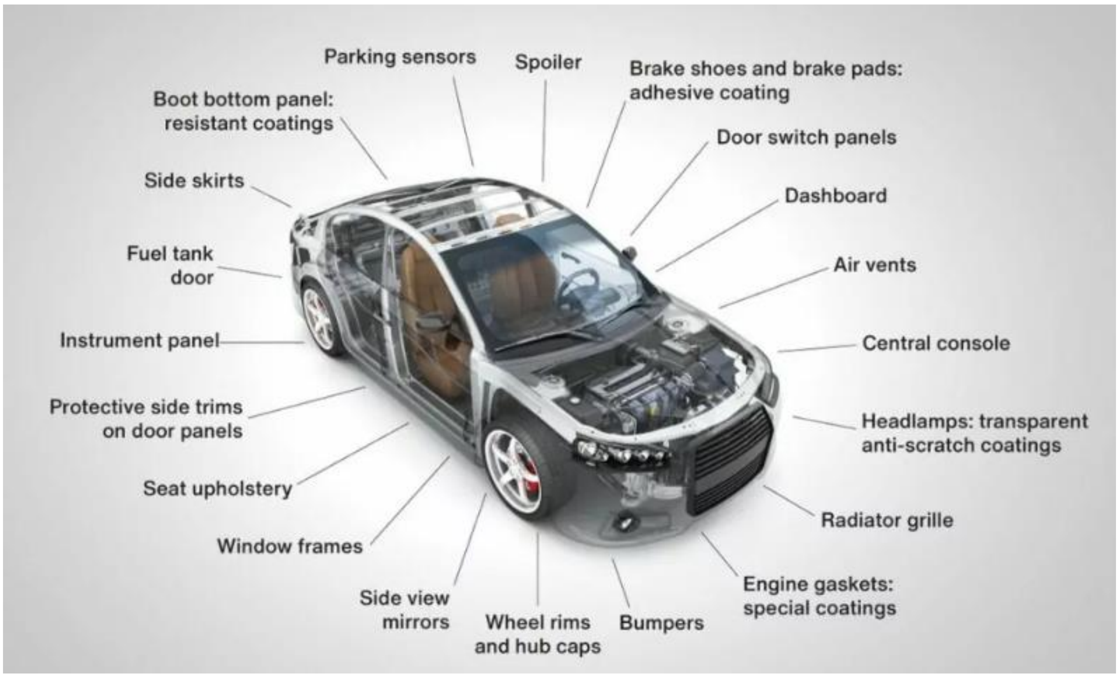


Fig. 3 Main elements of contemporary cars

(Asfa, 2023)

Typical examples of initially mechanical and today mechatronic system are the turning and braking (handbrake example) systems. They are two basic vehicle control modules.

The typical mechanical handbrake system, shown in Fig. 4, was responsible for the ability to lock the rear wheels to prevent the vehicle from moving at parking mode. In the past it was a system of connections with steel cables and regulators responsible for even distribution of braking force on both rear wheels. Importantly, the performance of the brake had to be also optimized in terms of functionality, so that a lot of force was not required to use it. Its activation requires the driver's reaction. The lever must be pulled, and above all, the driver must remember about it. The mechanical handbrake is controlled solely by the driver. The advantage of such solution is the ability to manually set the braking force and the ability to use it when trying to get out of a sideslip.

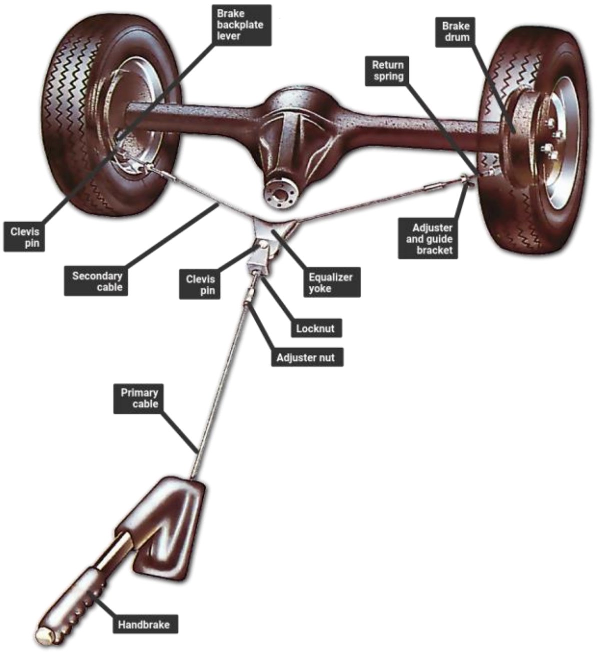


Fig. 4 Mechanical handbrake system in a car

(Muir, 2023)

The successor to the mechanical handbrake is the electronic parking brake (sometimes called the electromechanical parking brake), which is an advanced mechatronic system. It is controlled by signals sent via transmission buses, so there is no need to use the wire connecting the front and rear of the vehicle. The solution is shown in Fig. 5.

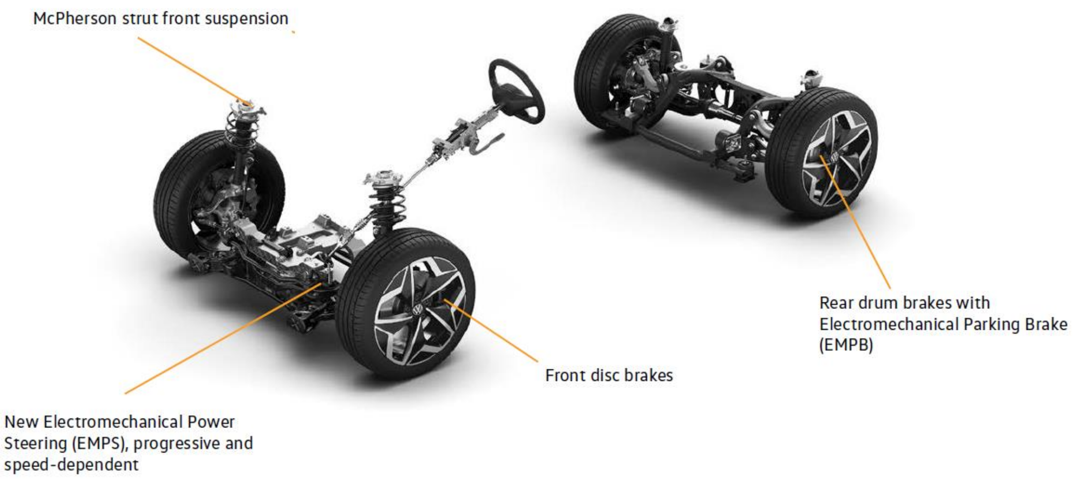

McPherson strut front suspension
Rear drum brakes with Electromechanical Parking Brake (EMPB)
Front disc brakes
New Electromechanical Power Steering (EMPS), progressive and speed-dependent

Fig. 5 Electronic parking brake

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

An exemplary executive system with an actuator is shown in Fig. 6.

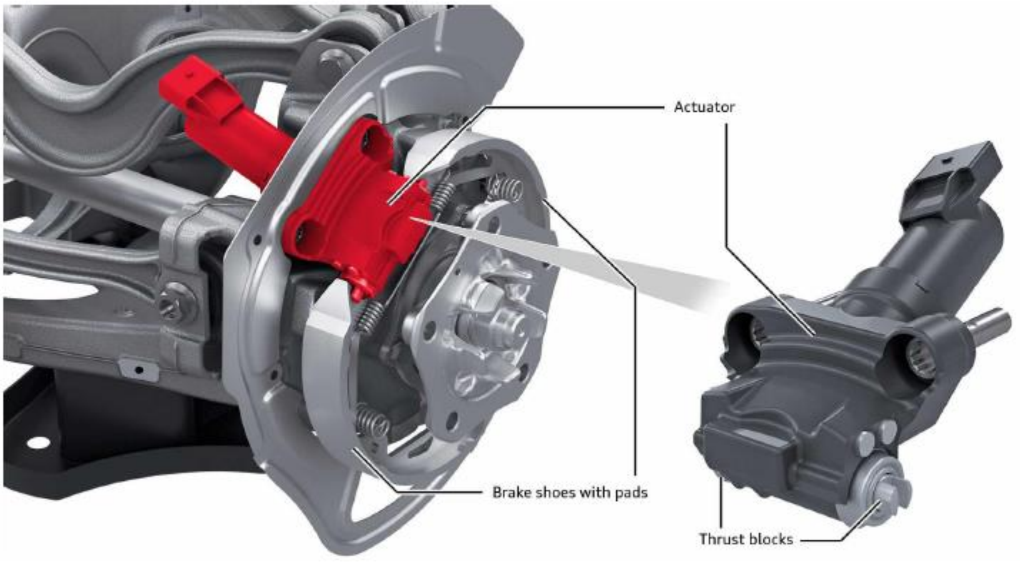


Fig. 6 Brakes executive system with an actuator

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

The possibility of electronic control of the parking brake also increases its range of possibilities, including the possibility of:

- locks on all wheels (not just one axle),
- control automation, activation/deactivation can be done as a result of an action taken by the driver by pressing the button in the center console or by the vehicle control system
- emergency braking using the electromechanical parking brake module.

Another example of the transformation of mechanical systems into mechatronic ones is steering the control system. This system, next to the driving/acceleration and braking systems, plays one of the most fundamental functions in car operation. The implementation of this system is mostly related to the vehicle motor. At early stages of the development of the automotive industry, the design of the steering system responsible for the turning function was also solely mechanical. In case of mechanical solution, the steering wheel is connected to the steering column, which connects the steering wheel to the shaft, which in turn transmits its movements to the steering gear. This solution ensures the required safety, because after the loss of power or hydraulic support, it is still possible to turn the wheels in the car.

The consecutive mechatronic generations of the steering systems are to steer by wire. In this concept there is no mechanical connection between the steering wheel and the transmission. The steering shaft is replaced with signal wires which connect the steering column to the steering gear that is physically controlled by an electric motor.

The concepts of both the braking system control solutions are presented in Fig. 7. The version A means the mechanical and version B means the mechatronic control system.

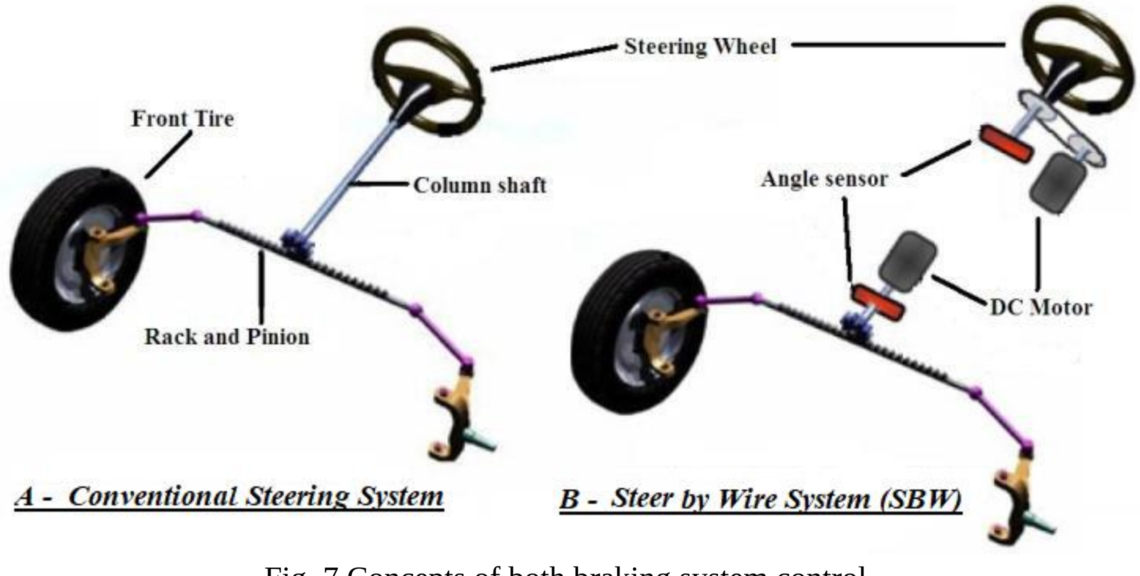


Fig. 7 Concepts of both braking system control

(Fahami, Zamzuri, Mazlan, & Zulkarnain, 2013)

It should be emphasized that in contemporary cars, mechatronic systems constitute a major part of the control systems. Without them, taking into account user demands, it is difficult to achieve the implementation of the required vehicle functionality. These include, among others:

- Electronic ignition system – system responsible for supply the voltage to the sparking plugs of an internal-combustion engine,
- Antilock brakes system (ABS) – system that protects the vehicle from locking the wheels during heavy braking
- Traction control system (TCS) – system included in the group of Advanced Vehicle Control Systems, whose main task is to prevent excessive slip of the vehicle wheels during acceleration, manifested by their spinning. The traction control system is part of the Electronic Stability Control (ESC) system
- Cruise Control system – system which allows to maintain a set speed without using the accelerator
- Active suspension system – system responsible for keeping the road, ensuring stability and comfort while driving thanks to the continuous adjustment of the suspension damping to the road conditions
- Airbag system – system responsible for protecting the head and chest of the driver and passengers in the event of a frontal collision
- Door locking system – system responsible for locking and unlocking the door. In addition to the standard operations of opening and closing the vehicle using a remote key or key, it manages automatic locking after exceeding a certain speed or unlocking in case of an accident.

2.1.2 Current directions of development of mechatronics systems in cars

A modern car vehicle contains a significant number of mechatronic modules and elements that cooperate to optimize performance or increase safety and driving comfort. Nowadays, mechatronics plays a key role in the process of transforming vehicles into intelligent and efficient means of transport, ranging from engine management, optimization of automatic transmissions to the development of advanced driver assistance systems. Currently, in the automotive industry, significant emphasis is placed on the development of data and information interoperation and entertainment systems. This is primarily aimed at increasing travel safety, considering the drivers' demands to rest and find themself better in the current road conditions. The expectations of the car market regarding the near future focus primarily on the areas of increasing resistance to cyberattacks. It should be stressed that the integration of cars with Internet of Things systems according to the concept of Industry 4.0 brings many new opportunities and facilities, but also many hazards to which the car must be resistant. The pursuit of cost optimization and full automation is related to the development of autonomous cars driving faster and faster. According to bibliography and automotive market reviews the main goals in development of mechatronics systems in cars are aimed at:

- Autonomous driving, which is one of the most significant advances in mechatronics. The goal is to create the possibility of fully autonomous driving, which is at the level five in the five-point scale of autonomy. Currently, some manufacturers are beginning tests at the third level of autonomy, i.e., under certain conditions the driver can give up driving the vehicle and the vehicle subsystems control it themself. The rush to achieve higher and higher levels of autonomy is also possible thanks to the rapid development of mechatronic components, such as advanced sensors (LiDAR, radar, cameras), efficient processors and sophisticated control algorithms. They enable vehicles to navigate in real time and make decisions without human intervention. Achieving full autonomy in driving is undoubtedly going to revolutionize transport, making it safer, more efficient, and accessible to everyone, due to the possibility of replacing the driver with algorithms.
- Electrification and energy efficiency, which is related to the need to increase the current range, and thus to supply more and more energy to battery-powered electric vehicles as well as hybrids. It is also a factor that is undoubtedly going to significantly affect the development of the battery systems. This involves the need for continuous improvement and integration of mechatronic systems. Battery management systems become more efficient, optimizing energy consumption, and extending the range of electric vehicles. In addition, mechatronics also plays a key role in the development of regenerative braking systems, making cars more energy efficient.
- Continuous ADAS improvement – Advanced Driver Assistance Systems (ADAS), presented in Fig. 8, is also continuously evolving. Thanks to this, the ADAS system is able to better predict potential road hazards, provide more precise interventions and offer advanced features such as advanced pedestrian detection, predictive collision avoidance and traffic pattern analysis. In this aspects mechatronics also contributes since it is possible to implement artificial intelligence approaches, including deep learning capabilities to make the car

operation more precise.

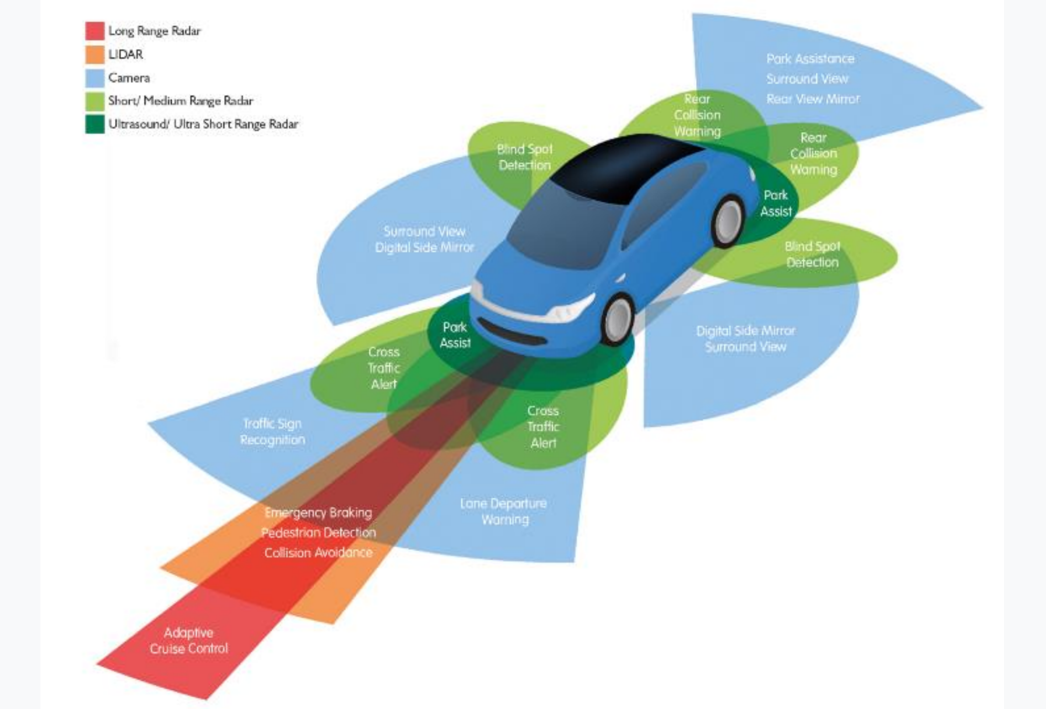


Fig. 8 Advanced Driver Assistance Systems

(Advanced Driver Assistance Systems (ADAS), 2023)

- Predictive maintenance and health monitoring, which is also related to the application of mechatronic systems. They enable real time monitoring by the car itself and determine the technical state with the use of sensors and built-in diagnostics procedures. Predictive maintenance algorithms analyze the data and proactively alert drivers about potential risks and malfunctions, enabling timely repairs and minimizing downtime and keeping the vehicle in top working order.
- Personalization and User Profiles implemented with the use of mechatronic systems enable the adaptation of cars to individual preferences of drivers through personalized user profiles. It is especially expected during long journeys when driver comfort is extremely important. The personalization of settings, from the position of the seats, the height of the headrests, adjusting the angles of the mirrors, through the preferred parameters of the air conditioning and ending with the infotainment system, is a key factor affecting the safe driving. The innovative concept of enabling the engine power configuration using software parameters, opens new marketing opportunities of the service market. It is assumed that soon such service as purchasing a subscription for an improved configuration of the car in a specific period is going to be possible.

- Cybersecurity and Over-the-Air Updates in cars, which are connected to data collection systems is also related to the key role of mechatronics. This aspect of car operation should ensure robust cybersecurity. Carrying out the attack on mechatronic control systems may turn out to be so problematic that the driver loses the ability to continue driving. It should be emphasized that a huge threat is not only taking over control, but also effectively destabilizing the regular operation of the car.

  Advanced encryption methods and intrusion detection systems are going to be integrated into the mechatronic architecture to protect against potential cyber threats. It is possible that the vehicle architecture is extended with additional devices checking whether there would be an attack on the communication buses. Changing some parameters of mechatronic control systems is possible by means of wireless software updates. It allows the continuous improvement and implementations of new functionalities and protections without the need of visit the vehicle service.

2.1.3 Rapidly evolving road infrastructure technologies using mechatronic approaches

For very long time, the road transport was based on similar and unchanged means. Regardless of it concerned the transport of people or goods. The elements of the transport environment and infrastructure described in (Miyata, 2018), i.e., the driver, car, and road, were solely managed by people. The rapid progress in mechatronic technologies, and also new possibilities of integrating technologies according to the Industry 4.0, have made it possible to connect the elements of transport environment with the use of digital data exchange approaches. As the result, the traffic infrastructure is possible to be managed not only by people, but also by modern information technologies including methods based on the artificial intelligence. Thus, the digital transformation, which is a part of the fourth industrial revolution (Industry 4.0), had brought completely new opportunities for the road transport. Moreover, the introduction of the Internet of Things concept enabled the implementation of many functionalities that significantly increase safety while driving a car and increase the comfort of its use. Nowadays, driving a car is possible to check such information as the road state, traffic jams, or collisions. The cooperation of systems and sensors, which the car is equipped with allows the vehicle to react quickly to different situations that may happen. Therefore, the improvement and further development of all collision avoidance mechanisms is strongly expected. Devices and approaches such as radars or cameras have been known for a long time, but they were usually implemented locally, and used to a single vehicle. The idea of connecting the entire available road infrastructure brings a significant change. The collected information can be combined and analyzed together and then used in real time to manage the road traffic environment, as shown in Fig. 9. Nowadays, these vehicular communication systems are seen as parts of bigger eco-systems following the idea of Industry 4.0. In case of the automotive industry, they include such approaches as V2X, V2V, V2I, V2N and V2P.

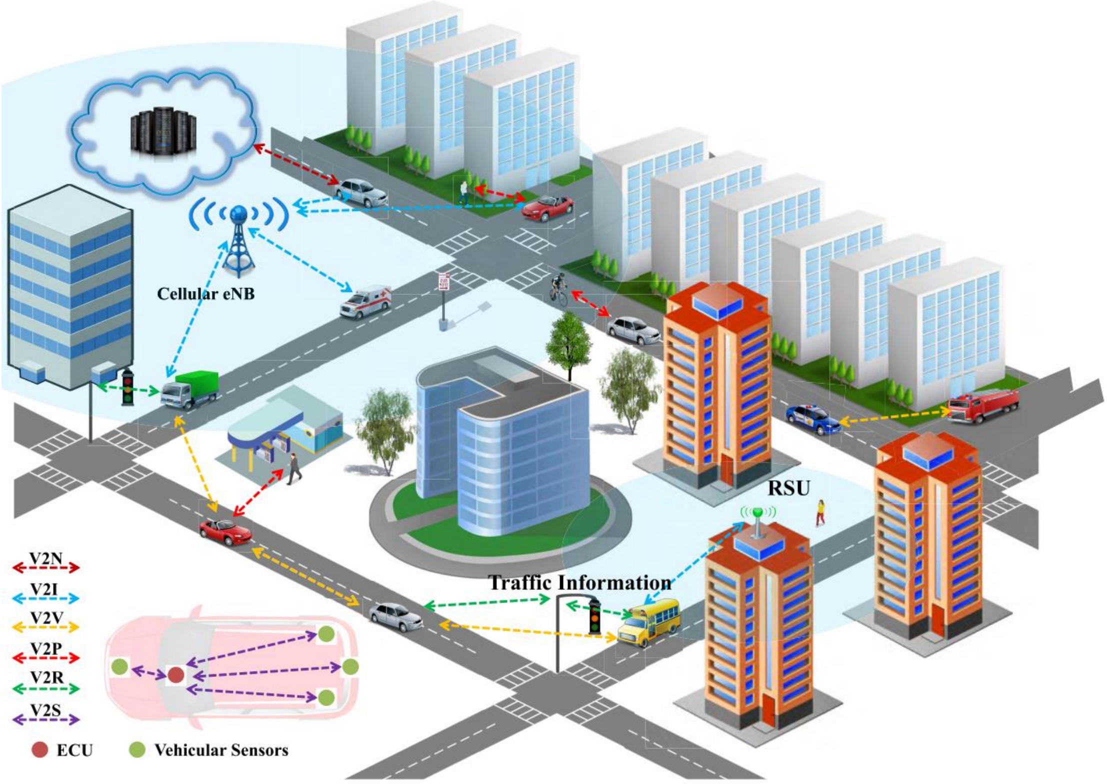


Fig. 9 An overview of V2X scenario following ideas of the Industry 4.0

(Tong, Hussain, Bo, & Maharjan, 2019)

Vehicle to everything (V2X)

V2X, also known as a vehicle to everything, covers all V2V and V2I and V2N and V2P technologies, as shown in Fig. 10. V2X technology assumes that every vehicle on the road is equipped with the ability to communicate with the road infrastructure. As described in (Aries, 2021) V2X can notify drivers about all kinds of dangerous situations, such as accidents and traffic jams nearby and other dangerous behavior in the vicinity of the vehicle. The V2X system is also used to manage services such as toll or parking automation. Undoubtedly, widely understood V2X communication is the basis for autonomous safe driving. This type of communication carries a very large potential for possibilities and the development of new functionalities for the future. However, at the same time it is associated with the risk of cyberattacks aimed at this system. In (Nowdehi, Automotive Communication Security Methods and Recommendations for Securing In-vehicle and V2X Communications, 2019) the authors presented a discussion on risks associated with exposing a safety-critical integrate system to an external network and propose methods and recommendations to improve the security. Therefore, it seems necessary to create and use two-way transmission supervision with using artificial intelligence methods. Such approach makes it possible to watch over the security of such a critical system in real time. The maintenance of the system is based on detection of an anomaly, which could be a symptom of an ongoing attack. The results of the system operation, and especially the way they are interpreted and presented to the user make it possible to elaborate approaches based on augmented intelligence. Such approach is understood as the implementation of artificial intelligence methods that are focused on presenting possible ready solutions to the user, who is supposed to select the preferable one. The most important factor in the applications of augmented intelligence is the fact that the final decision is always undertaken by the user. As pointed out by (Wang, Shao, Ge, & Yu, 2019) prior to marketization, the reliability and maturity of technology must be ensured. Therefor testing is an important part of V2X technology.

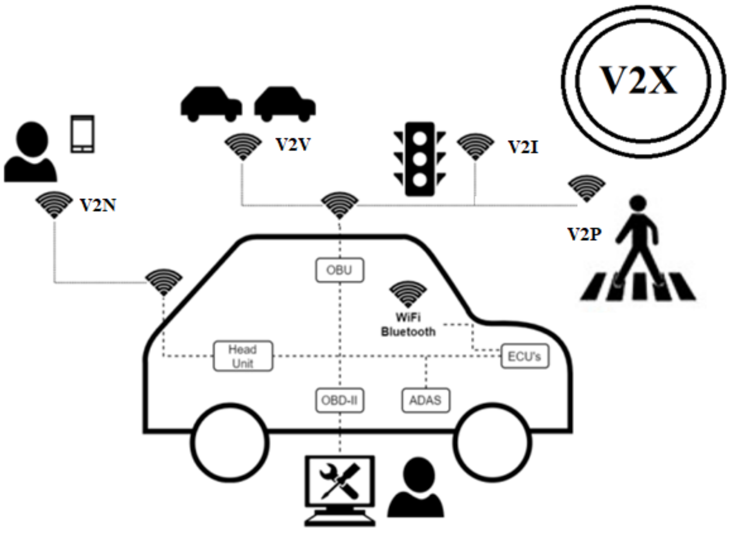


Fig. 10 Vehicle to everything infrastructure (V2X) in a concept of the Industry 4.0

Vehicle to Vehicle (V2V)

Vehicle-to-vehicle communication technology, commonly known as V2V, enables two-way data and information exchange between vehicles. It is based on dedicated short-range DSRC communication. The main goal of this approach is a possibility to effectively avoid collisions between vehicles on the road. For a motor vehicle, information about the position and speed of other vehicles that are also equipped with V2V is available using a wireless communication protocol. The collected data can be used to warn drivers of potential hazards, which in turn reduces the likelihood of a collision or congestion on the road. The range of this system is estimated at about 300 meters. In case of leaving the range or bypassing a larger vehicle blocking the field of vision, the driver can react earlier. This makes driving more predictable and safer for all road users.

Vehicle to Infrastructure (V2I)

The acronym V2I stands for vehicle-infrastructure communication technology. The approach makes it possible to record information about current events on the road. Live road safety information is transmitted wirelessly to alert the driver on approaching vehicles. The spectrum of information sent is wide, it is such information as the traffic volume on a given road section, the current status of traffic lights, weather conditions, height restrictions (e.g. regarding bridges). This system also plays an extremely important role in the implementation of autonomous vehicles.

Vehicle to Network (V2N)

The abbreviation V2N stands for vehicle-to-network communication technology, which aims to transfer information between the vehicle and the traffic management using cellular networks as describes (Making the Connection with Vehicle to Network (V2N), 2022). The implementation of this process is possible only with the use of the network infrastructure with high throughput, low latency, and high operational reliability. V2N networks can be implemented in areas of highly efficient cellular technology and 5G technology. The V2N network ensures mutual communication between all elements of the traffic infrastructure, largely using available relay towers in urban areas and along main roads.

Vehicle to Pedestrian (V2P)

V2P stands for Vehicle-Pedestrian Communication Technology and refers to direct communication between a vehicle and a pedestrian or multiple pedestrians in proximity. Moreover, the communication may involve other vulnerable road users, such as cyclists or VRU (Vulnerable Road Users) motorcyclists, as detailed in (Kabil, Rabieh, Kaleem, & Azer, 2022). The main task of such approach is to increase the protection of traffic participants which are the most exposed to potential collisions. This is extremely important since worldwide the number of pedestrian deaths is almost a quarter of all traffic-related deaths. According to reports (World Health Organization, 2018) this number is still increasing. V2P is directly based on the local network infrastructure. It helps to warn the pedestrian about the approaching vehicle and warn the vehicle about unprotected road users. The development of V2P is necessary in a context of introducing autonomous self-driving vehicles, which are described in the (Development and Evaluation of Vehicle to Pedestrian (V2P) Safety Interventions, 2019) report.

2.2 Potential hazards to car vehicle system

The contemporary electric cars are very complicated mechatronic systems. Due to the high functionality, their producers decided to divide their structure into modules that are managed by appropriate ECUs. Currently, the number of electronic control modules in premium brand cars is over 100, and sometimes it is close to 200. The possibility of electronic control of the mechanical executive systems gives great opportunities in terms of optimizing processes in the vehicle, maintenance, and diagnostics, as well as being the basis for the implementation of autonomous vehicles to the market. However, a special attention should be paid to the fact that in addition to these undeniable benefits, it also carries great risks in terms of possible cyberattacks.

Destabilization of a vehicle and taking control of one of the electronic control modules responsible for the most important functions related to the vehicle's safety, may lead to a collision, and in the worst scenario, even to people deaths, including also other users of the traffic environment. The critical functionalities include the basic functions responsible for the vehicle movement, i.e. drive, braking, turning, but also any activity that may prevent the drivers from performing a maneuver or give them an incorrect description of the current road situation. The main functionalities for which destabilization of their correct operation may pose the very high risk are described below.

Running gear

The running gear, shown in Fig. 11, includes the chassis, suspension, and braking systems, which are responsible for stability and comfort while driving the car. This assembly includes such elements as shock absorbers, stabilizers, springs, and brake assemblies that work together to ensure a smooth and fully controlled operating and ride. Taking control over this module or even destabilizing its operation may cause failure of the braking or steering system, which may result in uncontrolled driving and finally in the collision.

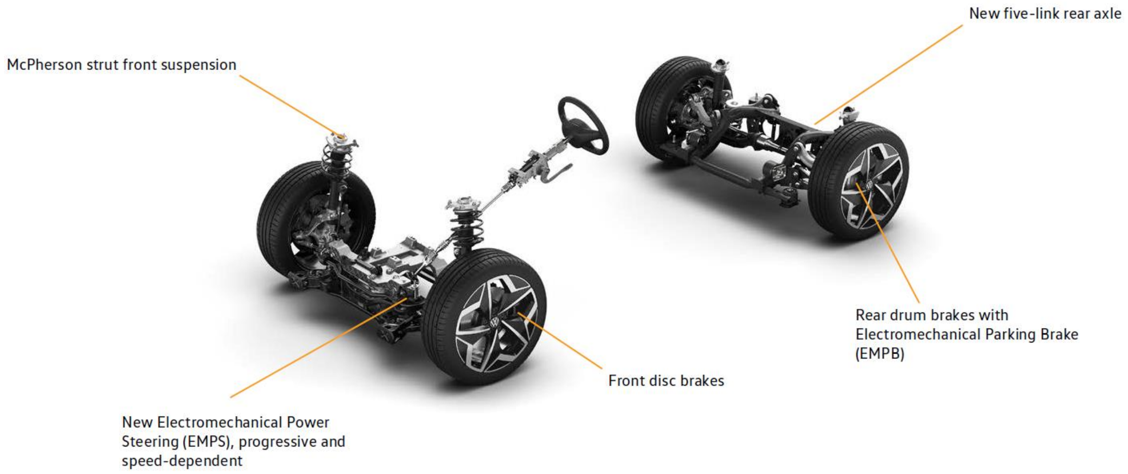

New five-link rear axle
McPherson strut front suspension
Rear drum brakes with Electromechanical Parking Brake (EMPB)
Front disc brakes
New Electromechanical Power Steering (EMPS), progressive and speed-dependent

Fig. 11 Running gear

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Electrics and Electronics

One of the main built-in elements of this system is the power supply system, which manages voltages. The system protects the car with the use of fuses (shown in Fig. 12). It is responsible for meeting the electrical needs of all 12V DC consumers in the car. When the vehicle is on, 12V is obtained from the high-voltage battery by means of an DC-DC inverter. However, to be able to start the vehicle, power supplied from a smaller 12V battery is additionally required. It is also responsible for allowing the flow of the high voltage (control relays).

Powering the electronic control units (ECUs) are responsible for managing engine performance, transmission, and other critical systems. The unit includes the electrical systems that play various functions of the vehicle, such as both exterior (see Fig. 13) and interior (see Fig. 14) lighting, air conditioning, power windows, and many more elements. Taking control over the module or even destabilizing its operation can be very dangerous, because affecting the operation of such functions as: blinker, brake lights, or even interior lighting (blinding the driver at night) can indirectly lead to a collision. The critical event seems to be a complete cut-off of power to the systems responsible for turning and braking at high speed.

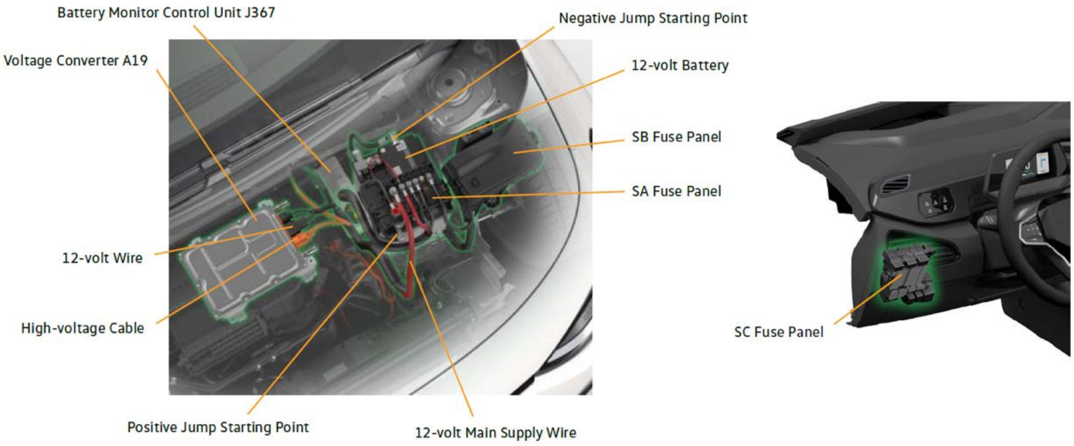


Fig. 12 Onboard Supply System

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Head Light

Tail Light Cluster

Fig. 13 Head and taillights

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

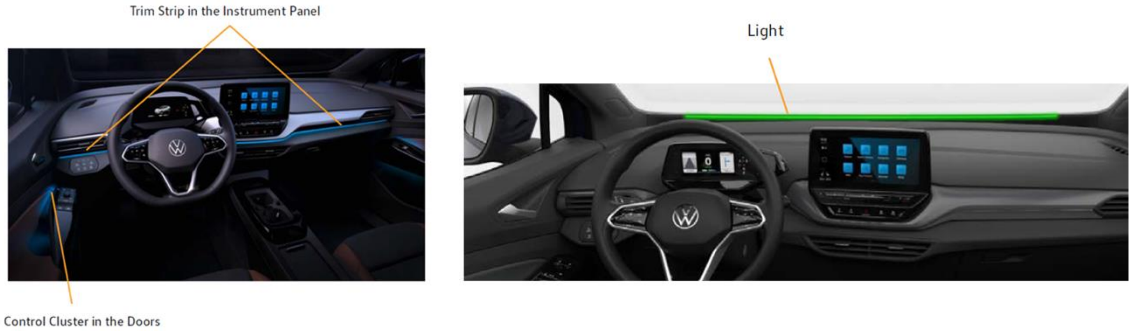

Trim Strip in the Instrument Panel
Light
Control Cluster in the Doors

Fig. 14 Internal Lighting

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

High-voltage system

The high-voltage system manages the flow of electricity from the battery to the electric motor and other vehicle components that need the high power for their correct operation. In addition to the battery, it contains components such as an inverter, DC-DC converter, and related protection mechanisms to handle and distribute large amounts of electricity. Main components of the high-voltage system in electric car are shown in Fig. 15.

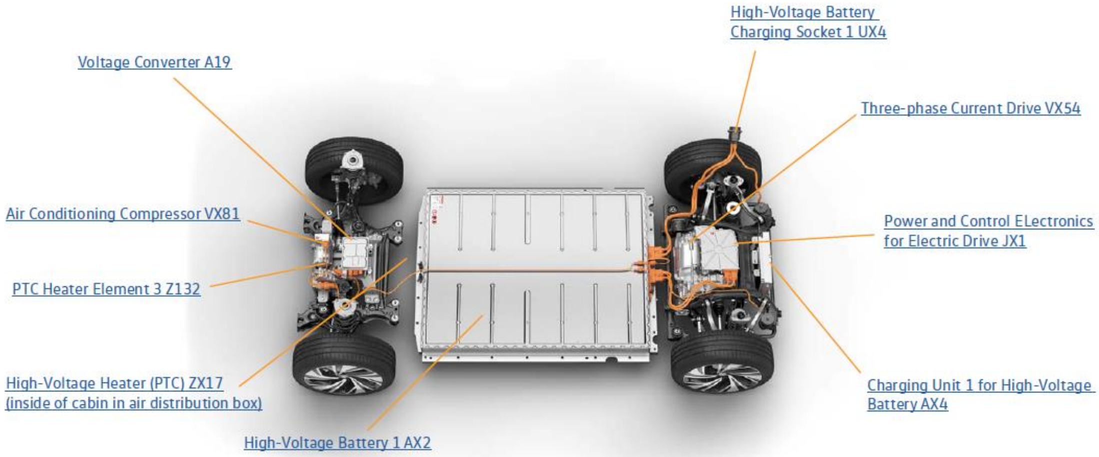

High-Voltage Battery Charging Socket 1 UX4
Voltage Converter A19
Three-phase Current Drive VX54
Air Conditioning Compressor VX81
Power and Control ELectronics for Electric Drive JX1
PTC Heater Element 3 Z132
High-Voltage Heater (PTC) ZX17 (inside of cabin in air distribution box)
Charging Unit 1 for High-Voltage Battery AX4
High-Voltage Battery 1 AX2

Fig. 15 High-Voltage System overview

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

The Voltage (Fig. 16) Converter provides the 12-volt electrical system with voltage and pre-charges the capacitor in the Power and Control Electronics for Electric Drive. It serves as the second energy source.

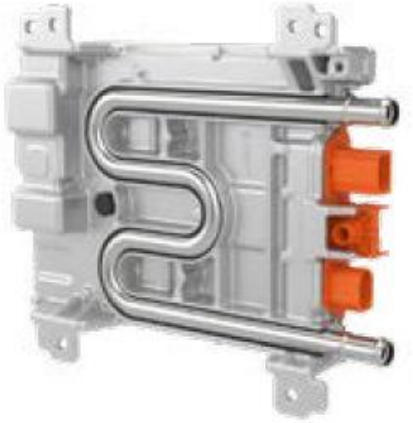


Fig. 16 Voltage Converter to 12 volts

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Charging Unit (Fig. 17) 1 for High-Voltage Battery is located in the rear of the ID.4. It converts the alternating current from the charging connection into the direct current for charging the high-voltage battery.

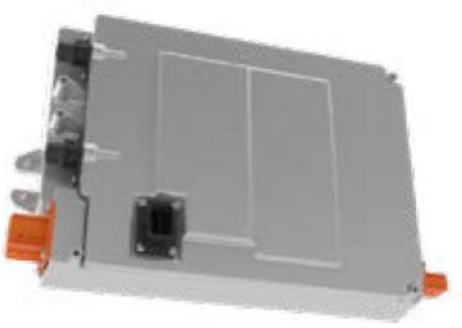


Fig. 17 Charging Unit for High-Voltage Battery

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Power and Control Electronics for Electric Drive (Fig. 18) converts the customer's power requests into electrical signals. The power electronics control the three-phase current drive. DC voltage from the high-voltage battery is converted into the three-phase AC voltage for acceleration.

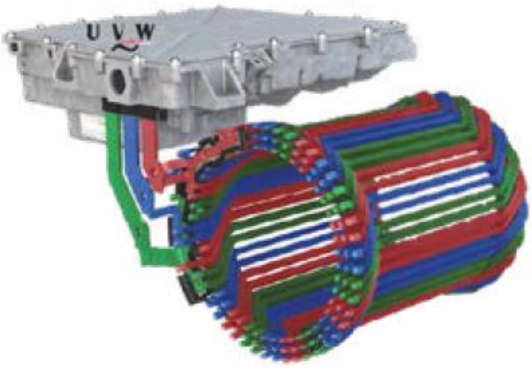


Fig. 18 Power and Control Electronics for Electric Drive

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

The high-voltage Battery (Fig. 19) is a lithium-ion battery. This is in the vehicle underbody. This location provides the low center of gravity and optimized weight distribution. The High-voltage Battery supplies the electrical energy for driving and is offered in both the 62 and the 82 kWh configuration.

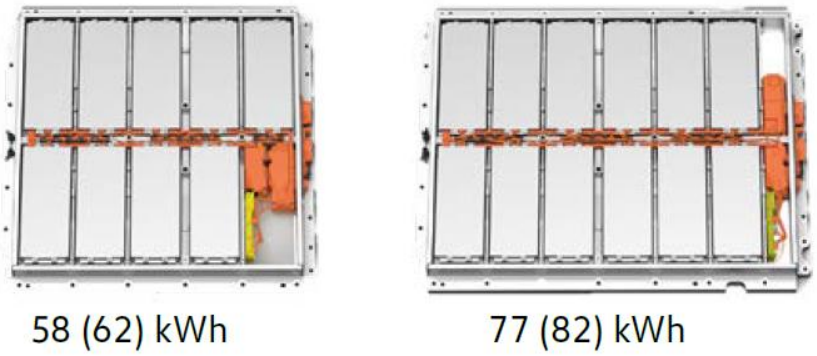


Fig. 19 High Voltage Battery

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Air Conditioning Compressor (Fig. 20) is integrated into the high-voltage system. It is used for heating both the interior and the high-voltage battery.

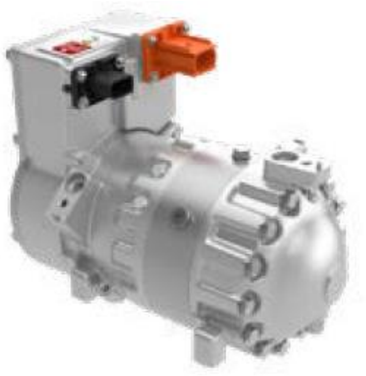


Fig. 20 Air conditioning Compressor

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

High-Voltage Battery Charging Socket (Fig. 21) can charge the high-voltage battery. Either AC or DC charging is possible. Status lights indicate the vehicle’s current charging status.

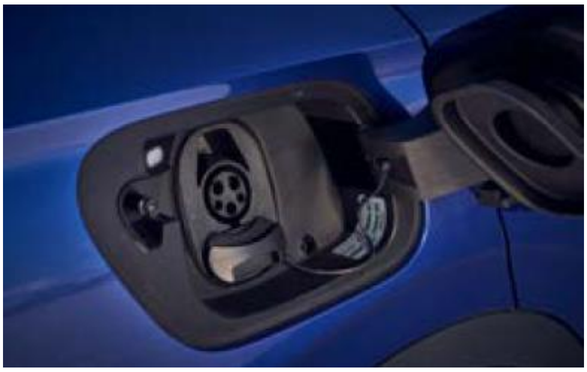


Fig. 21 High-Voltage Battery Charging Socket

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Three-phase Current Drive (Fig. 22) can drive the vehicle as an electric motor or charge the high-voltage battery as an alternator.

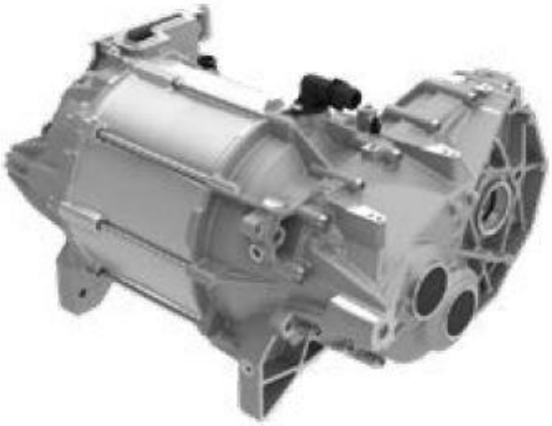


Fig. 22 Three-phase Current Drive

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

High-voltage heater (Fig. 23) is the cabin air heater and is controlled by an air conditioning control module.

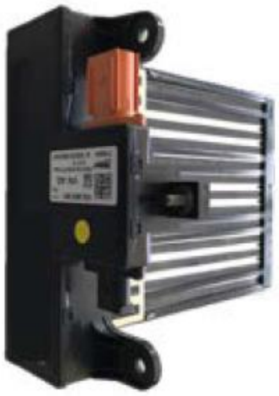


Fig. 23 High-Voltage Heater

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Undertaking control of this module or even destabilizing this system is very dangerous. An example is a sudden power cut off when driving at high speed, as well as the risk of incorrect control of the high-voltage battery, which accumulates large amounts of energy.

Safety and driver assist systems

This system manages advanced functions and uses safety technologies designed to enhance the safety of the driver and passengers. It includes, among others, subsystems such as adaptive cruise control, lane assist, tire pressure monitoring system, light assist, emergency braking (Fig. 24) or airbag deployment (see Fig. 25) and collision avoidance systems. These technologies prevent accidents and mitigate the effects of collisions.

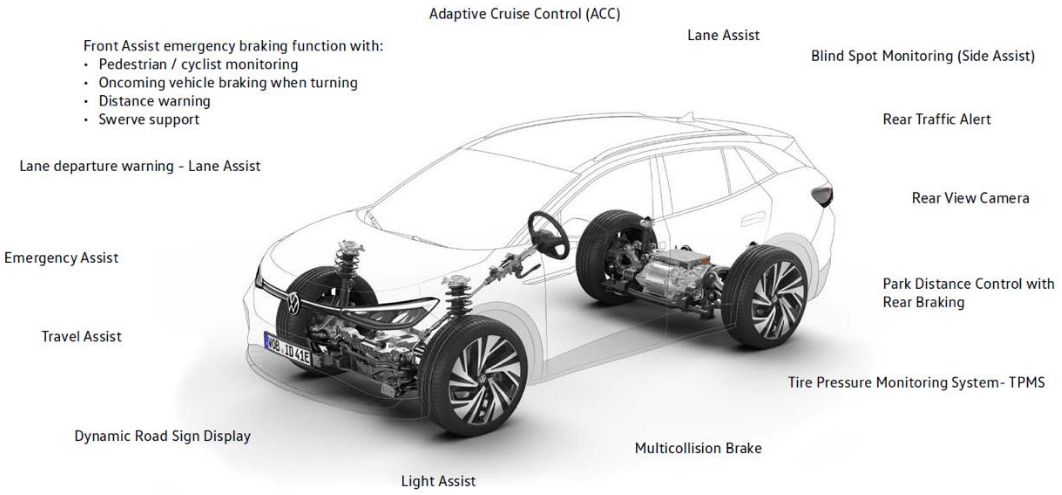

Adaptive Cruise Control (ACC)
Front Assist emergency braking function with:
• Pedestrian / cyclist monitoring
• Oncoming vehicle braking when turning
• Distance warning
• Swerve support
Lane Assist
Blind Spot Monitoring (Side Assist)
Rear Traffic Alert
Lane departure warning - Lane Assist
Rear View Camera
Emergency Assist
Park Distance Control with
Rear Braking
Travel Assist
Tire Pressure Monitoring System- TPMS
Dynamic Road Sign Display
Multicollision Brake
Light Assist

Fig. 24 Safety and driver assist systems

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

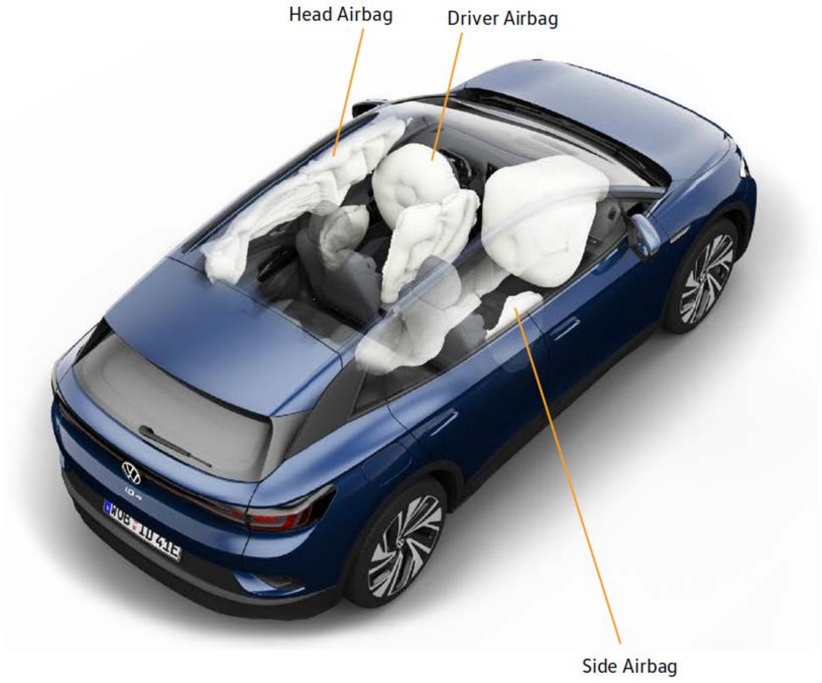


Fig. 25 Airbag deployment

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

An effective attack on the sensors that activate airbags, or the lane assist system can cause a direct threat.

Infotainment

The infotainment system (Fig. 26) combines entertainment, communication, and navigation functions inside the vehicle. Its main role is to ensure vehicle performance, safety, comfort, and overall driving experience. Thanks to the use of voice control, this functionality is easily accessible to the driver. The whole system consists of: audio system, touch screens, navigation systems, integration with smartphones (e.g. Apple CarPlay, Android Auto). The infotainment systems provide passengers with a range of multimedia and connectivity options.

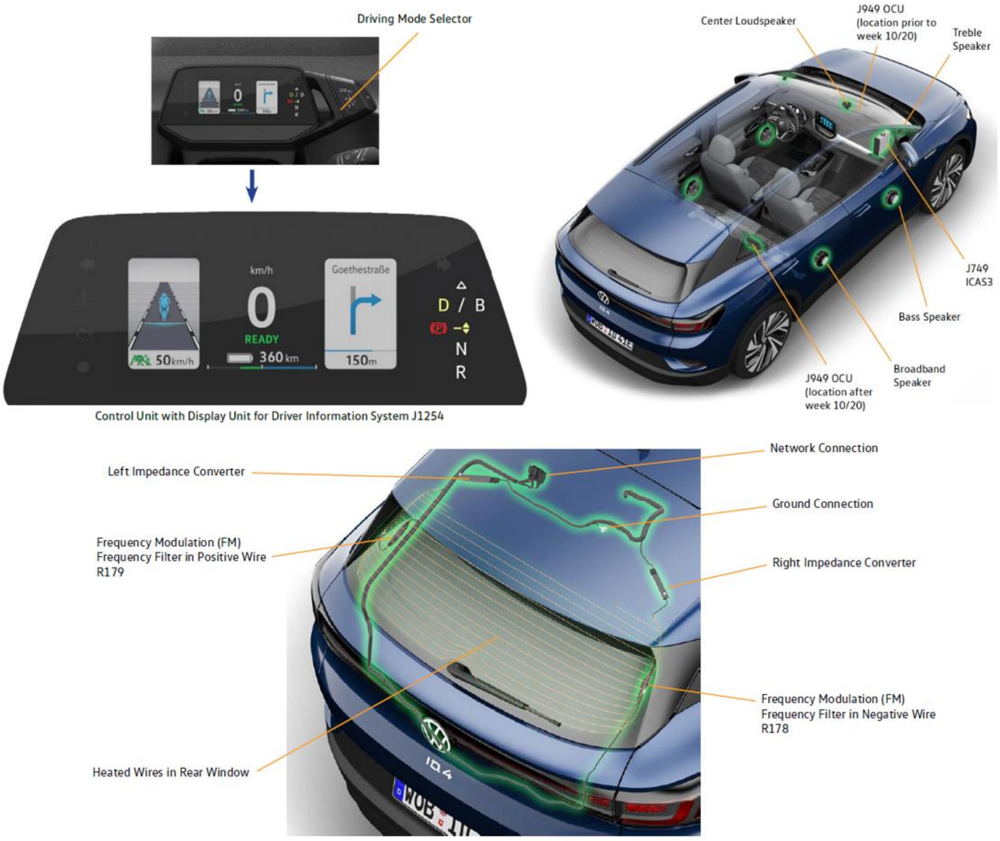

Driving Mode Selector
km/h
0
READY
360 km
50km/h
Goethestraße
150m
D / B
N
R
Control Unit with Display Unit for Driver Information System J1254
Center Loudspeaker
J949 OCU (location prior to week 10/20)
Treble Speaker
J749 ICAS3
Bass Speaker
Broadband Speaker
J949 OCU (location after week 10/20)
Left Impedance Converter
Network Connection
Ground Connection
Frequency Modulation (FM) Frequency Filter in Positive Wire R179
Right Impedance Converter
Frequency Modulation (FM) Frequency Filter in Negative Wire R178
Heated Wires in Rear Window

Fig. 26 Infotainment system

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Taking control or even destabilizing this system can be also dangerous, as indirectly the driver may be confused or frightened, which may also lead to a collision. Examples are attacks on the audio system, which suddenly turns on at maximum volume, or incorrectly displayed information about a working blinker.

2.3 Cybersecurity in automotive embedded systems

Being resistant to cyber-attacks in the automotive sector is critical to protecting lives, personal data, vehicle functionality, brand reputation, legal compliance, financial stability and industry sustainability. In other words, it must be considered every possible attack scenario and remedies have to be prepared for them. The section below describes what types of attacks we can deal with from a functional perspective, presents examples of successful attacks on motor vehicles and describes the currently used protection against cyber-attacks.

2.3.1 Possible types of cyber-attacks

An example of characteristics of embedded systems is presented in (Ruiz, et al., 2012), where authors describe the development of these systems basing on embedded components. The improvement and implementation of such systems as a very challenging task. The difficulty makes the fact that they are distributed and should operate in real-time. From the security point of view, the level of effort required to make the embedded environment resistant to threats is also very high. In the mentioned paper a methodology for the analyzing and modeling threats understood as attacks on the systems consisting of embedded components was discussed. The key factor is to identify and classify the threats. The key role is played by the Intruder Model that allows to understand a source of the risk and suggest potential defensive actions which are basis for a definition of the Threat Model.

The automotive industry imposes an additional layer of requirements related to the complete safety of the vehicle and to ensure human protection at the highest possible level. The paper (Gnacy–Gajdzik, Gajdzik, Przystałka, & Sternal, 2022) discusses the need of ISO 26262 standard implementation. According to this, the system safety is achieved through the application of a variety of safety measures. It simultaneously increases the complexity of implementing the security process for the embedded road environment. Although the rapid development of electronics gives new opportunities, it should be emphasized that the available resources are always valuable. Even though it is possible to use faster and faster processors with greater capabilities (such as more memory or more cores for calculations) for protection, the price of the module is still very high. It plays a crucial role due to the huge volume of production.

As (Desnitsky & Kotenko, 2014) noted, the embedded device specificity implies usage of combined protection mechanisms characterized by the proper security level and acceptable resource consumption. Therefore, a dual approach to the problem seems reasonable. It gives the possibility to use complex and expensive security measures when it is critical, and a low-cost method that increases the level of security, when it is enough. Threats can be classified in various ways, according to different criteria. Exemplary, considering the origin of threats they can be divided into the external and internal ones. According to the functionality one enumerates eavesdropping and data interception, destabilization, or takeover attempt. An exemplary classification of threats was described in (Rae & Wildman, 2003), where authors divided them according to types of intruders. The attacks considered from functional point of view (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021) it was suggested to consider the following classification: data eavesdropping, data recording and scenarios replaying and brute force attacks.

Data eavesdropping

This type of attack is relatively easy to implement because it does not require additional processing power of the executive system to process information in a short time. It consists in connecting to the existing network using a device with a compatible interface and listening to the transmitted data. Most of such attacks involve the wireless transmission, as it involves relatively easy physical access to the network. If the transmission is not encrypted, it is enough to place an additional receiver of the intruder's module (e.g., battery-powered) within the range of the attacked wireless network, thus gaining access to the transmitted data. In the literature, a variety of solutions to minimize the risk of such attacks can be found. In (Garnaev & Trappe, 2022) a new type of anti-eavesdropping strategy was considered. The basic goal of increasing the secrecy rate was to achieve this approach in cases of the most unpredictable ways for the adversary. A paper (Zou & Wang, 2016) is an example of description of an optimal sensor scheduling a scheme to protect the legitimate wireless transmission against the eavesdropping attack. The sensor with the highest secrecy capacity is scheduled to transmit its sensed information to the sink. Authors of (Das, Bhowmik, & Giri, 2017) claim that overhearing is a big issue in Wireless Sensor Network (WSN) for consuming a major portion of the energy. Thus, they focus on designing of a semantic preamble listening for the semantic sensor network to avoid overhearing. They propose an ontology for the sensor nodes and the discovered events. In (Ndonda & Sadre, 2017) a multipath routing strategy was described. It alternates between several paths from the source host to the destination host. The approach cannot capture the entire communication. Unfortunately, it causes critical delays. The authors also propose a priority multipath routing strategy which avoids such delays. In (Wu, Jiang, Luo, & Li, 2021) a dual denoising auto-encoder (DDAE) was presented. It was based on an unified scheme (in the sense of sharing the DDAE models) to protect the cyber-physical systems (CPS) from being eavesdropped, and to detect the typical attacks, i.e., false data injection (FDI) attacks, denial-of-service (DoS) attacks, and replay attacks. Authors of (Babaghayou, Labraoui, Ari, Ferrag, & Maglaras, 2020) focus on looming on the security and privacy threats, as a result of Internet of Vehicles technology. V2X gives lots of profits especially reducing the number of crushes by connecting a vehicle to the road infrastructure. Nevertheless, as each technology it has also some weak points, which must be secured, see Fig. 27.

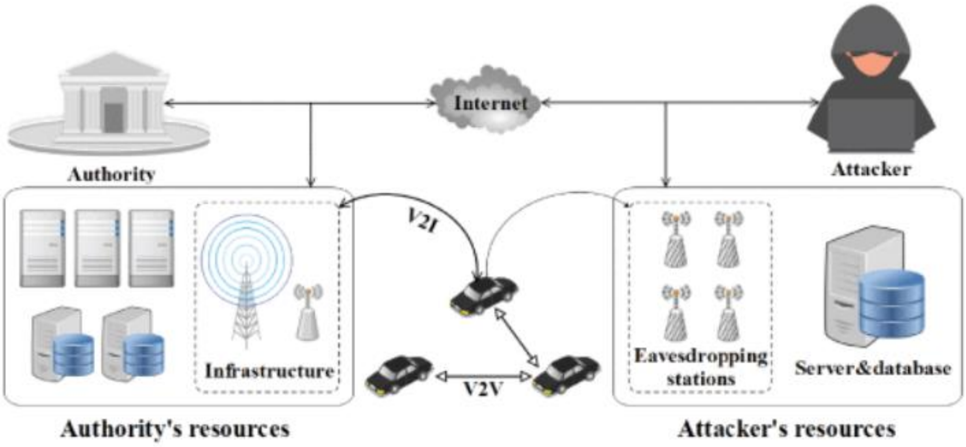


Fig. 27 Data eavesdropping scenario in V2X

(Babaghayou, Labraoui, Ari, Ferrag, & Maglaras, 2020)

Carrying out the eavesdropping attack in the wire infrastructure is much more difficult because of physical connections of the intruder module to the transmission bus is required. Even though it is difficult to add the intruder module to CAN bus, this kind of attacks should be also considered as feasible and considered in the phase of planning software architecture. It could seem that having a read-only access to the raw data is not related to any risk, but this is not true. Nowadays, thanks to the use of artificial intelligence algorithms and methods of reverse engineering, it is possible to decode information based on the read bytes of data. As presented by (Gajdzik, 2023) manual detection and identification of signals on the can bus supported by proper software is possible. In (Gajdzik, Timofiejczuk, Gnacy-Gajdzik, & Przystałka, 2023) the implementation of a deep neural network to identify the anomaly considered as a symptom of ongoing attacks was characterized. The authors of the paper provided also verification of this approach. The similar strategy of using artificial intelligence methods can be implemented to morph read data into the information with lots of details.

Data recording and scenarios replaying

Data sent via the CAN bus is very often not encrypted, it is usually transmitted openly. The reason is the encrypting on the sender side requires decryption on the receiver side, and then additional design costs are charged. One notes that this is in line with backward compatibility requirements. Moreover, the CAN is most often not protected. However, frames are included in secure operations. The consequence of the lack of encryption is the possibility of taking control over an executive module in the vehicle. An example is eavesdropping on the data sent to the CAN bus. Then, at the time of their activation, the intruder module is used, i.e., triggering on the bus. As confirmed by (Gajdzik, Timofiejczuk, & Sebzda, 2021), it is exemplary possible to control in these ways turning on or off the LED. In case of the E2E control frame, an additional problem may be the correct value of the checksum calculated based on contents of the frame and index. To perform the successful attack, index synchronization is required, i.e., having collected data for all 16 index values (including the CRC) and their repetition in the proper order. Such solution is still not used if it is not possible to implement and effectively take control over the application. As an additional type of protection minimizing the risk threat, in (Gajdzik, Timofiejczuk, & Sebzda, 2021) time window concept was proposed. The solution let us increase the security of transmission on the CAN bus.

Brute force attacks

Another type of the attack that can pose a great threat to the health and life of vehicle users is sending random sequences of data to the CAN bus. It may happen that a randomly sent set of bits activates one of electronic modules. Having regarded how the CAN bus works, i.e., the frames with specific identifiers are sent cyclically every certain amount of time (in practice, from 10 milliseconds to several seconds), such attack takes a long time. However, having considered so-called smart brute force attack, which consists in sending prepared data sequences (not all possible bit combinations) it is feasible to achieve the success. Considering the contemporary computing power of dedicated embedded systems, as researched by (Gillela, Prenosil, & Ginjala, 2019), there are certainly no performance limitations to be able to carry out this type of attacks.
Since IoV (Internet of Vehicles) is a part of IoT, it is extremely important that there is a possibility to detect this type of attacks, which are pointed out by (Raikar & Meena,

2021).

CAN bus message changing methods

There are two possibilities for connection the intruder device module to the CAN bus in a car:

- The intruder module is connected to the CAN bus parallelly (device has only 1 CAN bus interface), see Fig. 28. The only possible action that can be performed consists in reading and sending CAN messages. It must be emphasized that there is no option to block the transmitted message or replace its content.

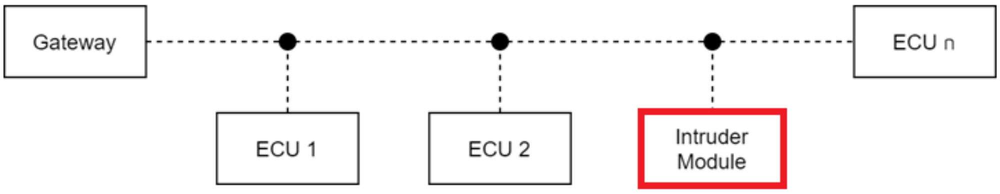


Fig. 28 Intruder as a parallel module

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)

- The intruder module is connected to the CAN bus as a bridge (the device has 2 CAN bus interfaces), see Fig. 29. The scope of possible actions to be performed by these modules are: reading, sending, blocking and replacing the content of messages.

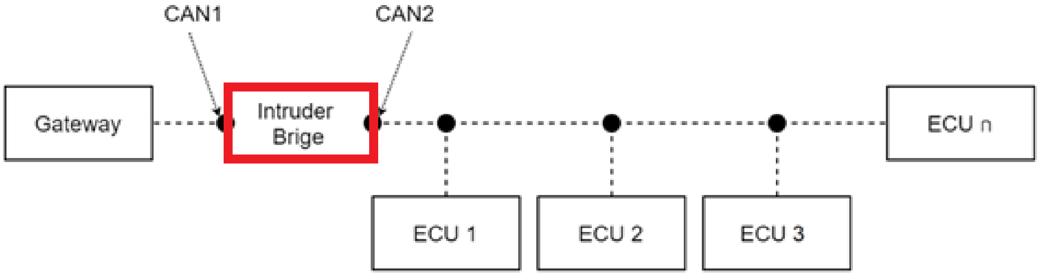


Fig. 29 Intruder as a bridge

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)

2.3.2 Examples of successfully performed cyber-attacks on car vehicles

In the research focused on anomalies detection (D'Andrada, Araujo-Filho, & Campelo, 2020) CAN is characterized in detail in (Bosch, 1991). The CAN FD is described by (Hartwich, & Bosch , 2012) and (Falch, 2022). These buses are considered to be the most pervasive in-vehicle network technologies used in cars. However, since CAN was designed with no security concerns, different solutions to mitigate the risk of cyber-attacks must be considered. There are numerous experiments in the literature examining the possibilities of attacking the CAN bus. Examples are (Koscher, et al., 2010) and (Liu, Zhang, Sun, & Shi, 2017) dealing with analyzing the security of contemporary cars. In (Kang, Song, Jeong, & Kim, 2018) a possibility of implementation of diagnostic interface OBD II was examined and illustrated. The authors use reverse engineering methods to identify CAN message and then conduct the injection of a fake message.

The paper (Staggs, 2013) also focuses on the reverse engineering methodology, which is demonstrated on the basis of the transformation of the speedometer and tachometer (instrument cluster) of 2003 Mini Cooper. A functional clock was controlled via spoofed CAN messages sent by an Arduino microcontroller. To understand the meaning of the messages contained in the CAN frames, reverse engineering techniques are typically used. They are time-consuming, labor-intensive, and require access to a physical vehicle. The attempt to optimize and solve this problem is also analyzed in research conducted by (Young, Svoboda, & Zambreno, 2020) with the use of a machine learning classifier. It analyzes messages and determines their relationship with other messages and vehicle functions. The purpose of the research presented in (Buttigieg, Farrugia, & Meli, 2017) was also to analyze the security of the CAN protocol. The BMW E90 (series 3) instrument cluster was used as a concept study in the experiment. It was shown that it is possible to create an additional (low-cost) device that, when connected to the CAN bus, is able to effectively send messages from the instrument cluster. In the research performed by (Giannopoulos, Wyglinski, & Chapman, 2017) the author noticed that having access to the internal CAN bus can be extremely dangerous. The reason in that from the bus level access, an attacker has the ability to control or manipulate with the critical systems, such as the antilock brakes and cruise control, potentially affecting driver safety. In (Gajdzik, Timofiejczuk, & Sebzda, 2022) it was proven that exchanging the payload of the CAN frame with fake content is possible. To counteract such events in (Koyama, et al., 2019) it was suggested to use countermeasure as an anomaly-detection system based on intervals or payloads. Authors of (Aliwa, Rana, Perera, & Burnap, 2021) present a spectrum of buses used in automotive. They surveyed and classified current cryptographic and IDS (Intrusion Detection System) approaches and compare them basing on such criteria as real-time constraints, types of hardware used and changes in CAN Bus behavior. They also concluded with mitigation strategies limitations and research challenges for the future.

In (Woo, Jo, & Lee, 2015) it was also pointed out that with the advent of the connected car environment, on-board networks (e.g. CAN) are now cooperating with external networks (e.g. 3G/4G/5G mobile networks), allowing an adversary to launch a long-range wireless attack using CAN vulnerabilities. Authors of (Nowdehi, Lautenbach, & Olovsson, 2017) noted that after vehicles have evolved from mostly mechanical machines into devices controlled by an internal computer network, it became extremely important to secure the CAN bus, which is the most prevalent automotive bus. They also proposed several solutions to alleviate the risk, like CAN message authentication.

In (Checkoway, et al., 2011) the possibility of remote access to a car through the CD player, Bluetooth and other wireless communication systems was investigated. Authors of (Choi & Jin, 2019) also focus on the remote access to a car and analyze the infringement cases through infotainment devices. This topic is extremely important, because as (Simacsek, 2019) describes, taking over of a car with the use of remote control was proven and fully described in (Greenberg, 2015). Researchers Chris Valasek and Charlie Miller remotely took over control of Jeep Cheroke, accessing the car through the multimedia system. This case became probably the most famous example of the cyber-attack in the world. The incident also presented that not only attacking the critical features like braking, steering or accelerating systems is dangerous. As Chris and Charlie described, while driving 70mph (about 112 kmph) the vents in the Jeep Cherokee started blasting cold air at the maximum setting, next the radio switched to the local hip hop station and began blaring at full volume. There was no possible to stop it with the use of the control knob and the power button. Finally, the windshield wipers turned on, and wiper fluid blurred the glass. Such sudden and unforeseen vehicle behavior can distract or even scare the driver, who can cause a hazard on the road.

In (Khandelwal, 2016) other very recognizable Tesla hacked incident was presented. A team of security researchers from the Keen Security Lab hacked into the Tesla Model S car using multiple software flaws. In 2017, a team of Chinese researchers Sen Nie, Ling Liu and Wen Lu, along with director Samuel Lv, demonstrated how it could remotely take control of Tesla's brakes and apply the brakes from a distance of 20 km, violating the CAN bus that controls many vehicle systems in the car. The researchers were also able to remotely unlock the car's doors, take control of the dashboard's computer screen, open the trunk, move the seats, turn on wipers, and fold the side mirrors while the vehicle is moving. The hack attack requires the car to be connected to a malicious Wi-Fi hotspot and is triggered only when the car's web browser is used.

2.3.3 Security methods against cyber-attack

In the era of rapid technological advancements and ever-expanding digital landscape, the safeguarding of sensitive information and critical infrastructures against the pernicious threats of cyber-attacks has emerged as a paramount concern. As cyber-attacks continue to grow in frequency, sophistication, and impact, institutions and organizations across the globe are compelled to fortify their defense mechanisms.

End-to-End Protection

The introduction of the End-to-End (E2E) protection mechanisms marked a significant development in the automotive industry, primarily aimed at safeguarding safety-critical communications. As (Forest & Jochim, 2011) describe, this protocol was devised to enable the detection of systematic faults that might arise from software defects and random hardware malfunctions, thereby affecting the integrity of transmitted data. It is necessary to clarify that E2E was not originally developed for purposes related to data recovery, data encryption or cybersecurity purposes.

Authors of (Staron & Durisic, 2017) notice that a comprehensive implementation of the E2E on both the transmitting and receiving sides ensures that the following objectives are met:

- protection against data corruption such as bit flipping
- detection of the stuck lost or incorrect sequence of received data.

Each of these aspects is achieved by including a checksum byte in the transmitted message. The checksum calculation includes the entire data section of the message, supplemented by an additional byte from the shared key table that is not explicitly transmitted. The selection of the key table element for the checksum calculation depends on the value of the counter that follows the checksum field in the message layout. This counter is incremented continuously from 0 to 15, and its current value dictates the specific key table element to be used for the checksum calculation. This mechanism empowers the system to take proactive measures, potentially entering a safe state when such irregularities are identified. It should be highlighted that the diligent monitoring of the counter's behavior plays a pivotal role in executing this approach effectively.

Encryption

The encryption serves as a key and fundamental method in the field of information security. It is strategically used to protect confidential information from the illegal access or inadvertent disclosure. This cryptographic procedure entails the transformation of the plain text, in an intelligible form, into the ciphertext through a series of mathematical operations performed by cryptographic algorithms with a designated cryptographic key. The overarching goal underlying the encryption is to deliberately obscure data to a degree that makes it intelligible only to individuals with the required decryption key, thereby preventing unauthorized parties from perceiving the original content of the protected information. (Andrade, et al., 2023) introduced a model to enhance the security of safety systems in vehicles equipped with Controller Area Network with Flexible Data Rate (CAN FD) communication protocols. In (Andrade, et al., 2023) it was noticed that the proposed solution leverages the established HMAC (Keyed-Hash Message Authentication Code)/SHA-2 (Secure Hash Algorithm 2) for data authentication, while employing the AES256 encryption algorithm for data encryption. These authentication and cryptographic methodologies are strategically integrated into the data frame structure to optimize the security, processing efficiency, and minimizing the bus load associated with the data frame.

As (Hubaux, Capkun, & Luo, 2004) noted, Public Key Infrastructure (PKI) algorithms involve complex mathematical operations resulting in manipulation of sizable numerical values, typically within the range of 1024-4048 bits, depending on chosen algorithm's security level. Despite their computational complexity, these algorithms offer advanced functionalities, including robust data encryption and rigorous integrity verification. To ensure privacy in potentially vulnerable communication channels, PKI algorithms rely on digital signatures and key distribution protocols. Moreover, asymmetric cryptographic techniques are purposefully engineered to secure transmitted data and facilitate mutual authentication among network nodes. In (Jadoon, Wang, Li, & Zia, 2018) some of the common asymmetric cryptographic solutions with security requirements support were presented. Their limitations, discussed in the mentioned paper, are characterized in Tab. 1.

Tab. 1 Asymmetric cryptographic solutions
(Jadoon, Wang, Li, & Zia, 2018)

Asymmetric Cryptographic solutions	Security Requirements support	Limitations
Anonymous keys and certificates	Authentication/Availability/Privacy Preservation	Computational hardness
ID-based proxy signatures	Authentication/Privacy Preservation/Non-Repudiation	Vulnerable to reveal private key
Elliptic Curve Cryptography	Authentication/Availability/Privacy Preservation	Vulnerable to replay attack
RSU-aided Authentication Methods	Authentication/Privacy Preservation	Compromise on an RSU can result in disclosure of information
Smart Cards for identification	Message authentication/privacy preserving	Storage

Mechanisms required to provide security of an application could be carried out with the use of software, hardware implementations, or a combination of both. Summarizing, some forms of software implementations are always required. Typically, the hardware is provided to accelerate the execution of cryptographic operation algorithms to satisfy application requirements. For instance, the SHA-256 algorithm implemented for the checksum of memory contents can be twice faster due to hardware acceleration compared to the software-only example. The benefits of the hardware acceleration become even more attractive with asymmetric solutions cryptographic algorithms such as RSA and ECC. It is especially important when the key size is increased.

Sessions

The Unified Diagnostic Services (UDS) is a diagnostic communication protocol used in electronic control units (ECUs) within automotive. The document is specified in the (ISO 14229-1:2020 Road vehicles — Unified diagnostic services (UDS), 2020). Modern vehicles are equipped with a diagnostic interface designed for off-board diagnostics. This interface allows a computer, often called the client, or a diagnostic tool known also as the tester, to be connected to the vehicle's communication system. The interface let it possible that the Unified Diagnostic Services (UDS) requests can be sent to various controllers in the vehicle. They are required to provide a response, either positive or negative. This feature allows users to access the fault memory of individual control units, update them with new firmware, involve in low-level interactions with their hardware (such as activating or deactivating specific outputs) and use specialized functions, often called routines. These procedures are used to provide insight into the environment and operating conditions of the electronic control unit (ECU) to diagnose any faulty or undesirable behavior. The Diagnostic Session Control is one of the key services in the Unified Diagnostic Services (UDS). Its primary functionality is to manage the diagnostic sessions of electronic control units (ECUs). This service basically enables the transition from one diagnostic session to another. These diagnostic sessions provide a facility to enable or disable specific sets of diagnostic functions and features in the ECU. It is important to understand that not all UDS services can access the ECU directly. Some services are only accessible when the ECU is in the Default session, while others can interact with the ECU in alternative sessions. Essentially, the Diagnostic Session Control serves as the gateway, determining which services can access the ECU. Vehicle manufacturers are the ultimate arbiters in deciding which sessions grant access to specific services. For instance, in the Default session, it might be impossible to perform software upgrades on the ECU. Such ECU reprogramming can take place only in a dedicated programming session, under the supervision of authorized engineers.

Authentication - Digital signature

The cryptographic authentication is a process of verifying the identity of a data sender. As the author in (Soja, 2014) claims, designers must anticipate every form of the attack to prevent access to embedded systems and data. In the embedded systems the authentication can be employed to confirm the origin of data when it is exchanged between different control units through external interfaces. It can be also applied to verify the reliability of the software image before running or when downloading from an external source before the image is programmed into the on-chip flash memory. The authentication usually ensures data integrity if the entire data or software image is to create an authentication code (better known as a digital signature). Any modification to the data or the software image trigger an authentication failure. There are both symmetric and asymmetric cryptography supported by the authentication algorithms. The symmetric cryptographic authentication is based on a shared secret key. The transmitter generates a message authentication code (MAC) using the secret key. The asymmetric cryptography employs a public key to authenticate data received from the owner of the private key. This digital signature scheme is based on the sender generating a unique signature, which is created based on some combination of the message and the sender's private key characterizing both the message and the signature to the receiver. The signature is commonly provided by calculating the checksum of the entire message and then encrypting only the checksum with the private key. The recipient of the message and signature can then execute the same checksum operation on the message and compare it with the checksum that was decrypted from the signature using the public key. If they do not correspond to each other, the data is corrupted during transmission, or the transmitter is not the expected one. The alternative authentication method derives from hash algorithms and is known as HMAC, which is typically added to the name of the underlying cryptographic algorithm. This code is defined as the keyed-hash message authentication code and is derived from sharing of the secret key. The key is integrated with the message in a way that ensures it is resistant to attacks. The resultant HMAC is sent with the message and checked by the receiver with the same shared secret key. This ensures that the HMAC authentication belongs to the symmetric cryptography.

2.4 Selected applications of artificial intelligence in automotive

The rapid development of algorithms and applications of artificial intelligence (AI) has been observed for several years. The artificial intelligence has also a major impact on the development of the automotive industry through optimizing various aspects of vehicle design, manufacturing, maintenance, and safety. Especially the safety is the most critical topic, so any supporting functions based on the AI are pivotal. In (Halim, Kalsoom, Bashir, & Abbas, 2016) the artificial intelligence techniques for driving safety and vehicle crash prediction were presented. The most common applications of artificial intelligence in the automotive industry include:

- Autonomous Driving

  This is the most complex control system that relies heavily on the artificial intelligence algorithms. These systems use such devices as sensors, cameras, lidar and radar to perceive the surroundings and make real-time decisions about safe navigation based on current road conditions around the vehicle.

- Advanced Driver Assistance Systems (ADAS)

  The ADAS features such as an adaptive cruise control, lane assist, and automatic emergency braking use the artificial intelligence algorithms to enhance driver safety and comfort. The artificial intelligence approaches let processing data registered by sensors to ensure the control of the vehicle through warnings provided to the driver and assist in the event of dangerous situations on the road.

- Traffic Management

  AI-based traffic management systems help reduce congestion and improve traffic flow by analyzing real-time data from traffic cameras, GPS devices and other sources to adjust traffic signals and routes. The importance of this technology is growing rapidly with the development of car connected systems, which is known as Vehicle to everything

- Energy Efficiency

  AI algorithms optimize energy management systems for hybrid and electric vehicles. During recuperation, they manage the energy recovery process. While charging, they determine the best parameters allowing us to charge the battery safely and relatively quickly, and moreover to ensure the battery long life.

- Predictive Maintenance

  Communication systems with the outside world together with the artificial intelligence approaches make it possible to process data registered by sensors located in vehicles. Results of data processing and analysis provide the information on the technical state of the car and its modules. Constant monitoring some crucial parameters let us predict breakdowns, failures or required maintenance time. Such approaches lead to the maintenance costs reduction and increase vehicle uptime.

- Natural Language Processing (NLP)

  Voice assistants such as Apple's Siri, Google Assistant and Amazon's Alexa are becoming increasingly popular in automotive. The NLP technology allows drivers to control various functions such as navigation, entertainment and air conditioning using voice commands. Due to the lack of the need for touch control by physically pressing a button or touch screen, the level of safety while driving has significantly increased because the driver can constantly monitor the road situation outside the vehicle.

- Infotainment and Personalization

  AI-based infotainment systems learn driver preferences and behavior to offer personalized content and recommendations. They help you avoid stressful situations and improve your overall car travel experience.

- Gesture and Emotion Recognition

  There is a series of applications based on artificial intelligence approaches that can interpret the driver's gestures and facial expressions and assess the speed and correctness of the driver's reaction to the traffic situation around the vehicle to increase safety by recognizing when the driver is drowsy or irritable.

- Cybersecurity

  With increasing vehicle connectivity (V2X), the artificial intelligence methods play a key role in identifying and preventing cyber threats, protecting vehicle systems against intrusions involving data theft, driving destabilization or taking control of a selected electronic control module. Authors of (Tong, Hussain, Bo, & Maharjan, 2019) focus on V2X together with AI and address various research challenging V2X system.

Fig. 30 presents percentage overview of the AI applied to V2X applications.

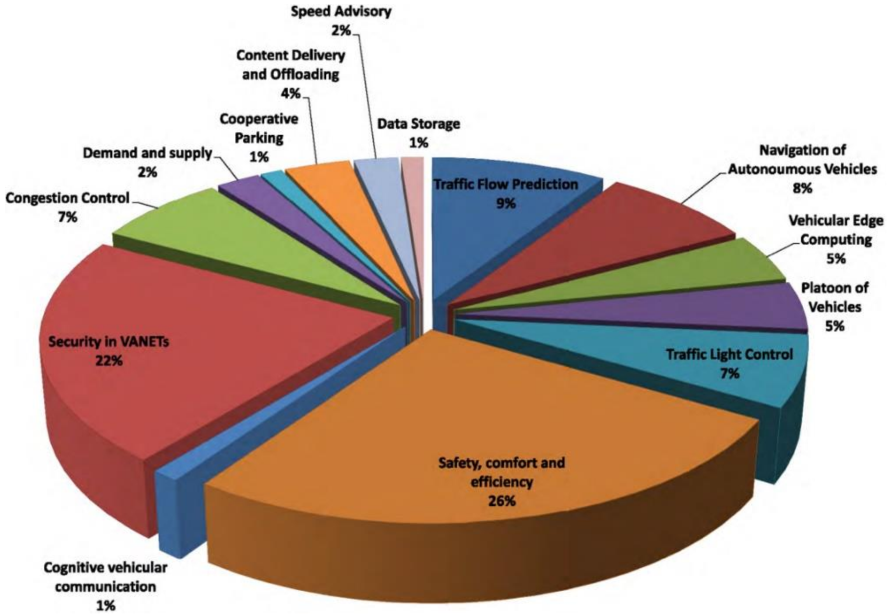


Fig. 30 Overall representation of AI applied to V2X applications

(Tong, Hussain, Bo, & Maharjan, 2019)

In (Tong, Hussain, Bo, & Maharjan, 2019) the AI applications and its branches were discussed. The overview of the term and techniques within AI is presented in Fig. 31.

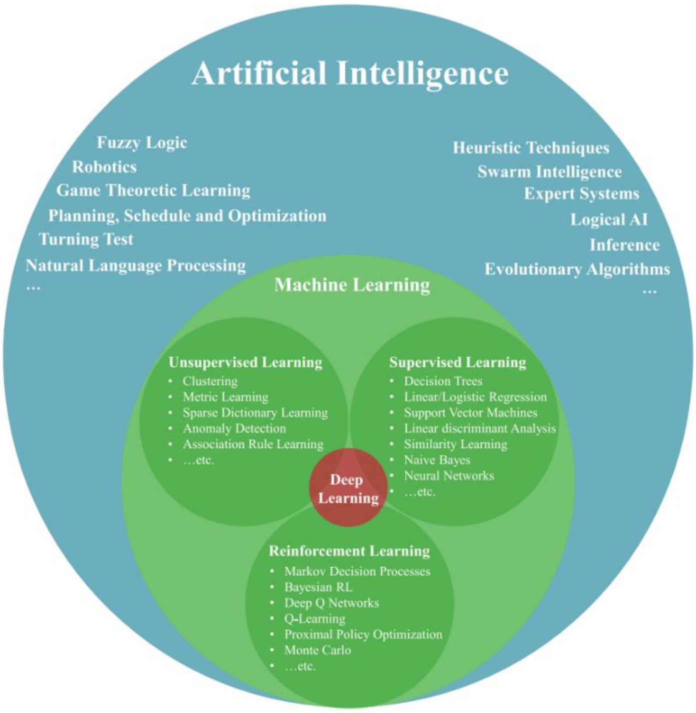


Fig. 31 AI and its branches and development trends

(Tong, Hussain, Bo, & Maharjan, 2019)

The review of literature dealing with the AI applications let us to summarize contemporary trends and directions. The most frequently described applications are: heuristic techniques, expert systems, natural language processing, automatic inference, and machine learning. The algorithms and approaches that are used to develop the enumerated applications are still evolutionary algorithms, fuzzy logic, and neural networks.

Various AI techniques were employed to tackle the intricate and ever-changing challenges of the V2X concept. Fig. 32 provides an overview of the AI techniques being applied contemporary in the V2X. It should be stressed that different kinds of deep learning including application of swarm intelligence emerged as two prevalent and extensively adopted methods. The growing accessibility of computational resources, storage capacity, and the continuous advancement of the AI algorithms have solidified a robust trajectory for the AI-driven research in V2X, empowered by the 5th generation of mobile networks.

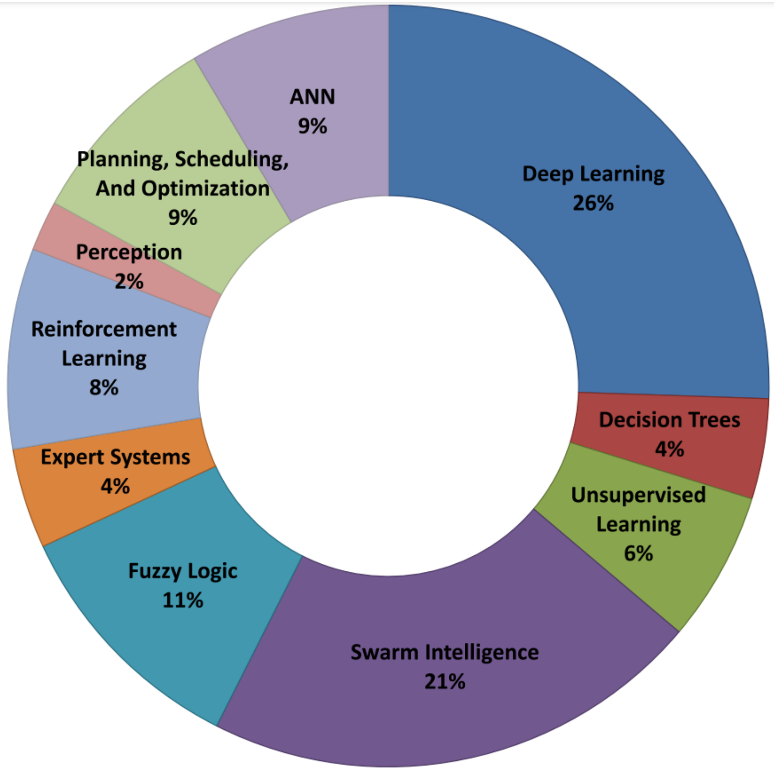


Fig. 32 The AI techniques used in V2X applications

(Tong, Hussain, Bo, & Maharjan, 2019)

The deep learning is an approach developed on the basis of the three primary categories of Machine Learning (ML): unsupervised learning, supervised learning, and reinforcement learning. It is usually characterized by an application of a special structure neural network. The neurons are organized in a multiple, at least 3 layers structure. This network comprises an input layer, hidden layers, and an output layer. Each neuron is employing a non-linear transformation function such as ReLU, tanh or sigmoid. The proper scaling of the input data holds paramount significance, as it can significantly impact the network's predictive or classification capabilities. As the number of hidden layers increases, the network's capacity to learn also grows. However, beyond a certain threshold, adding more hidden layers does not yield any performance improvements. The training of a deep network is a challenging task, demanding substantial computational resources. In the context of application in the automotive and especially for data gained from vehicles in motion, the implementation of mobile computing servers can offer significant advantages, especially considering a car connected idea V2X. Fig. 33 provides a visual representation of the concept, depicting neurons, the input layer, hidden layers, and the output layer within a deep neural network.

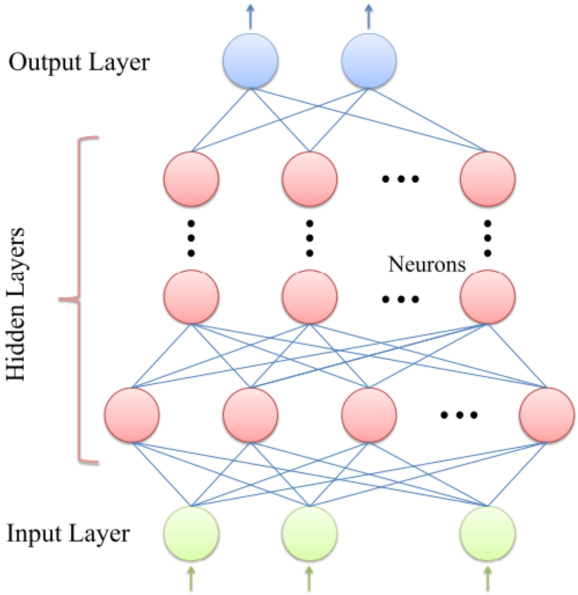


Fig. 33 Typical deep neural network

(Tong, Hussain, Bo, & Maharjan, 2019)

The applications of artificial intelligence approaches to problems in automotive industry is related to processing and analyzing very large amounts of data collected from various sensors. Additionally, to observe certain dependencies and trends occurring in the data, the calculation models should consider numerous aspects. It often requires the application of complex and sophisticated approaches. Examples are deep neural networks presented above. They are characterized by a specific learning model that allows for the processing of very large amounts of time-dependent data. Based on the bibliography related to such problems one can conclude that among a big number of different deep-learning methods a good solution seems to be the use of an autoencoder model based on the recurrent neural network (RNN). There are also examples of applications of the approach in the automotive industry.

The autoencoder is a type of the artificial neural network that converts input data into the internal representation and then reproduces the result at the output. A graphical example of the autoencoder operation is presented in the Fig. 34.

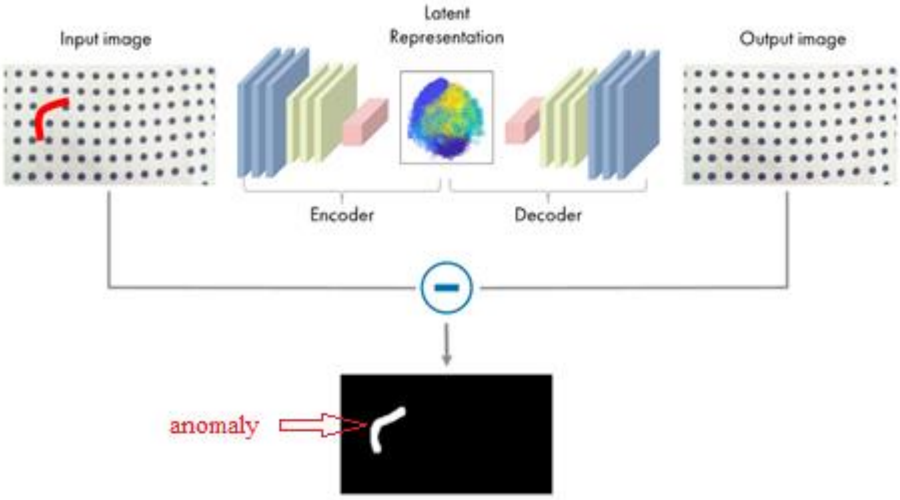


Fig. 34 Autoencoder concept

(Autoencoders, 2023)

The number of neurons in the hidden layer is smaller than in the input layer. Thus, at first the process of information encoding takes place. Then the internal representation is obtained, and the states of the outputs are reproduced using the decoder. Next, by comparing the original state with the reconstructed one, it can be inferred whether there is an anomaly that may be a sign of an ongoing attack. The anomaly detection is one of the main applications of autoencoders, in addition to reducing redundancy, classification and generating new features. The autoencoders, thanks to their natural properties, are very often used as the deep learning approach.

The author of (Lendave, 2021) describes that in the RNN to train networks, data is backpropagated and at each time step or loop operation gradient is being calculated. The gradient is used to update the weights in the networks. Now if the effect of the previous sequence on the layer is small then the relative gradient is also small. In case the gradient of the previous layer is smaller then this makes weights to be assigned to the context smaller and this effect is observed when we deal with longer sequences. Due to this property, the network does not learn the effect of earlier inputs and thus the short-term memory problem appears. To overcome this problem specialized versions of the RNN are created. In their structures LSTM (Long Short-Term Memory) or GRU (Gated Recurrent Unit) layers are included.

The key difference between the GRU and the LSTM is that the GRU has two gates (reset and update gates) whereas the LSTM has three gates (input, output, and forget gates). As in (Lendave, 2021) concludes, the GRU uses less training parameters and therefore uses less memory and provides the solution faster than the LSTM. However, the LSTM is more accurate in case of a very large dataset. One can choose the LSTM when dealing with large sequences and when high accuracy is concerned. The GRU is usually used when less memory consumption is required and providing the results is expected faster.

The main differences between the LSTM and the GRU are shown in the following diagrams Fig. 35 and Fig. 36.

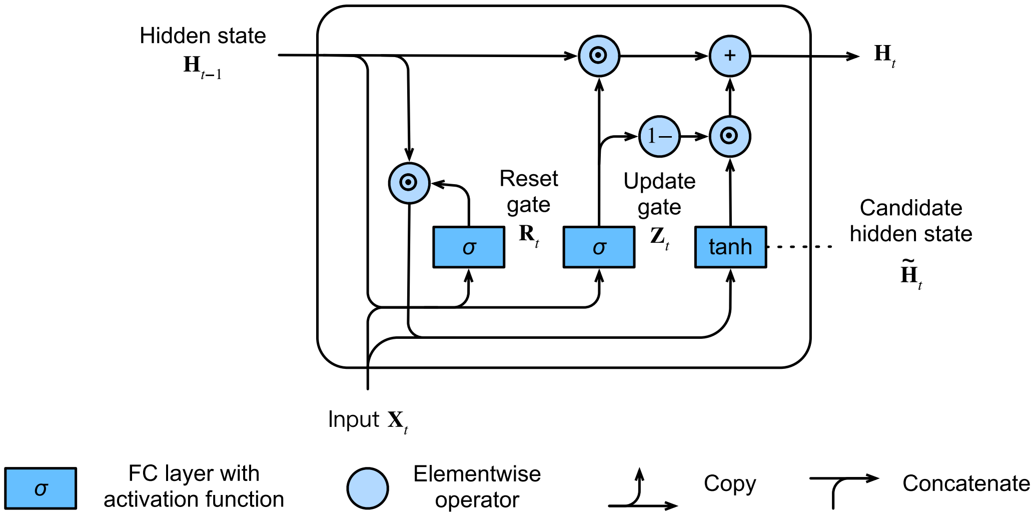


Fig. 35 Computing the hidden state in GRU model

(Long Short-Term Memory (LSTM), 2023)

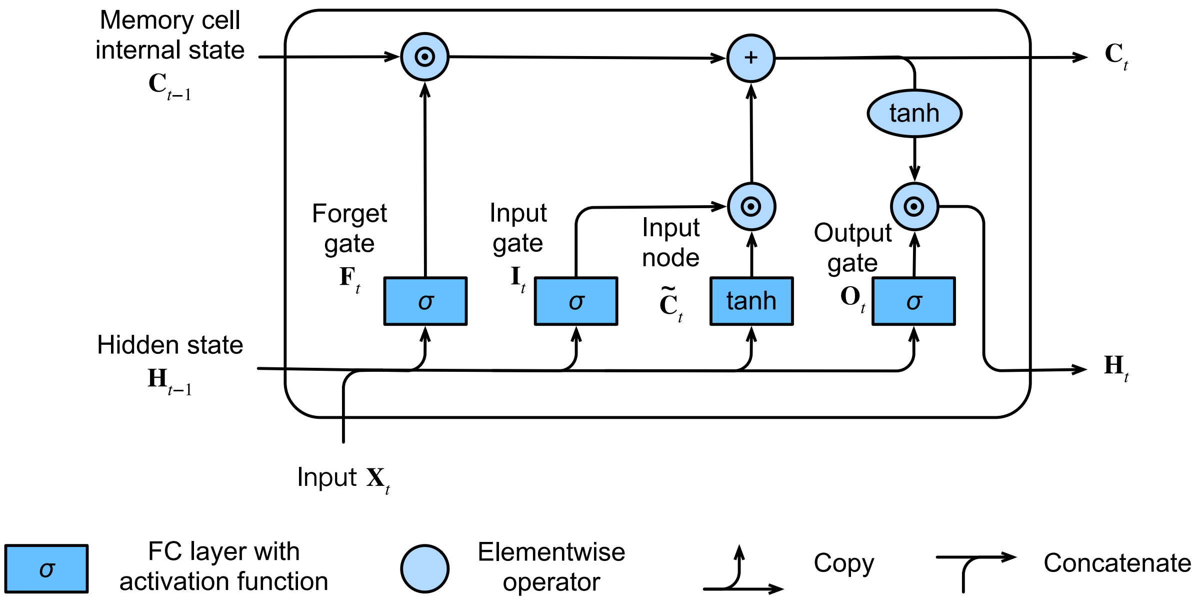


Fig. 36 Computing the hidden state in the LSTM model

(Long Short-Term Memory (LSTM), 2023)

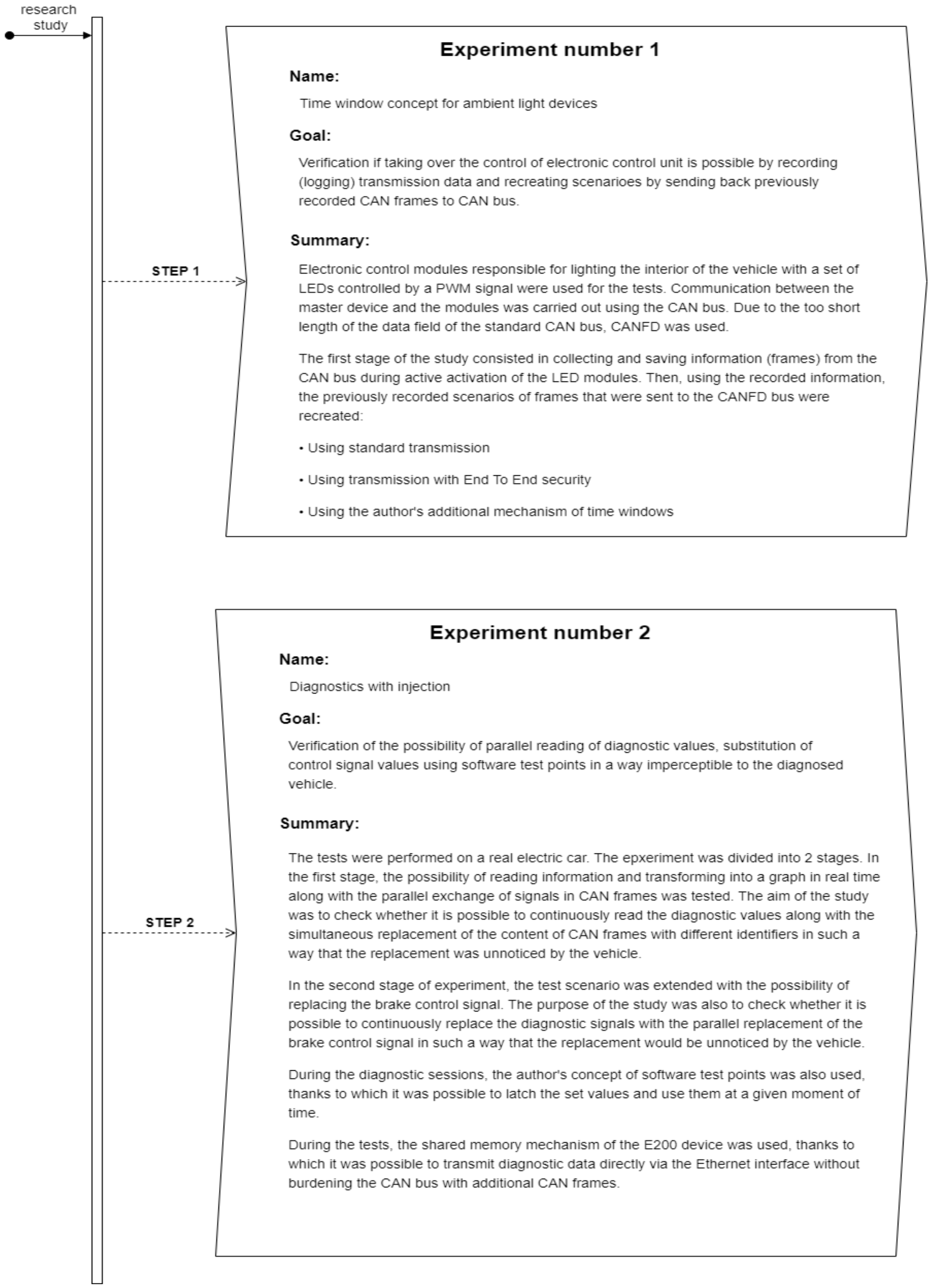
Chapter 3

Experimental research and elaborated solutions

The contemporary vehicles are very complex mechatronic systems consisting of dozens, and in the case of better equipped versions, even over a hundred electronic control modules that cooperate with each other. To control the vehicle big sets of data are exchanged in real time with the use of transmission buses maintaining strict time requirements. A good example of a development of cars in recent years are changes of the handbrake system. In the past it used to be a mechanical system, and now it is a mechatronic one. The widespread introduction of electronic systems replacing mechanical elements is not only the result of technological development, aesthetic considerations, and the possibility of minimizing control elements, but also by economic factors. Considering the number of mechatronic systems constantly exchanging information during the vehicle operation it can be concluded that nowadays the vision of an attack on a car is very likely and in fact it happens often and often. The electronic systems controlling the executive modules can be attacked in two ways:

- taking control over the module,
- destabilizing the correct operation of the module.

Considering such attacks, some experiments were planned and carried out, as one of the tasks during PhD project. The goal was to check the possibility of performing an effective attack on a selected executive element that is a part of the vehicle. In subsequent experiments, the simulated attacks were ordered to the increasing complexity of the attack. Starting from a simple attack, involving recording and transmission and its subsequent playback (sending logged frames on the bus), through replacing the signal values in a transparent way during carrying out some regular procedures. It has been proven that attacks on currently manufactured vehicles, composed of mechatronic systems, were successfully completed. The performed tests demonstrated that it is possible to take control over a certain functionality of the vehicle. As the result of the PhD project the low-cost software encryption mechanisms were proposed. The main goal of the performed tasks was to significantly hinder this type of attack. It was confirmed by the verification tests. The last experiment was focused on the application and use of artificial intelligence algorithms to detect attacks on the vehicle. One assumed that during the attack some anomalies are going to be visible among the signals sent from frames on the CAN bus. To discover the anomalies deep learning algorithms were used. Time dependencies in the analyzed data were taken into account. It should be emphasized that the entire experiment was carried out in accordance with the "black box" approach. The set of data was processed and analyzed without knowing the structure and character of the signals. All conducted studies were divided into four experiments presented in the Fig. 37.



Experiment number 1

Name:

Time window concept for ambient light devices

Goal:

Verification if taking over the control of electronic control unit is possible by recording (logging) transmission data and recreating scenarioes by sending back previously recorded CAN frames to CAN bus.

Summary:

Electronic control modules responsible for lighting the interior of the vehicle with a set of LEDs controlled by a PWM signal were used for the tests. Communication between the master device and the modules was carried out using the CAN bus. Due to the too short length of the data field of the standard CAN bus, CANFD was used.

The first stage of the study consisted in collecting and saving information (frames) from the CAN bus during active activation of the LED modules. Then, using the recorded information, the previously recorded scenarios of frames that were sent to the CANFD bus were recreated:

- Using standard transmission
- Using transmission with End To End security
- Using the author's additional mechanism of time windows

Experiment number 2

Name:

Diagnostics with injection

Goal:

Verification of the possibility of parallel reading of diagnostic values, substitution of control signal values using software test points in a way imperceptible to the diagnosed vehicle.

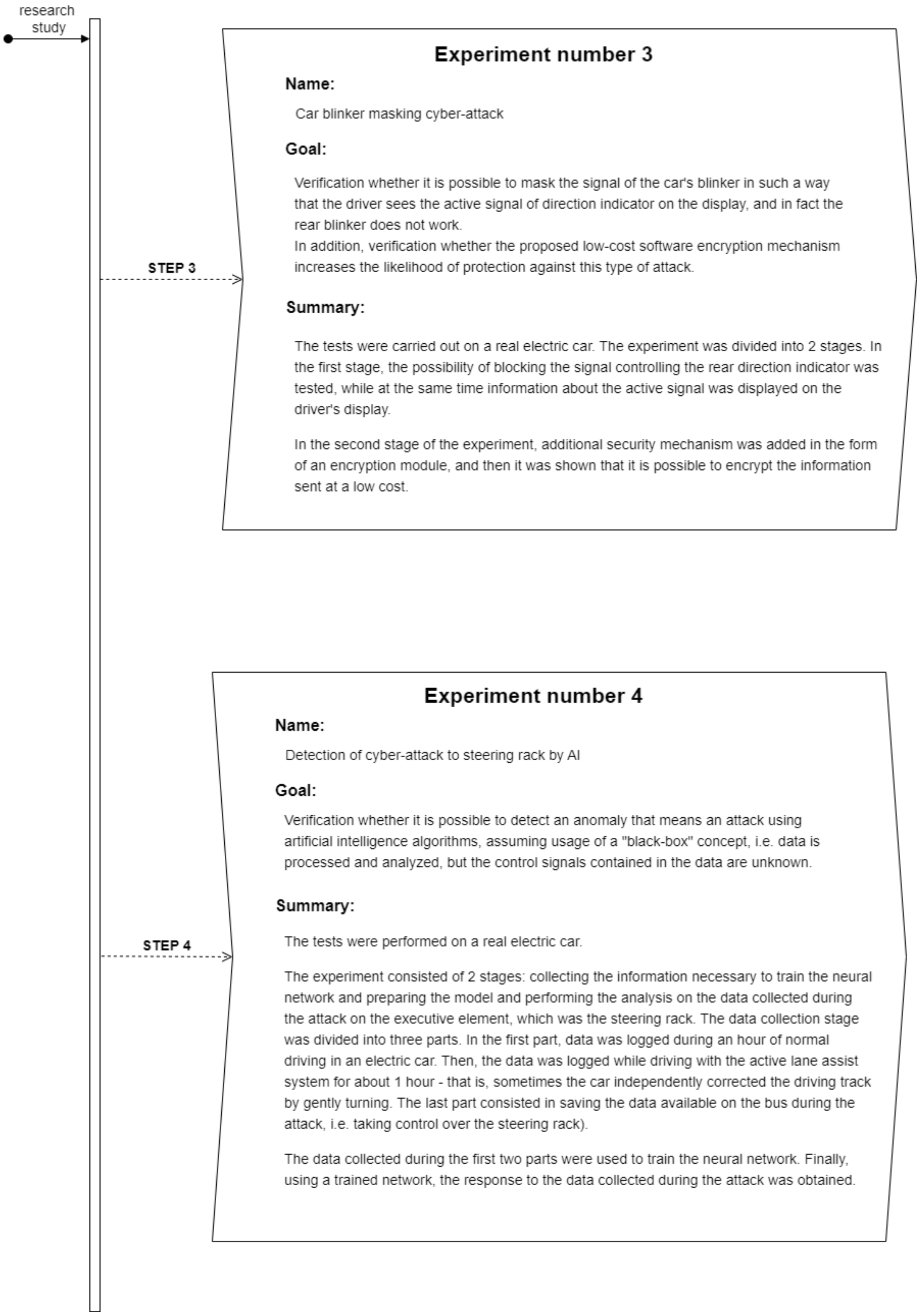
Summary:

The tests were performed on a real electric car. The epxeriment was divided into 2 stages. In the first stage, the possibility of reading information and transforming into a graph in real time along with the parallel exchange of signals in CAN frames was tested. The aim of the study was to check whether it is possible to continuously read the diagnostic values along with the simultaneous replacement of the content of CAN frames with different identifiers in such a way that the replacement was unnoticed by the vehicle.

In the second stage of experiment, the test scenario was extended with the possibility of replacing the brake control signal. The purpose of the study was also to check whether it is possible to continuously replace the diagnostic signals with the parallel replacement of the brake control signal in such a way that the replacement would be unnoticed by the vehicle.

During the diagnostic sessions, the author's concept of software test points was also used, thanks to which it was possible to latch the set values and use them at a given moment of time.

During the tests, the shared memory mechanism of the E200 device was used, thanks to which it was possible to transmit diagnostic data directly via the Ethernet interface without burdening the CAN bus with additional CAN frames.



Experiment number 3

Name:

Car blinker masking cyber-attack

Goal:

Verification whether it is possible to mask the signal of the car's blinker in such a way that the driver sees the active signal of direction indicator on the display, and in fact the rear blinker does not work.
In addition, verification whether the proposed low-cost software encryption mechanism increases the likelihood of protection against this type of attack.

Summary:

The tests were carried out on a real electric car. The experiment was divided into 2 stages. In the first stage, the possibility of blocking the signal controlling the rear direction indicator was tested, while at the same time information about the active signal was displayed on the driver's display.

In the second stage of the experiment, additional security mechanism was added in the form of an encryption module, and then it was shown that it is possible to encrypt the information sent at a low cost.

Experiment number 4

Name:

Detection of cyber-attack to steering rack by AI

Goal:

Verification whether it is possible to detect an anomaly that means an attack using artificial intelligence algorithms, assuming usage of a "black-box" concept, i.e. data is processed and analyzed, but the control signals contained in the data are unknown.

Summary:

The tests were performed on a real electric car.

The experiment consisted of 2 stages: collecting the information necessary to train the neural network and preparing the model and performing the analysis on the data collected during the attack on the executive element, which was the steering rack. The data collection stage was divided into three parts. In the first part, data was logged during an hour of normal driving in an electric car. Then, the data was logged while driving with the active lane assist system for about 1 hour - that is, sometimes the car independently corrected the driving track by gently turning. The last part consisted in saving the data available on the bus during the attack, i.e. taking control over the steering rack).

The data collected during the first two parts were used to train the neural network. Finally, using a trained network, the response to the data collected during the attack was obtained.

Fig. 37 Overview of research study splitted into experiments

3.1 Time-window concept for internal ambient light devices

The objective of this investigation was to perform a comparative examination of the vulnerability to an attack on the executive module that is controlled by the CAN FD bus. The experiment was performed in three scenarios:

A. employing the time windows approach to establish the validity of signals,
B. using transmission with End-to-End protection,
C. using standard transmission.

The current study is based on the application of software modifications. The software is characterized by a very important advantage to modify and adapt easily to technological requirements. The updating the software is substantially cheaper in comparison to modification of the hardware structure.

The element that was attacked in this experiment is marked in the Fig. 38 and corresponds to interior ambient lighting.

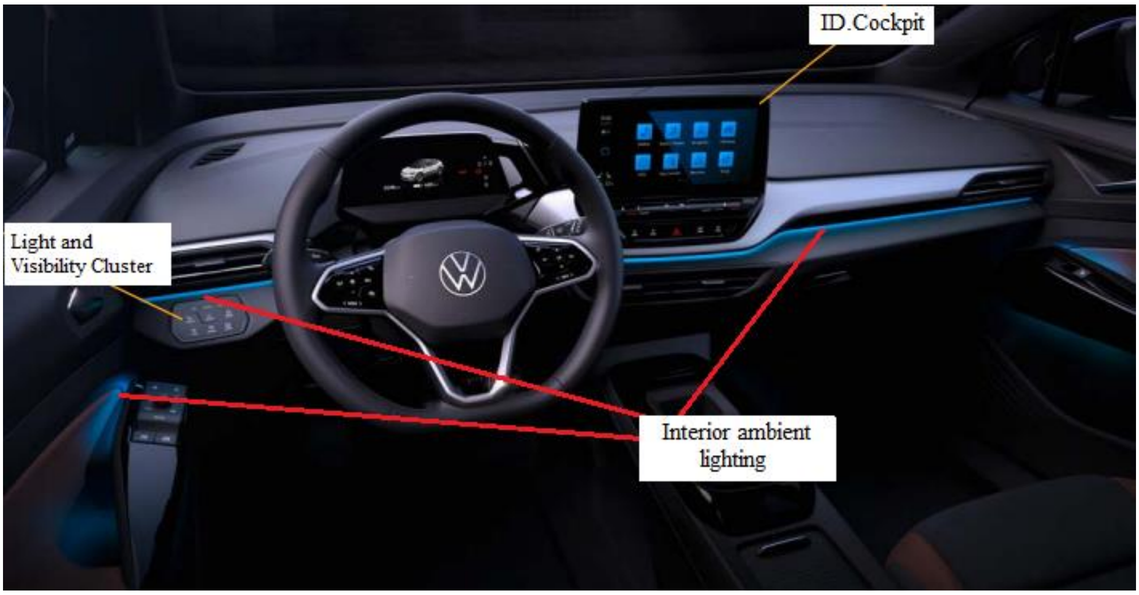


Fig. 38 Interior ambient lighting

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Plan of the experiment

In the experiment an attack was prepared using a method of recreating previously recorded data transmission. The first step is to connect an additional device to the data transmission bus, which can register frames responsible for controlling a given module (e.g., switching on or off a selected LED channel) during its regular operation. Then the recorded scenarios are being played back by the intruder module at the selected moment, see Fig. 39. The expected result is to activate the attacked module after playing the recorded data sentence.

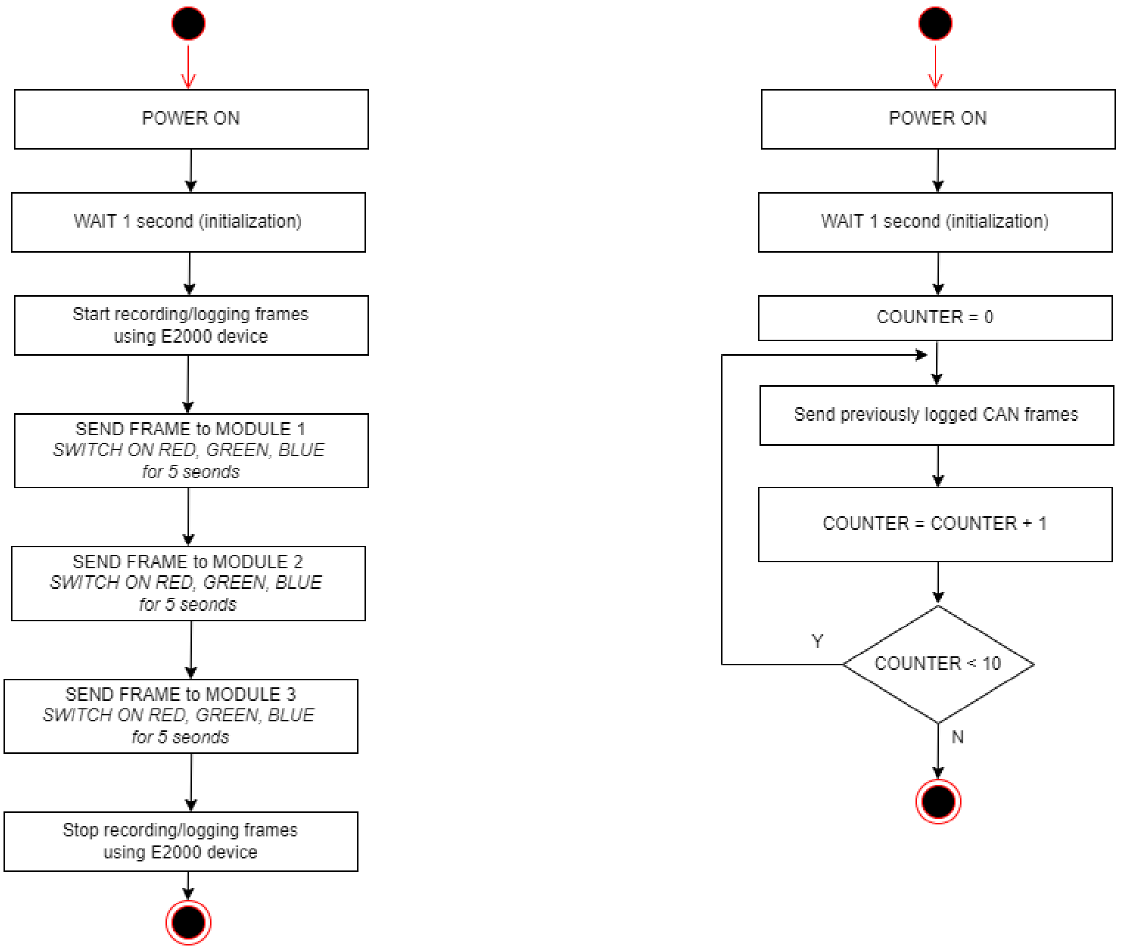
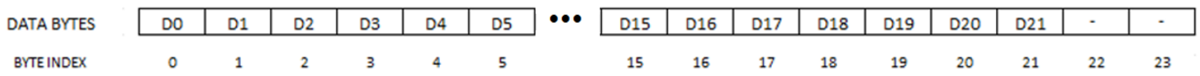

POWER ON
WAIT 1 second (initialization)
Start recording/logging frames using E2000 device
SEND FRAME to MODULE 1
SWITCH ON RED, GREEN, BLUE
for 5 seonds
SEND FRAME to MODULE 2
SWITCH ON RED, GREEN, BLUE
for 5 seonds
SEND FRAME to MODULE 3
SWITCH ON RED, GREEN, BLUE
for 5 seonds
Stop recording/logging frames using E2000 device
POWER ON
WAIT 1 second (initialization)
COUNTER = 0
Send previously logged CAN frames
COUNTER = COUNTER + 1
COUNTER < 10
Y
N

Fig. 39 Algorithm to perform attack

Three different transmission variants on the CAN bus were tested:

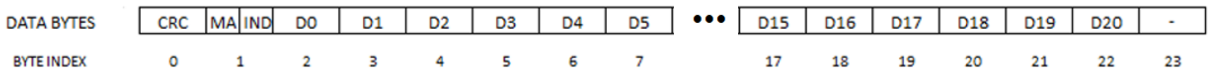
A. standard transmission (only control information is contained in the frame in the data field)



DATA BYTES	D0	D1	D2	D3	D4	D5	•••	D15	D16	D17	D18	D19	D20	D21	-	-
BYTE INDEX	0	1	2	3	4	5		15	16	17	18	19	20	21	22	23

Fig. 40 Standard transmission data

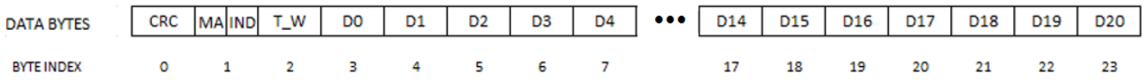
B. transmission using the End-to-End protection control mechanism



DATA BYTES	CRC	MA	IND	D0	D1	D2	D3	D4	D5	•••	D15	D16	D17	D18	D19	D20	-
BYTE INDEX	0	1		2	3	4	5	6	7		17	18	19	20	21	22	23

Fig. 41 End-to-End protection data

C. transmission using the End-to-End Protection control mechanism and additional protection in the form of a time window for which the signals in the frame are valid



DATA BYTES	CRC	MA	IND	T_W	D0	D1	D2	D3	D4	•••	D14	D15	D16	D17	D18	D19	D20
BYTE INDEX	0	1		2	3	4	5	6	7		17	18	19	20	21	22	23

Fig. 42 Ent-to-End protection with time window data

where:

CRC – cyclic redundancy check, used to detect random errors that occur during the transfer and storage of the binary data

IND – index of a key used for the E2E protection (range: 0..15)

T_W – timestamp defining a valid time window, 8-bit time window alive counter

D0 .. *D23* – data bytes of the CAN FD frame with length = 24

Detailed structures of frames from Fig. 40, Fig. 41 and Fig. 42 are shown in appendix in Fig. 83, Fig. 84 and Fig. 85.

Regardless of the selected variant, the CAN FD bus standard was used in the experiment. It is because the standard CAN frame is characterized by too short data field to be able to put there all required control signals in one message.

During tests performed for variants B and C, the CAN FD bus with the End-to-End protection (E2E) mechanism was used. It ensures the appropriate order of delivered frames. This also means that frame skipping is eliminated, and it is easier to detect bit swapping during transmission. The proposed approach consists in calculating the checksum from the data field starting from byte number 1 (byte number 0 contains information about the value of the calculated CRC) based on the key built into the module. Each executive module stores 16 key values depending on the current index, which varies from 0 to 15 according to the relation index = (index+1)%16. The algorithm for calculating the CRC is publicly known, so having a sufficiently large number of captures from the data bus (so-called logs) the proper software can be developed. This software recreates the 16 key values for the module. However, it should be noted that the E2E mechanism is not used for data encryption. The signal values are sent openly, so by eavesdropping on the bus and analyzing the current index, one can send a previously registered frame with the next index and attack the executive module. The aim of the presented research was to check the resistance to attacks consisting in recording transmissions and then sending previously saved frames to the bus.

In addition, for variant C, it was proposed to add a mechanism to minimize the risk of such an attack by adding supplementary information to the data field (so-called time window marker) shown in Fig. 43. This is the current value of an alive counter based on the current time counted from the start of the entire system. The time window counter is incremented each 100ms. Its initial value is initialized with a special frame sent by the device controlling the remaining modules at a system start-up, and then it is synchronized at a specified time (in this study a period of 10 seconds was assumed). The executive module, receiving a new frame with control data, checks whether the frame includes a valid time stamp before processing the data.

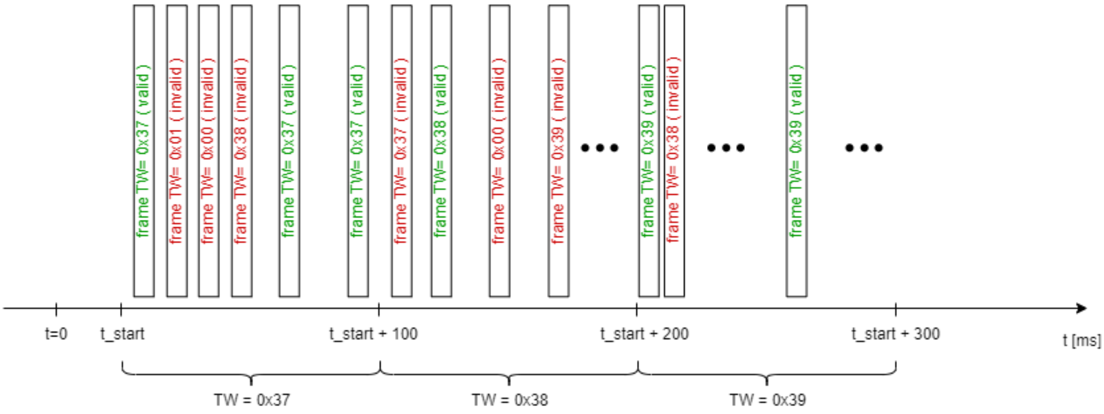


Fig. 43 Time window concept

Research environment / test bench

The test devices and environment used in the study consisted of a master module and 3 executive modules responsible for controlling LED lighting, communicating with each other via the CAN FD bus. In addition, the MicroDAQ E2000 (shown in Fig. 45) intruder module was attached to the bus, which was used to record the original frames and then play them back. The architecture of this system is shown in Fig. 44.

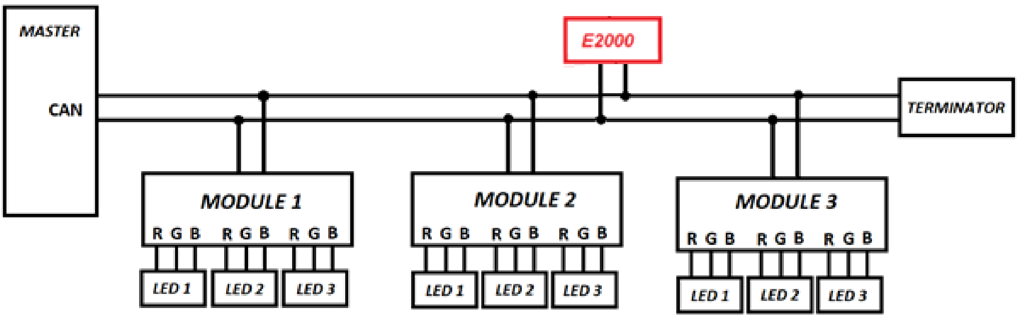


Fig. 44 Diagram of the test system

Each module contains 3 LEDs controlled by PWM. It was assumed that the information controlling a single LED is on 7 bytes: the PWM value for each channel is sent on 2 bytes (i.e., the maximum value is 65535) and the value of the lighting time is written on 1 byte. In the module a space was reserved for the 4-bit module address, which is placed depending on the variant as a separate byte or for the variant with E2E it uses the remaining 4 free bits on the first byte. Summing up, to control the module with 3 LEDs as an actuator via the CAN bus, depending on the variant, 22, 23 or 24 bytes were needed – a detailed description of the data field is presented in Tab. 2.

Tab. 2 Table of data bytes order for 3 variants in experiment

BYTE	**VARIANT A (NO E2E)**	**VARIANT B (E2E)**	**VARIANT C (E2E+TW)**
0	MOD_ADDR	CRC	CRC
1	PWM_LED_1_R_L	MOD_ADDR + E2E_KEY_IND	MOD_ADDR + E2E_KEY_IND
2	PWM_LED_1_R_H	PWM_LED_1_R_L	TIME_WINDOW
3	PWM_LED_1_G _L	PWM_LED_1_R_H	PWM_LED_1_R_L
4	PWM_LED_1_G_H	PWM_LED_1_G _L	PWM_LED_1_R_H
5	PWM_LED_1_ B _L	PWM_LED_1_G_H	PWM_LED_1_G _L
6	PWM_LED_1_ B _H	PWM_LED_1_ B _L	PWM_LED_1_G_H
7	LED_1_TIME_ON	PWM_LED_1_ B _H	PWM_LED_1_ B _L
8	PWM_LED_2_R_L	LED_1_TIME_ON	PWM_LED_1_ B _H
9	PWM_LED_2_R_H	PWM_LED_2_R_L	LED_1_TIME_ON
10	PWM_LED_2_G _L	PWM_LED_2_R_H	PWM_LED_2_R_L
11	PWM_LED_2_G_H	PWM_LED_2_G _L	PWM_LED_2_R_H
12	PWM_LED_2_ B _L	PWM_LED_2_G_H	PWM_LED_2_G _L
13	PWM_LED_2_ B _H	PWM_LED_2_ B _L	PWM_LED_2_G_H
14	LED_2_TIME_ON	PWM_LED_2_ B _H	PWM_LED_2_ B _L
15	PWM_LED_3_R_L	LED_2_TIME_ON	PWM_LED_2_ B _H
16	PWM_LED_3_R_H	PWM_LED_3_R_L	LED_2_TIME_ON
17	PWM_LED_3_G _L	PWM_LED_3_R_H	PWM_LED_3_R_L
18	PWM_LED_3_G_H	PWM_LED_3_G _L	PWM_LED_3_R_H
19	PWM_LED_3_ B _L	PWM_LED_3_G_H	PWM_LED_3_G _L
20	PWM_LED_3_ B _H	PWM_LED_3_ B _L	PWM_LED_3_G_H
21	LED_3_TIME_ON	PWM_LED_3_ B _H	PWM_LED_3_ B _L
22	---	LED_3_TIME_ON	PWM_LED_3_ B _H
23	---	---	LED_3_TIME_ON

where:

NO E2E – without End-to-End protection

E2E – with End-to-End protection

E2E + TW – with End-to-End protection and using a time window concept

CRC – check sum for End-to-End protection

MOD_ADDR – 4-bit module address

E2E_KEY_IND – key index for End-to-End protection, range: 0..15

PWM_LED_1_R_L – PWM low significant byte for channel number 1 and red color

PWM_LED_1_R_H – PWM high significant byte for channel number 1 and red color

PWM_LED_1_G_L – PWM low significant byte for channel number 1 and green color

PWM_LED_1_G_H – PWM high significant byte for channel number 1 and green color

PWM_LED_1_B_L – PWM low significant byte for channel number 1 and blue color

PWM_LED_1_B_H – PWM high significant byte for channel number 1 and blue color

LED_1_TIME_ON – time of switching LED to “on” position for channel number 2

PWM_LED_2_R_L – PWM low significant byte for channel number 2 and red color

PWM_LED_2_R_H – PWM high significant byte for channel number 2 and red color

PWM_LED_2_G_L – PWM low significant byte for channel number 2 and green color

PWM_LED_2_G_H – PWM l high significant byte for channel number 2 and green color

PWM_LED_2_B_L – PWM low significant byte for channel number 2 and blue color

PWM_LED_2_B_H – PWM high significant byte for channel number 2 and blue color

LED_2_TIME_ON – time of switching LED to “on” position for channel number 2

PWM_LED_3_R_L – PWM low significant byte for channel number 3 and red color

PWM_LED_3_R_H – PWM high significant byte for channel number 3 and red color

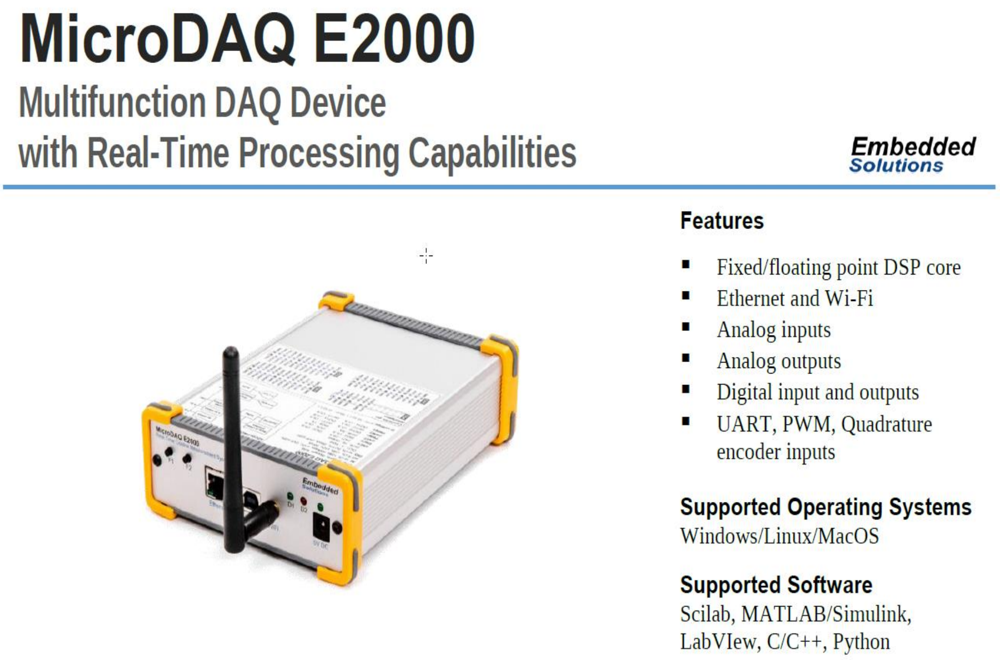
PWM_LED_3_G_L – PWM low significant byte for channel number 3 and green color

PWM_LED_3_G_H – PWM high significant byte for channel number 3 and green color

PWM_LED_3_B_L – PWM low significant byte for channel number 3 and blue color

PWM_LED_3_B_H – PWM high significant byte for channel number 3 and blue color

LED_3_TIME_ON – time of switching LED to “on” position for channel number 3



MicroDAQ E2000

Multifunction DAQ Device with Real-Time Processing Capabilities

Embedded Solutions

Features

- Fixed/floating point DSP core
- Ethernet and Wi-Fi
- Analog inputs
- Analog outputs
- Digital input and outputs
- UART, PWM, Quadrature encoder inputs

Supported Operating Systems

Windows/Linux/MacOS

Supported Software

Scilab, MATLAB/Simulink, LabVIew, C/C++, Python

Fig. 45 MicroDAQ E2000 device

Verification tests

The first stage of the verification tests was based on recording the transmission on the CAN bus during regular operation, when the executive modules were activated. The goal of the tests was to determine the feasibility of a successful attack of the frame scenario type. The frames were recorded while switching on successive channels of LEDs to “on” position for all modules, i.e. the first red, green and blue channels. The lighting time of the diode connected to the specific channel was about 5 seconds. Then, after selecting frames from a certain time, they were played back and sent to the bus. The subject of the observation was to check whether it is possible to control the required module by replaying previously recorded frames in 4 cases: when reproducing the full sequence of recorded frames and a 75%, 50% and 25% recorded frames sent during the original time interval. Each test was performed 10 times.

The tests were carried out for 3 different variants of CAN transmission:

A. transmission using the CAN FD bus, the length of the data field is 24 bytes, no additional protection during transmission
B. transmission using the CAN FD bus, the length of the data field is 24 bytes, the End- to-End protection, i.e. a mechanism protecting against losing a frame or changing the value of signals in a frame
C. transmission using the CAN FD bus, the length of the data field is 24 bytes, the End- to-End protection with an additional mechanism determining the validity of signals in a specific time (TW - time window). The duration of the time window validity was set to 100ms

The results of the verification tests performed are presented in Tab. 3:

Tab. 3 Results of verification tests for time window experiment

variant	**100% logged frames**		**75% of logged frames**		**50% of logged frames**		**25% of logged frames**	
	success	trials	success	trials	success	trials	success	trials
A	10	10	10	10	10	10	10	10
B	1	10	2	10	0	10	1	10
C	0	10	0	10	0	10	0	10

Tab. 4 Results of the effectiveness of the attacks carried out

variant	**100% logged frames**	**75% of logged frames**	**50% of logged frames**	**25% of logged frames**
	effectiveness	effectiveness	effectiveness	effectiveness
A	100%	100%	100%	100%
B	10%	20%	0%	10%
C	0%	0%	0%	0%

Conclusions

The proposed approach consisting in the implementation of the additional time window marker mechanism significantly increased the security of the data transmission on the CAN bus. As it is presented in Tab. 4, the effectiveness of attacks in case of secured by time window method dropped to zero. This mechanism increased the system resistance to attacks consisting in recording and replaying a recorded scenario to take control over the executive module. Analyzing the test results from attempts to take control over the module based on previously recorded transmissions and its playback, it can be concluded that it was not possible to take control over the attacked module in the case of using the End-to-End protection mechanism and an additional time window marker. However, the chance of a successful attack remains if an unsolicited intruder frame is sent in the same time window as the original frame, albeit significantly minimized.

The obtained results indicate the need to conduct further research to determine the optimal (minimum) length of time windows, ensuring correct transmission.

Entering the time window helps to identify whether the signals in a frame are valid or not, which prevents identical data fields from being reproduced later. Moreover, the additional protection can be obtained by using XOR operation on each byte of the data field, which masks the signal values and prevents eavesdropping. The signals are then not sent explicitly.

However, the implementation of this solution is related to meeting additional requirements, including the need of installing a real-time clock on each module and to synchronize the clocks of all modules on the bus. In addition, a redundant data field must be used to transmit the time window stamp value, which may reduce the capacity of the data field in the CAN frame. Nevertheless, in most cases it is not critical, because the CAN FD protocol provides the possibility of using as much as 64 bytes of data in one frame.

3.2 Diagnostics with injection

The purpose of this experiment was to analyze the possibility of performing a full diagnostic of a car vehicle module during its regular operation, i.e. in real conditions. It was assumed that to obtain defined test conditions, it is necessary to inject information and replace it in the captured CAN frames in real time. In the conducted research, the mechanism of latching key signals from the point of view of diagnostics, reading of variable values was used, while maintaining the original time cycles. Thanks to the mechanism of information latching and triggering them at a certain time and then reading them through shared memory, the need to expand the communication matrix with subsequent debug messages that would increase the degree of bus occupancy was eliminated. The attacked elements of the car are shown in Fig. 46 and corresponds to the braking system.

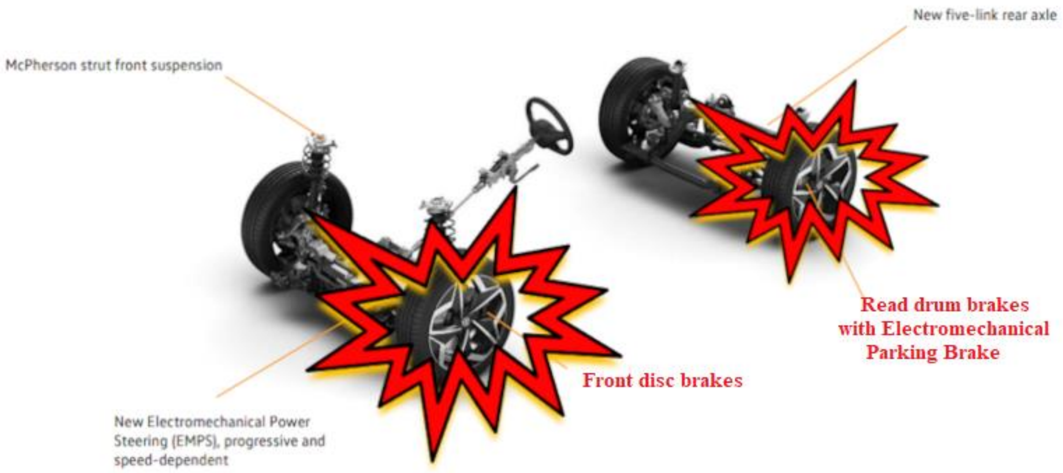


Fig. 46 Braking system

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Plan of the experiment

The experiment was aimed at verifying whether it is possible to exchange signals within the CAN in a way that is invisible to the vehicle undergoing a diagnostic procedure. The research was divided into 2 stages. The duration of each session was 2 minutes and was repeated 3 times. In the first stage (see Fig. 47), it was checked whether it is possible to simultaneously exchange signals in a larger number of frames on the CAN bus in a way imperceptible to the vehicle when reading diagnostic parameters. The test carried out included the current reading of parameters in the frame containing information about the current pressure in the brake system. Diagnostic data received from the device were directly processed and transformed into a graph. Such approach let us make possible to observe and analyze signals in real time. At the same time, during the diagnostic procedure, the maximum number of frames that can be replaced in real time was experimentally tested so that it would not be detected by the vehicle system. The tests were planned for the exchange of signals in 1, 5, 10, 15 and 20 CAN frames.

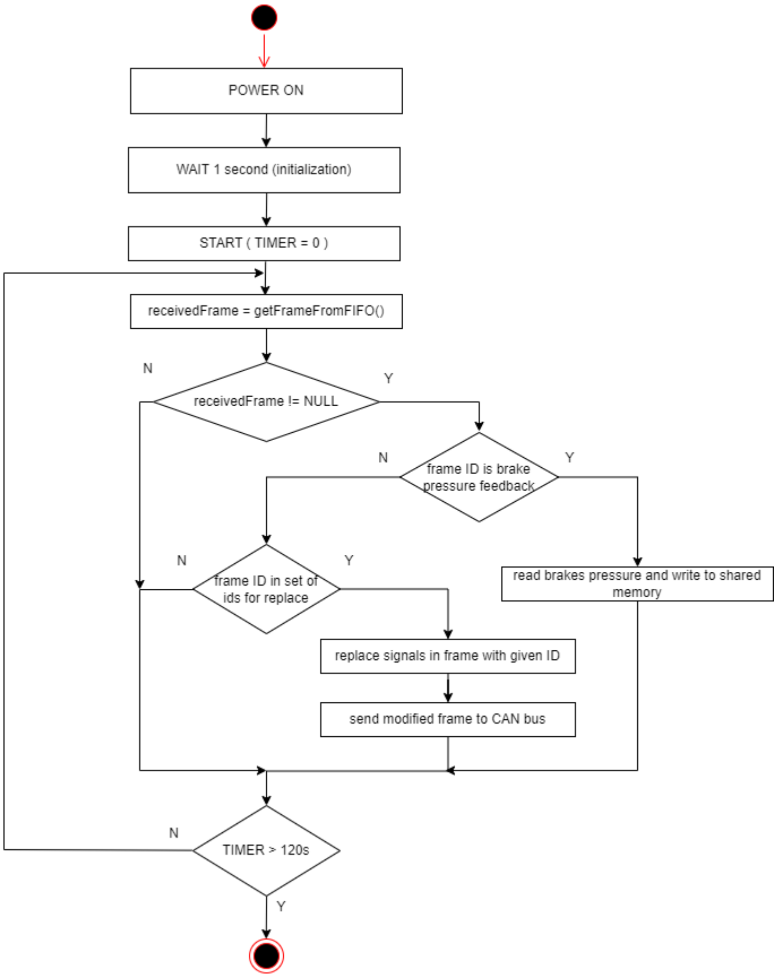

POWER ON
WAIT 1 second (initialization)
START (TIMER = 0)
receivedFrame = getFrameFromFIFO()
N
receivedFrame != NULL
Y
N
frame ID is brake pressure feedback
Y
N
frame ID in set of ids for replace
Y
read brakes pressure and write to shared memory
replace signals in frame with given ID
send modified frame to CAN bus
N
TIMER > 120s
Y

Fig. 47 Block diagram of the first stage of experiment

In the second stage of the experiment (see Fig. 48), it was checked whether it is possible to read any information contained in CAN frames with specific identifiers and to replace the value of the desired signal when required by the diagnostic procedure. Because only information about the current signal state is sent in the current CAN frame, it was sometimes necessary to latch the signal values in the module memory to use them at the desired moment. This functionality was available since one used the so-called software test points. During the tests, the shared memory mechanism was used as a mechanism for communication between the device subjected to the diagnostic procedure and the computer. The exchange of information by means of memory and then communication via the Ethernet interface, a 2-way data transmission made it possible to perform the attack in such way that practically did not affect the timing and load of the CAN bus with additional diagnostic messages. In the test, the flow values for the brake master cylinder were set (replacement of the signal control values along with the calculation of the checksum for the entire frame) and at the same time the parameters of the current pressure in the brake system were read out. In addition, frames with subsequent identifiers containing previously captured signal values were replaced. The tests of signal substitution were carried out for: 1, 5, 10, 15 and 20 CAN frames.

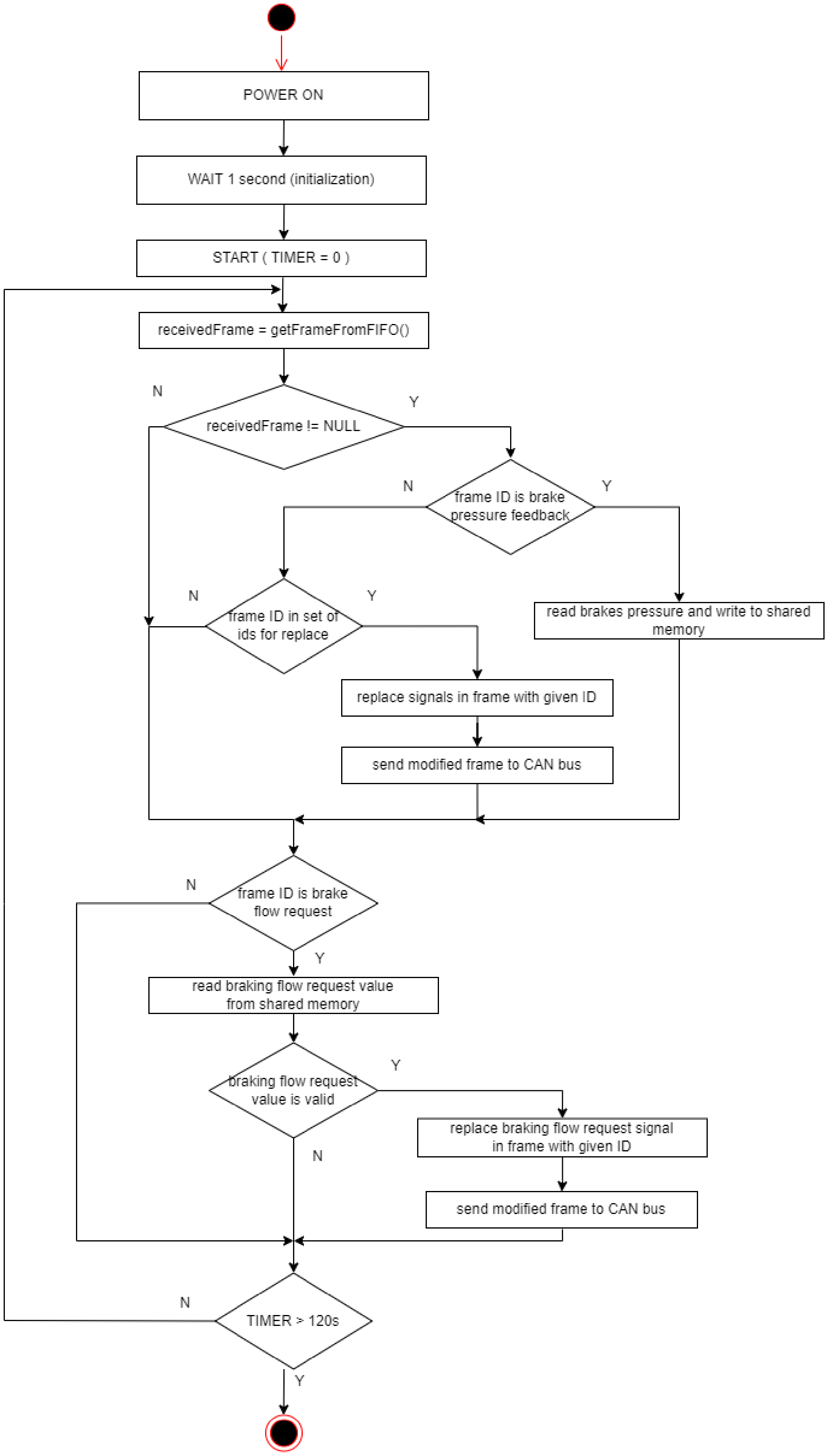

POWER ON
WAIT 1 second (initialization)
START (TIMER = 0)
receivedFrame = getFrameFromFIFO()
N
Y
receivedFrame != NULL
N
Y
frame ID is brake pressure feedback
N
Y
frame ID in set of ids for replace
read brakes pressure and write to shared memory
replace signals in frame with given ID
send modified frame to CAN bus
N
frame ID is brake flow request
Y
read braking flow request value from shared memory
Y
braking flow request value is valid
replace braking flow request signal in frame with given ID
N
send modified frame to CAN bus
N
TIMER > 120s
Y

Fig. 48 Block diagram of the second stage of experiment

Research environment / test bench

A real electric car was subjected to implementing the diagnostic procedures. Therefore, it was necessary to prepare points of entry into the communication system between electronic control units using the CAN bus. The best place for all CAN buses is the gateway. It is a reason why it was removed and connected to the rest of the test system using additional cables and adapters (shown in Fig. 50). Since the tests were carried out during the regular operation of the car, it was necessary to meet very strict time requirements for processing the information to be exchanged and reading the status of the parameters. It was important not to introduce the tested electronic system into an error state. Therefore, the very high efficiency of dedicated equipment became a critical parameter. During the preparations for the tests, it was estimated that in time of the manipulation of the transmitted signals, the time between the last byte of the received original frame and the last byte of the modified frame must be equal to less than one millisecond. This is due to the architecture of modern ECUs (Electronic Control Unit), whose operating systems in terms of schedules operate with a resolution of 1 millisecond. Such high performance is also required due to the necessity to modify the signals contained in the CAN frame and to recalculate the checksum necessary in the End-to-End Protection (E2E) mechanism. During the diagnostic tests, the MicroDAQ E2000 device (Fig. 45) was used, which meets the above-mentioned requirements. It is equipped with dual-channel CAN FD communication with multi-core processing pipeline support. In addition, it offers the Wi-Fi and Ethernet interfaces, which were used to transmit two-way transmission of diagnostic signals. Thanks to this solution, the original communication between modules on the CAN bus was not disturbed or changed in any way. In addition, the process of reading the values of "latched parameters" also used direct access to shared memory, which is the fastest possible solution.

The MicroDAQ E2000 device was connected in series to the bus number 4, responsible for the braking system and steering gear, as shown in Fig. 49. The real connection of Microdaq E2000 device to a car system is shown in Fig. 50.

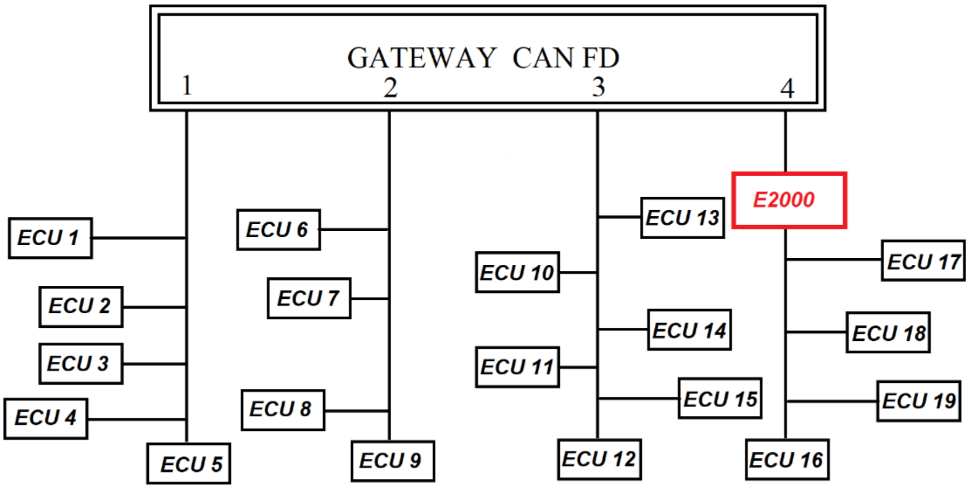


Fig. 49 Diagram of the system under test

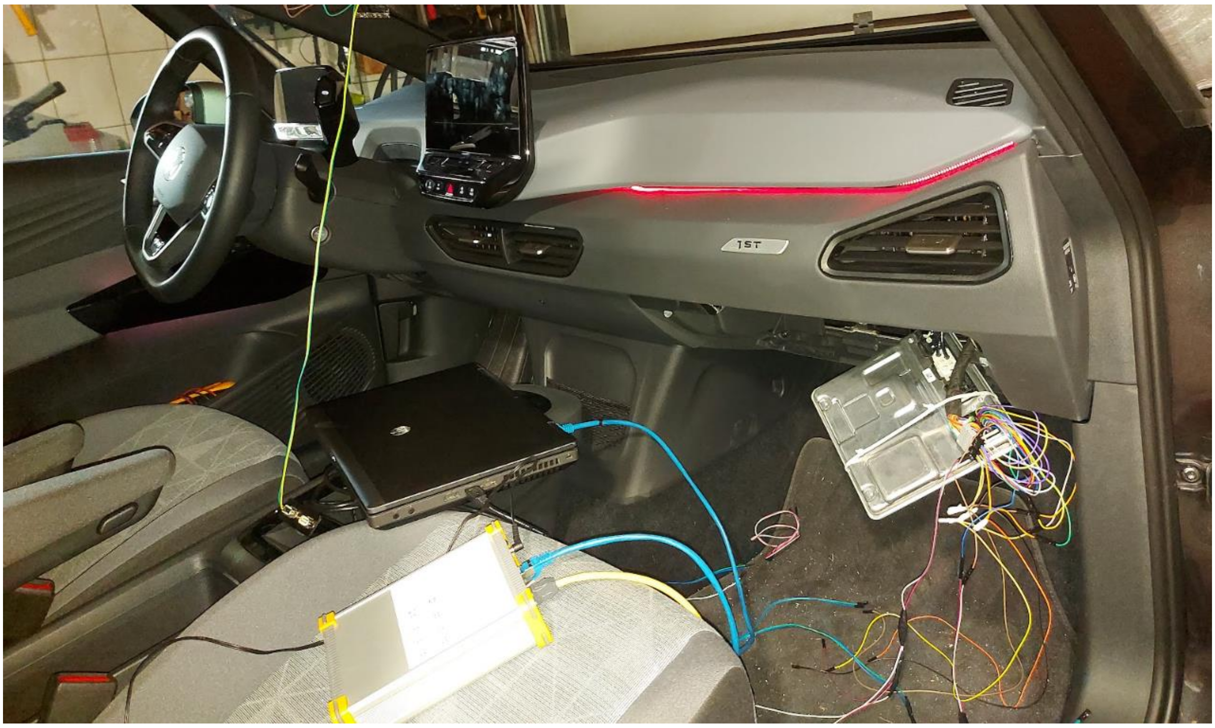


Fig. 50 Microdaq E2000 device connection to a car system

Verification tests

Two stages of research were carried out, each of them was the diagnostic session of duration equals to 2 minutes, and each session was repeated 3 times. The frames tested were the CAN FD frames with a length of 8 to 64 bytes and some of them used the End-to-End protection mechanism.

In the first stage, which included the current reading of parameters in the frame containing information about the current pressure in the braking system and the parallel replacement of the signal values in the frames, the results presented in Tab. 5 were obtained. All attempts to replace values within a maximum of 10 frames were successfully obtained. Diagnostic data received from the device were simultaneously directly processed and transformed into the graph. It let us make it practically possible to observe and analyze signals in the real time. An example of the values read using this method is shown in Fig. 51.

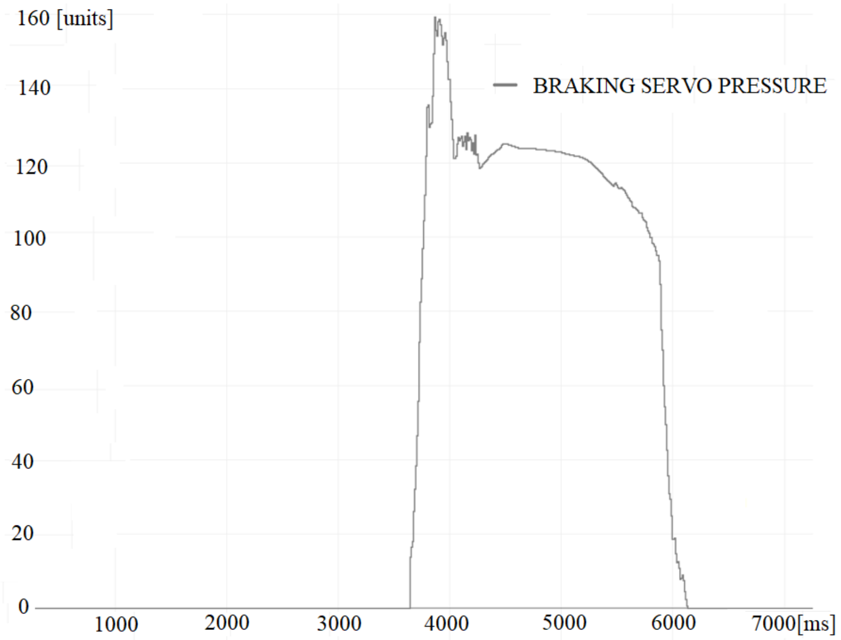


Fig. 51 Braking servo pressure feedback signal value

Tab. 5 Replaced frames efficiency results during reading diagnostic values

Number of replaced frames	**Success (no error detected) Session 1**	**Success (no error detected) Session 2**	**Success (no error detected) Session 3**
1	100 %	100 %	100 %
2	100 %	100 %	100 %
5	100 %	100 %	100 %
10	100 %	100 %	100 %
15	100 %	92 %	100 %
20	88 %	90 %	91%

In the second stage, the flow values or the brake pump were set (replacement of the signal control values along with the calculation of the checksum for the entire frame) and at the same time the parameters of the current pressure in the brake system were read out. Values of these signal are shown in Fig. 52. In addition, frames with subsequent identifiers containing previously captured signal values were replaced. The obtained results are presented in Tab. 6.

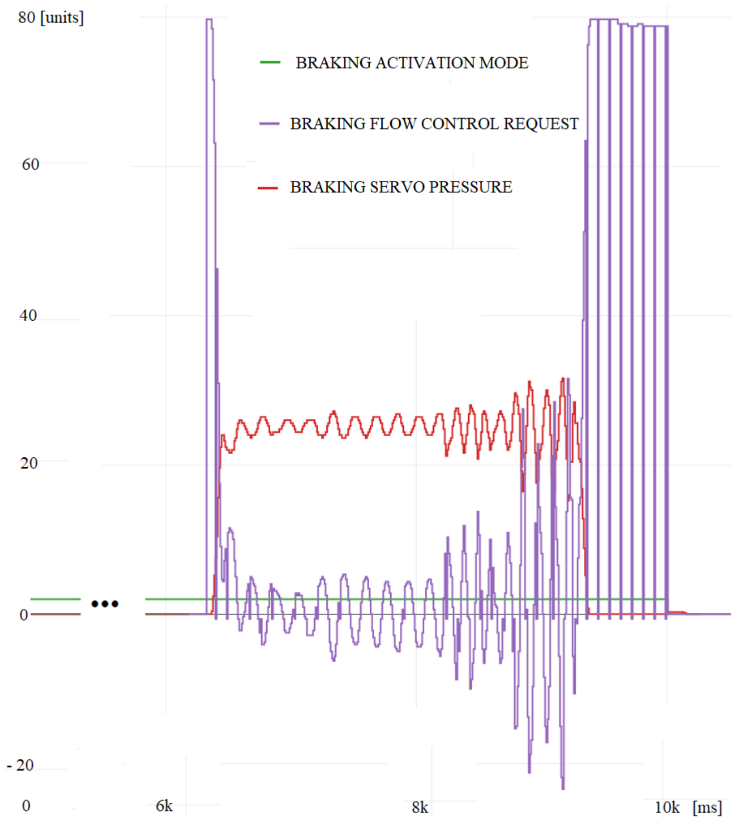


Fig. 52 Braking signal values

Tab. 6 Replaced frames efficiency results during reading and injecting diagnostic values

Number of replaced frames	**Success (no error detected) Session 1**	**Success (no error detected) Session 2**	**Success (no error detected) Session 3**
1	100 %	100 %	100 %
2	100 %	100 %	100 %
5	100 %	100 %	100 %
10	100 %	100 %	100 %
15	98 %	94 %	97 %
20	90 %	90 %	89 %

Conclusions

Implementation of mechanisms for reading values in the real time and the ability to inject values of the diagnostic signals allowed for the reconstruction of any test scenario. In this solution, the most important issue was that the input signals were not simulated, as is the case during the testing process, but the current real values were subjected to the diagnostics. Using the MicroDAQ E2000 device, it was possible to seamlessly send all frames in real time to the target diagnostic application. The use of software test points that allowed for latching values made it also possible to read buffered signal values. In addition, in parallel to the tests carried out in both stages, the maximum number of frames in which the signal values can be changed in a way imperceptible to the motor vehicle system was tested experimentally. The results obtained in the 3 series differ slightly from each other. The differences are mainly due to the time dependencies on the CAN bus, which affect the successive frames tested. The lengths of frames varied from 8 to 64 bytes. In addition, not all frames were characterized by the End-to-End Protection (E2E) mechanism implemented, so it was not always necessary to recalculate checksums, which took up additional processing time. However, it can be unequivocally stated that the MicroDAQ E2000 device used during the tests fully performed the task of both reading the signal value and injecting the value at the selected time while swapping frames, if the number of swapped frames was not greater than 10 each time.

3.3 Car blinker masking cyber-attack

The main purpose of the research conducted as a part of this experiment was to demonstrate that it is possible to successfully attack the electronic module in a car. The goal was to take control over a rear blinker. It was done through masking this information presented to the driver. Thus, the driver activating the indicator sees the expected status on the display, while the rear blinker does not work. In addition, an original concept of implementing additional low-cost protection of data transmission systems was proposed. Significantly hindering this type of attack, and then the effectiveness of its operation was verified. The proposed solution is based on a software approach to the topic of encryption, without the use of dedicated hardware modules, which, in addition decreases the cost of implementation as well as ensures easy modification and adaptation to the rapidly changing technologies. The attacked element in this experiment is marked in Fig. 53 and corresponds to rear blinker.

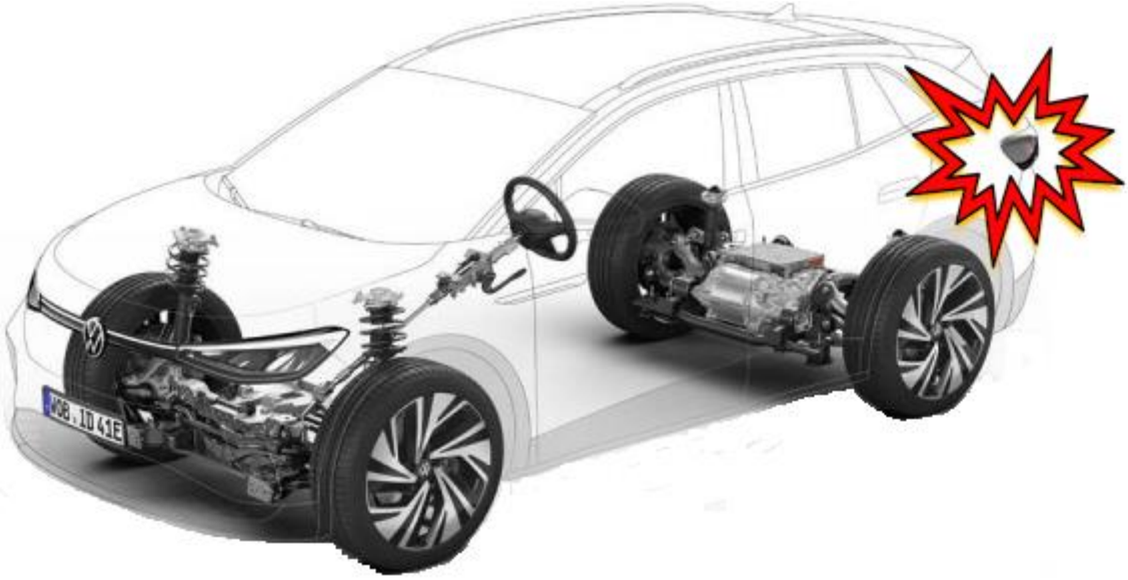


Fig. 53 Rear blinker

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Plan of the experiment

The research conducted during the experiment was divided into several stages. The main goal was to prove that it is possible to take control of the vehicle without having documentation describing in detail the information contained in the transmitted CAN frames. All control signals had to be found in advance. It was done using proprietary reverse-engineering methods. The target of the attack was the rear turn signal of the electric car. Moreover, making such an attack was hindered by additional assumption that the rear blinker signal is responsible for. During the attack its operation is inactive, while the driver constantly sees the status on the display confirming the correct operation of the blinker. The experiment also proves that a big threat is not only taking control of the main mechanisms in the vehicle, such as acceleration, braking or turning. Each takeover of control over a vehicle module can lead to unforeseen consequences. The applied approach, presented in Fig. 54, means that in the event of a successful attack even on the blinkers control signal, the result may be disastrous. The driver of the car number #2, approaching the red vehicle standing on the roadside, tries to avoid it, turns on the left turn signal and, convinced that he is signaling a left turn, enters the road of vehicle number #1 driving in the left lane. Throughout the turning maneuver, the driver is unaware of the attack in progress (that the rear turn signals are inoperative) because the correct status is displayed to him.

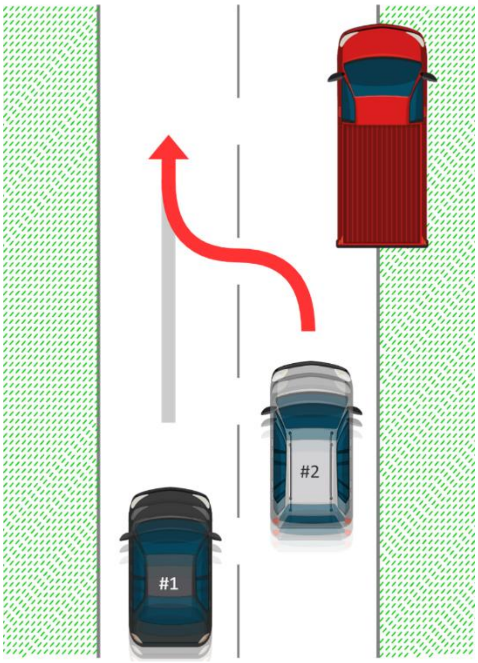


Fig. 54 Passing the stopped vehicle in the left lane

The first stage of the experiment consisted in collecting the appropriate amount of data from the CAN bus when the desired feature is not active, i.e., the direction indicators are turned off. At that time, the data was logged, which also included signals responsible for controlling the direction indicator when it is inactive. The research used the method presented in Fig. 55, which allowed to determine several CAN frame identifiers that could be responsible for controlling the direction indicator.

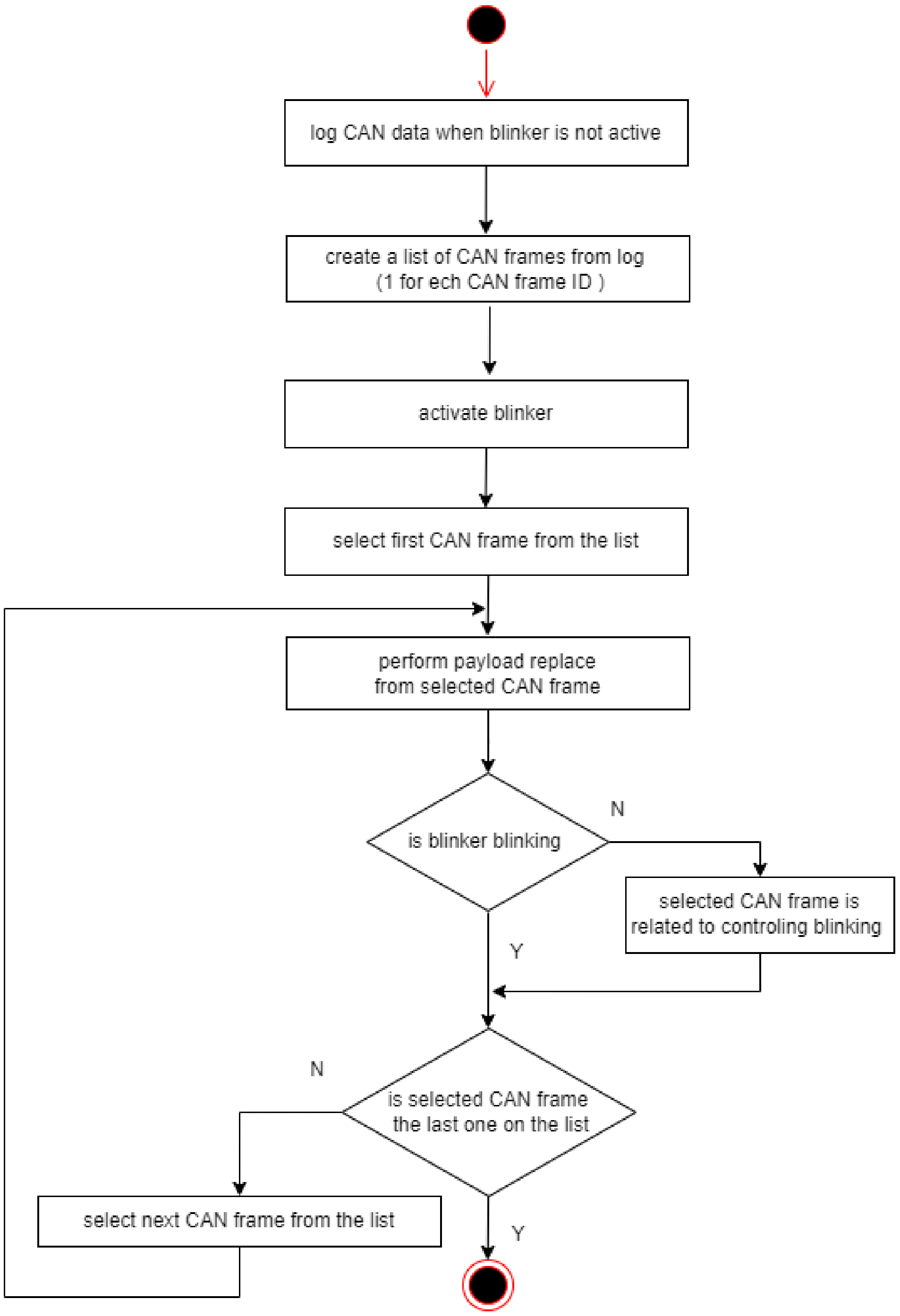

log CAN data when blinker is not active
create a list of CAN frames from log
(1 for ech CAN frame ID)
activate blinker
select first CAN frame from the list
perform payload replace
from selected CAN frame
is blinker blinking
N
selected CAN frame is
related to controling blinking
Y
N
is selected CAN frame
the last one on the list
select next CAN frame from the list
Y

Fig. 55 Block diagram of the research method to find CAN identifiers

Then, from the previously logged CAN frames, one frame was selected for each identifier. In this way, a list of CAN frames was created, which were used for substitution of the active signal. For each replaced frame, it was observed whether the blinker would stop working and if it was performed. This is the reason to qualify the identifier of a given CAN frame to the set of frames responsible for controlling the direction indicator. However, to make it possible to replace the CAN frames using a MicroDAQ E2000 device connected in series to the bus in a bridge mode, it was necessary to decode the keys to the End-to-End Protection (E2E) mechanism. Since the E2E protection method is not used for data encryption, but its task is to control the correctness of the CAN frame flow, the CRC calculation algorithm is publicly known. Therefore, it was possible to find the key values using the reverse engineering method and implementing a program that uses brute force. To perform it all the possible key values were checked, the CRC checksum was calculated on their basis and compared to the checksum saved in the logs. If the CRC values matched, it meant that the key was found. The key searches continued until 16 key values were found for indices 0 through 15. The entire process is shown in Fig. 56.

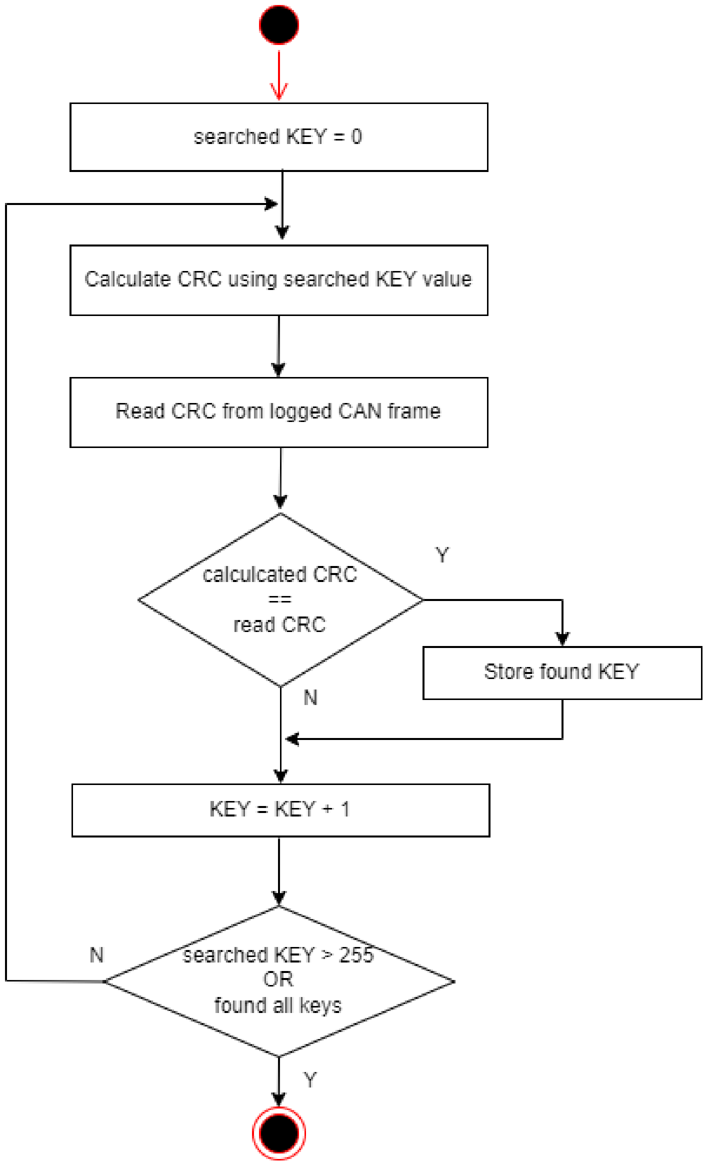


Fig. 56 Block diagram of searching E2E keys algorithm

Finally, having collected all potential CAN frames responsible for controlling the blinker it was needed to decode the signals (consecutive single bits) inside the CAN frames responsible for controlling the blinkers. To achieve it, a heat map concept was created to visualize graphical bits representation on the axe of time. On the vertical axis time is given, while all bits in CAN frame are shown on horizontal axis. So as the result the concept of graphical view for all bits in defined time was proposed, where white pixels represent a bit value equals to 0 and black pixels represent a bit value equals to1.

The exemplary heat map concept is shown in Fig. 57.

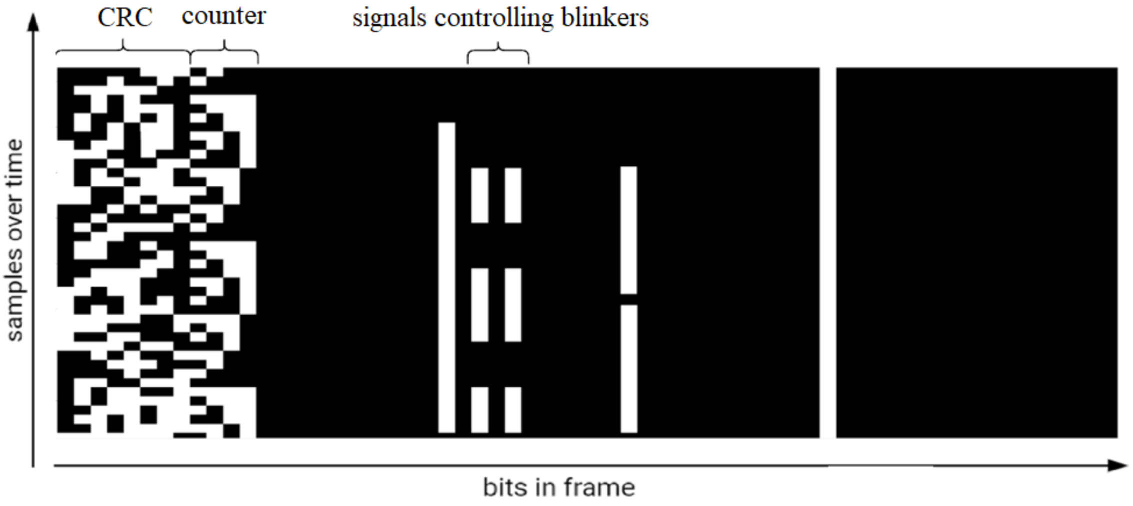


Fig. 57 Bits state visualization with the E2E protection

The last stage of the experiment consisted in testing the effectiveness of the proposed low-cost method of software encryption of CAN frame contents. The approach involves conducting the XOR operation on the data transmitted within CAN frames, with an emphasis on performing the XOR operation twice for dependency On the basis of these operations the initial value is being obtained. The main purpose of the proposed method is to make the decoding of control signals more difficult, e.g., using the methods presented earlier in this experiment. Since the research and tests were carried out on an electric car purchased in the showroom, and not on a test prototype, it was not possible to modify the software implemented in the control modules. Therefore, the simulation was made by adding 2 modules to the system: an encoder and a decoder. It should be stressed that the same effect if encryption was performed in the module transmitting the message and decryption on the receiving module were obtained.

Research environment / test bench

Therefore, the test object was a real car, it was necessary to prepare connection points to the communication system between electronic control units using the CAN bus. As it was described above during the tests the device was supposed to replace the CAN frames. One of the buses is coming directly from the main gateway was cut. At the same time, the device operating in the bridge mode was connected to the vehicle's communication system as shown in Fig. 58.

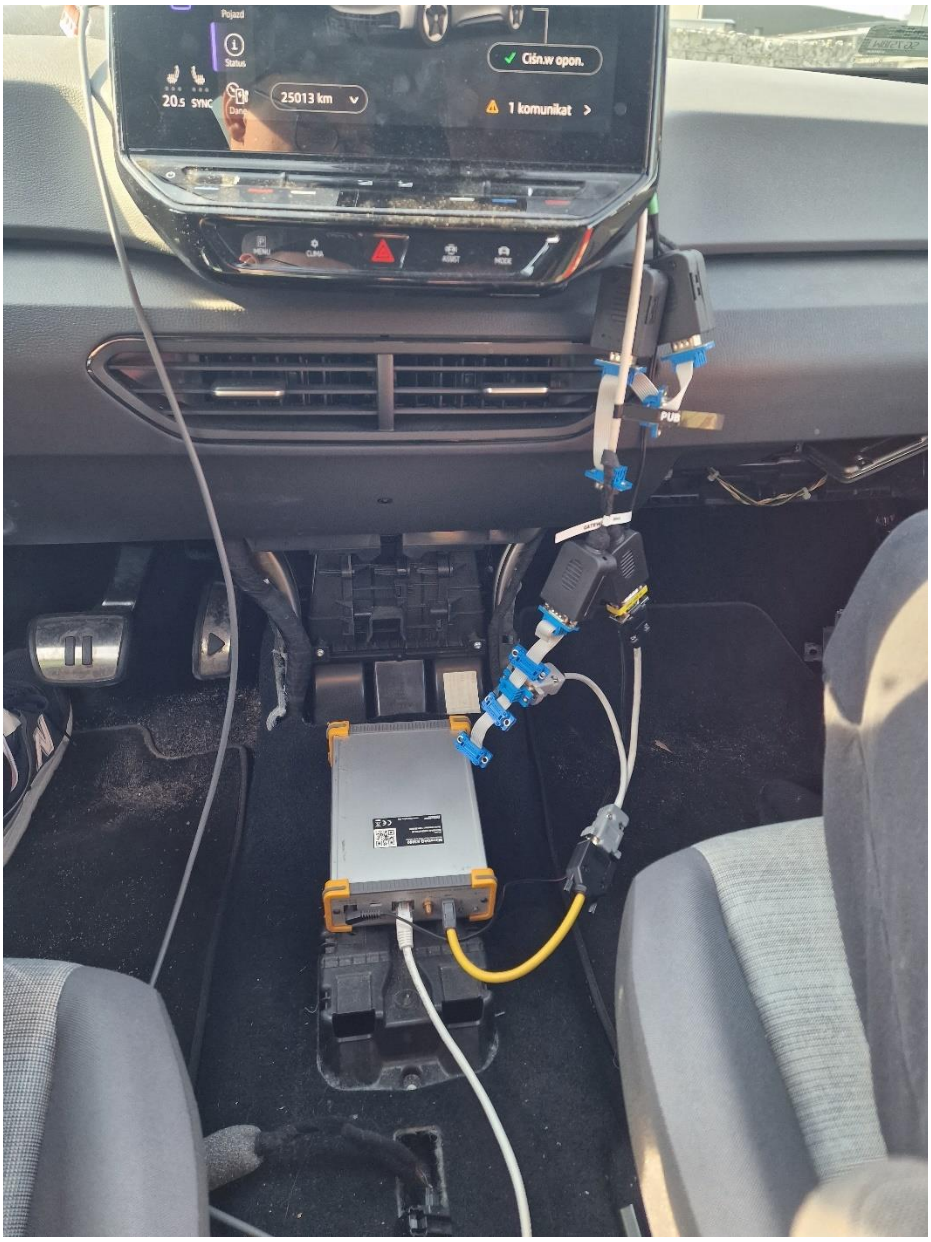
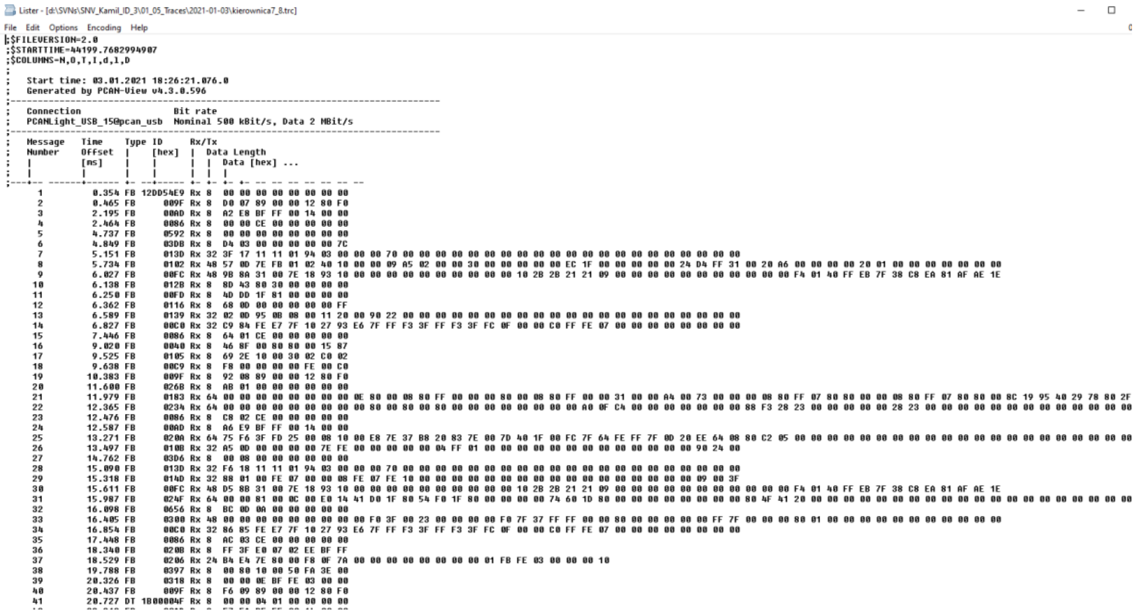


Fig. 58 Real car Microdaq E2000 device as a bridge connected to CAN bus

The first stage of the research consisted in logging the transmission when the blinker was turned off. The logging process was carried out using a standard PCAN-USB PRO device (shown in Fig. 59) available on the market. The obtained data was saved on the computer hard drive (example partial content of logged presented in Fig. 60).

Fig. 59 PCAN-USB PRO 2 channel CAN FD device


Lister - [d:\SVNs\SNV_Kamil_ID_3\01_05_Traces\2021-01-03\kierownica7_8.trc]
File
Edit
Options
Encoding
Help

```
;$FILEVERSION=2.0
;$STARTTIME=44199.7682994907
;$COLUMNS=N,O,T,I,d,l,D
;
;   Start time: 03.01.2021 18:26:21.076.0
;   Generated by PCAN-View v4.3.0.596
;-------------------------------------------------------------------------------
;   Connection                 Bit rate
;   PCANLight_USB_15@pcan_usb  Nominal 500 kBit/s, Data 2 MBit/s
;-------------------------------------------------------------------------------
;   Message   Time    Type ID     Rx/Tx
;   Number    Offset  |    [hex]  |  Data Length
;   |         [ms]    |    |      |  |  Data [hex] ...
;   |         |       |    |      |  |  |
;---+-- ------+------ +- --+----- +- +- +- +- -- -- -- -- -- --
      1         0.354 FB 12DD54E9 Rx 8  00 00 00 00 00 00 00 00
      2         0.465 FB     009F Rx 8  D0 07 89 00 00 12 80 F0
      3         2.195 FB     00AD Rx 8  A2 E8 BF FF 00 14 00 00
      4         2.464 FB     0086 Rx 8  00 00 CE 00 00 00 00 00
      5         4.737 FB     0592 Rx 8  00 00 00 00 00 00 00 00
      6         4.849 FB     03DB Rx 8  D4 03 00 00 00 00 00 7C
      7         5.151 FB     013D Rx 32 3F 17 11 11 01 94 03 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      8         5.734 FB     0102 Rx 48 57 0D 7E FB 01 02 40 10 00 00 09 A5 02 00 00 30 00 00 00 00 00 EC 1F 00 00 00 00 00 24 D4 FF 31 00 20 A6 00 00 00 00 20 01 00 00 00 00 00 00 00
      9         6.027 FB     00FC Rx 48 9B 8A 31 00 7E 18 93 10 00 00 00 00 00 00 00 00 00 00 10 2B 2B 21 21 09 00 00 00 00 00 00 00 00 00 00 00 F4 01 40 FF EB 7F 38 C8 EA 81 AF AE 1E
     10         6.138 FB     012B Rx 8  8D 43 80 30 00 00 00 00
     11         6.250 FB     00FD Rx 8  4D DD 1F 81 00 00 00 00
     12         6.362 FB     0116 Rx 8  68 0D 00 00 00 00 00 FF
     13         6.589 FB     0139 Rx 32 02 0D 95 0B 08 00 11 20 00 90 22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     14         6.827 FB     00C0 Rx 32 C9 84 FE E7 7F 10 27 93 E6 7F FF F3 3F FF F3 3F FC 0F 00 00 C0 FF FE 07 00 00 00 00 00 00 00 00
     15         7.446 FB     0086 Rx 8  64 01 CE 00 00 00 00 00
     16         9.020 FB     0040 Rx 8  46 8F 00 80 80 00 15 87
     17         9.525 FB     0105 Rx 8  69 2E 10 00 30 02 C0 02
     18         9.638 FB     00C9 Rx 8  F8 00 00 00 00 FE 00 C0
     19        10.383 FB     009F Rx 8  92 08 89 00 00 12 80 F0
     20        11.600 FB     026B Rx 8  AB 01 00 00 00 00 00 00
     21        11.979 FB     0183 Rx 64 00 00 00 00 00 00 00 00 0E 80 00 08 80 FF 00 00 00 80 00 08 80 FF 00 00 31 00 00 A4 00 73 00 00 00 08 80 FF 07 80 80 00 00 08 80 FF 07 80 80 00 8C 19 95 40 29 78 80 2F
     22        12.365 FB     0234 Rx 64 00 00 00 00 00 00 00 00 00 80 00 80 00 80 00 00 00 00 00 00 00 00 A0 0F C4 00 00 00 00 00 00 00 88 F3 28 23 00 00 00 00 00 28 23 00 00 00 00 00 00 00 00 00 00 00 00 00
     23        12.476 FB     0086 Rx 8  C8 02 CE 00 00 00 00 00
     24        12.587 FB     00AD Rx 8  A6 E9 BF FF 00 14 00 00
     25        13.271 FB     020A Rx 64 75 F6 3F FD 25 00 08 10 00 E8 7E 37 B8 20 83 7E 00 7D 40 1F 00 FC 7F 64 FE FF 7F 0D 20 EE 64 08 80 C2 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     26        13.497 FB     010B Rx 32 A5 0D 00 00 00 00 7E FE 00 00 00 00 00 04 FF 01 00 00 00 00 00 00 00 00 00 00 00 00 00 90 24 00
     27        14.762 FB     03D6 Rx 8  00 08 00 00 00 00 00 00
     28        15.090 FB     013D Rx 32 F6 18 11 11 01 94 03 00 00 00 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     29        15.318 FB     014D Rx 32 88 01 00 FE 07 00 00 08 FE 07 FE 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 3F
     30        15.611 FB     00FC Rx 48 D5 8B 31 00 7E 18 93 10 00 00 00 00 00 00 00 00 00 00 10 2B 2B 21 21 09 00 00 00 00 00 00 00 00 00 00 00 F4 01 40 FF EB 7F 38 C8 EA 81 AF AE 1E
     31        15.987 FB     024F Rx 64 00 00 81 00 0C 00 E0 14 41 D0 1F 80 54 F0 1F 80 00 00 00 00 74 60 1D 80 00 00 00 00 00 00 00 00 80 4F 41 20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
     32        16.098 FB     0656 Rx 8  BC 0D 0A 00 00 00 00 00
     33        16.405 FB     0300 Rx 48 00 00 00 00 00 00 00 00 00 F0 3F 00 23 00 00 00 00 F0 7F 37 FF FF 00 00 80 00 00 00 00 00 FF 7F 00 00 00 80 01 00 00 00 00 00 00 00 00 00 00 00
     34        16.854 FB     00C0 Rx 32 86 85 FE E7 7F 10 27 93 E6 7F FF F3 3F FF F3 3F FC 0F 00 00 C0 FF FE 07 00 00 00 00 00 00 00 00
     35        17.448 FB     0086 Rx 8  AC 03 CE 00 00 00 00 00
     36        18.340 FB     020B Rx 8  FF 3F E0 07 02 EE BF FF
     37        18.529 FB     0206 Rx 24 B4 E4 7E 80 00 F8 0F 7A 00 00 00 00 00 00 00 00 01 FB FE 03 00 00 00 10
     38        19.788 FB     0397 Rx 8  00 80 10 00 50 FA 3E 00
     39        20.326 FB     0318 Rx 8  00 00 0E BF FE 03 00 00
     40        20.437 FB     009F Rx 8  F6 09 89 00 00 12 80 F0
     41        20.727 DT 1B00004F Rx 8  00 00 04 01 00 00 00 00
```

Fig. 60 Example partial view of log file of data collected from CAN bus

Given that the tests were carried out on the real vehicle, strict time requirements had to be met to ensure that the car did not detect errors. One of the main challenges was the replacement of CAN FD frames sent from the computer, including the conversion of the CRC necessary in the End-to-End protection mechanism. The logical connection is presented in Fig. 61.

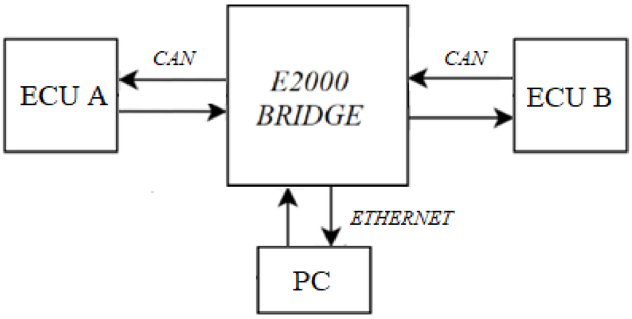


Fig. 61 Diagram of detailed logic connections of MicroDAQ E2000 device

Therefore, the very fast MicroDAQ E2000 device (Fig. 62) was used for the tests. The device meets all time requirements, while providing direct access to the memory via the Ethernet interface. One should underline that it was possible to send the frames that were next replaced in parallel to the device. One concluded that the MicroDAQ E2000 module connected in the bridge mode (sends frames from one side of the bus to the other, and when necessary, can replace the contents of the frames) was transparent for the tested car. All substitutions of frames did not cause permanent errors in the car during regular operation of the vehicle.

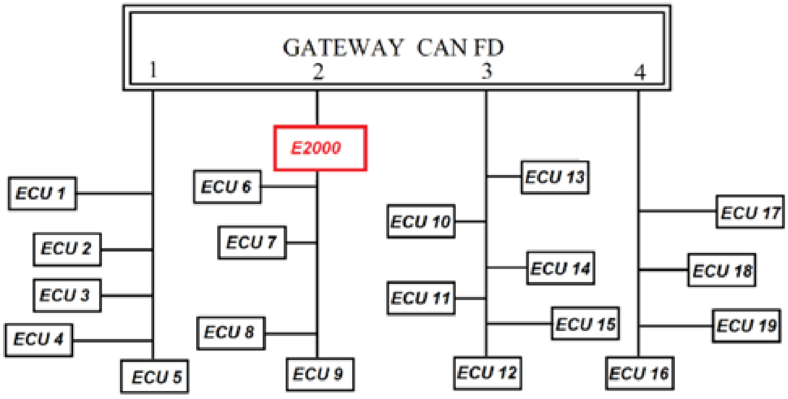
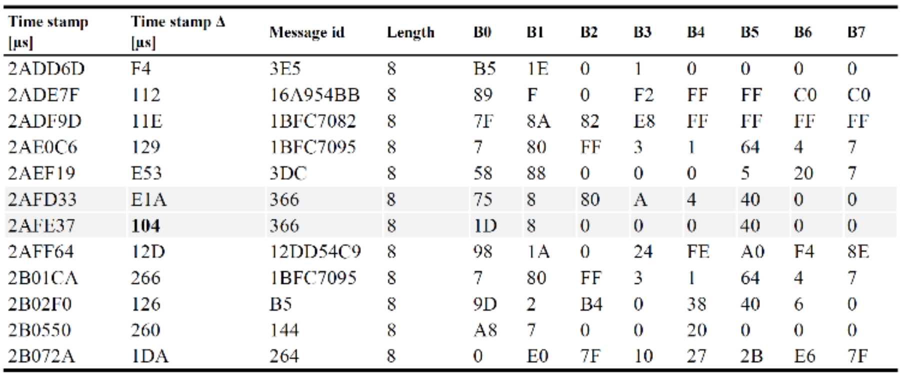


Fig. 62 Diagram of the system under the test

Verification tests

The verification of the obtained results was divided into two stages. At first the goal was to check whether it is possible to take control over the selected electronic control module without having detailed documentation on control signals contained in the CAN frames. Based on the reverse-engineering methods it was possible to make an effective attack and to take control of the rear turn signal of the tested electric car. The speed of replacing the content of the CAN frame and its transmission to the other side of the bridge was measured. It is marked in Fig. 63 in bold. The obtained time of about 100 microseconds is about 10 times lower than expected (frame replacement should take place in no more than 1 millisecond).



Time stamp [µs]	Time stamp Δ [µs]	Message id	Length	B0	B1	B2	B3	B4	B5	B6	B7
2ADD6D	F4	3E5	8	B5	1E	0	1	0	0	0	0
2ADE7F	112	16A954BB	8	89	F	0	F2	FF	FF	C0	C0
2ADF9D	11E	1BFC7082	8	7F	8A	82	E8	FF	FF	FF	FF
2AE0C6	129	1BFC7095	8	7	80	FF	3	1	64	4	7
2AEF19	E53	3DC	8	58	88	0	0	0	5	20	7
2AFD33	E1A	366	8	75	8	80	A	4	40	0	0
2AFE37	**104**	366	8	1D	8	0	0	0	40	0	0
2AFF64	12D	12DD54C9	8	98	1A	0	24	FE	A0	F4	8E
2B01CA	266	1BFC7095	8	7	80	FF	3	1	64	4	7
2B02F0	126	B5	8	9D	2	B4	0	38	40	6	0
2B0550	260	144	8	A8	7	0	0	20	0	0	0
2B072A	1DA	264	8	0	E0	7F	10	27	2B	E6	7F

Fig. 63 Can bus message log from attack on feature

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)

As part of this step, the following actions were successfully performed, leading to the takeover of the indicator control:

- the direction indicator was turned off and data on the CAN bus was logged
- a list of logged CAN frames was prepared; one payload was selected for each identifier (information contained in the CAN data field)
- a special program was prepared, which used the brute-force method to check all possible keys for all 16 indices and compare them with keys red from the logs
- 16 E2E keys were matched and found
- the direction indicator was turned on and while it was active, 1 CAN frame from the previously prepared list was replaced one by one, observing whether the rear direction indicator would be turned off.

  After replacing the single frame, the indicator turned off and was added to the list of frames potentially responsible for controlling the indicator
- after completing the frame replacement process, only 3 CAN frame identifiers were left on the list of "suspicious for display control": 0x144, 0x366, 0x264
- using the heat-map method and generating a graphic form with the use of a python script, the frame identifier, and the appropriate signals responsible for controlling the rear indicator were found.

The presented description of the performed experiments proved that it was possible to take control of the turn signal. In addition, it was checked that a single frame with a different identifier is responsible for signaling the status of the direction indicators on the driver's display. Thus, by replacing the turn control signal (disabling its operation), the driver still saw the correct status.

Based on the verification research, it has been proven that it is possible to take control of the vehicle.

Therefore, the concept of the low-cost security by means of software encryption of the data field was proposed. This approach significantly hinders the use of the presented methods to attack and successfully take control of the vehicle's electronic control modules. In the second stage of the experiment, the data encryption process was added to the transmission. However, it was not possible to change the software and reprogram the modules, so a simulation was performed. Instead of the software encryption module on the transmitting module, an additional module was used that encrypted the message. Simultaneously, instead of the software decryption module, an additional decryption module was used on the receiving module. Functionally, the same effect was obtained, and the results received in the experiment showed that the approach effectively hides the control signals.

The described situation is shown in figures below, Fig. 64 presents the architecture of the system with the encryption and decryption included in the transmitting module (ECU1) and receiving module (ECU2).

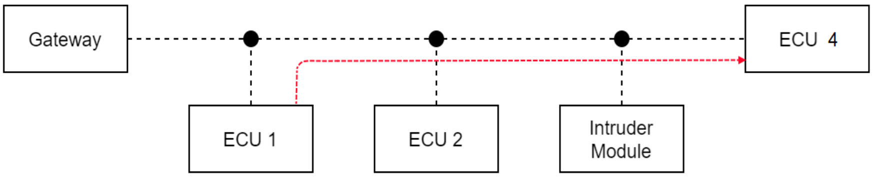


Fig. 64 Default architecture for sending CAN messages

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)

Fig. 65 presents the simulation, which is the result of adding the encoder and decoder modules.

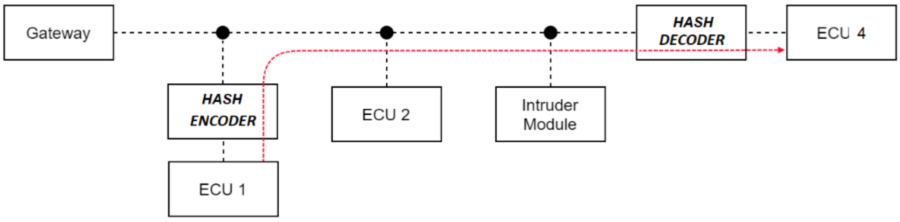
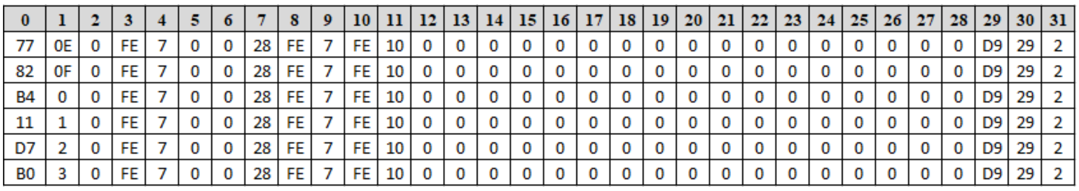


Fig. 65 Extended architecture for sending hashed CAN messages

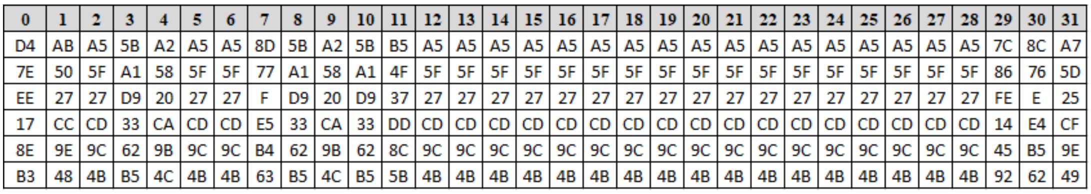
(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
77	0E	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
82	0F	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
B4	0	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
11	1	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
D7	2	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
B0	3	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2

Fig. 66 Data sent from module ECU 1

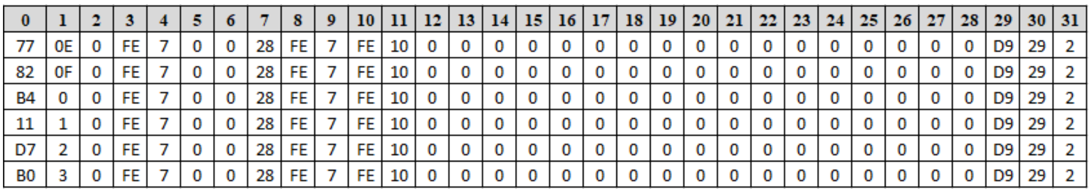
(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
D4	AB	A5	5B	A2	A5	A5	8D	5B	A2	5B	B5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	A5	7C	8C	A7
7E	50	5F	A1	58	5F	5F	77	A1	58	A1	4F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	5F	86	76	5D
EE	27	27	D9	20	27	27	F	D9	20	D9	37	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	27	FE	E	25
17	CC	CD	33	CA	CD	CD	E5	33	CA	33	DD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	CD	14	E4	CF
8E	9E	9C	62	9B	9C	9C	B4	62	9B	62	8C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	9C	45	B5	9E
B3	48	4B	B5	4C	4B	4B	63	B5	4C	B5	5B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	4B	92	62	49

Fig. 67 Data received by the hash decoder

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)



0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
77	0E	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
82	0F	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
B4	0	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
11	1	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
D7	2	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2
B0	3	0	FE	7	0	0	28	FE	7	FE	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D9	29	2

Fig. 68 Data received by the ECU 4

(Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021)

All presented tables include the control data from the examined CAN frame. It is visible that applying the XOR logical operation mechanism on subsequent data bytes to encrypt and decrypt the data, this data is the same. It is also presented in Fig. 66 and after the decryption in Fig. 68.

Conclusions

The experiment presented the application of methods that allow to take control of the electronic control modules without knowledge on control system of a given vehicle. Typically, such knowledge, i.e., control signals, is contained in the so-called DBC files containing information of decoded real data values on the CAN bus in a human-readable way. Selected methods making it possible to find the signals controlling with a specific functionality in the car were discussed in the thesis. The procedure always starts from a concept of logging control information from the CAN bus, when the direction indicator is turned off. The next step is to adjust the collected data and prepare a list of CAN frames for replacement when the direction indicator is active. It was proven that it is possible to find a sequence of bits controlling a given functionality. The expected result was to find a frame, or several CAN frames, which are going to turn off the direction indicator when it was on, after replacement. To replace the contents of the frames, when the End-to-End protection mechanism is present in the frame, the reverse engineering method was used, and all the necessary key values were found using the brute force method. In the next phase of the experiment, having already narrowed down the list of the frame identifiers that could be responsible for controlling the direction indicator, another method was used. One suggests the heat map presented in (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021), which allowed to graphically present the values of all bits in each frame for different timestamp values. In this way, the signals controlling the direction indicator were found. It was also shown that the turn control signal is different, independent of the turn status signal, which is visible in the driver's display. Having obtained confirmation of the takeover of control, in the last part of the experiment it was checked whether the use of an additional method encrypting the content of the data field of CAN frames would be able to hinder an effective attack using the methods described in the experiment. Unfortunately, having no possibility to change the software on the modules in the vehicle, it was decided to simulate the event that presents adding information encryption and decryption functionality. This was done using 2 additional hardware modules, the encoder, and the decoder. In practice, the same functionality was obtained when the software on the information sending and receiving modules was changed. One demonstrated that although the proposed method of the low-cost software encryption is not able to fully protect the transmission against potential decoding of the signals transmitted via the CAN bus, it significantly hinders this task.

To sum up, during the research it was proven that an attack on a turn signal can cause a direct threat to life, and the proposed encryption method makes it difficult to carry out this type of attack.

3.4 Detection of cyber-attack to steering gear by an artificial intelligence based approach

The main purpose of the research carried out as a part of this experiment was to prove that it is possible to detect an ongoing attack on the electronic control module in the electric car vehicle using selected artificial intelligence algorithms. It was assumed that during the attack on the vehicle, the signals sent via the CAN bus in the form of data bytes show an anomaly image, i.e., a state different from that expected during regular operation is going to be detected. The experiment was carried out without access to the documentation of the tested vehicle, i.e., without knowledge of the vehicle control signals. Taking it into account a black box approach was used. The data logged from the CAN bus was treated as a sequence of bytes, of which control signals should be included. The approach being developed during the research was based on the anomaly detection with the use of a deep neural network described in previous chapters of the thesis. Based on the network one was able to analyze the data appearing on the CAN bus and considering the time dependencies between them. The most important aspect is the possibility to determine the moment of the attack. The attacked element of the car is marked in Fig. 69 and corresponds to steering system.

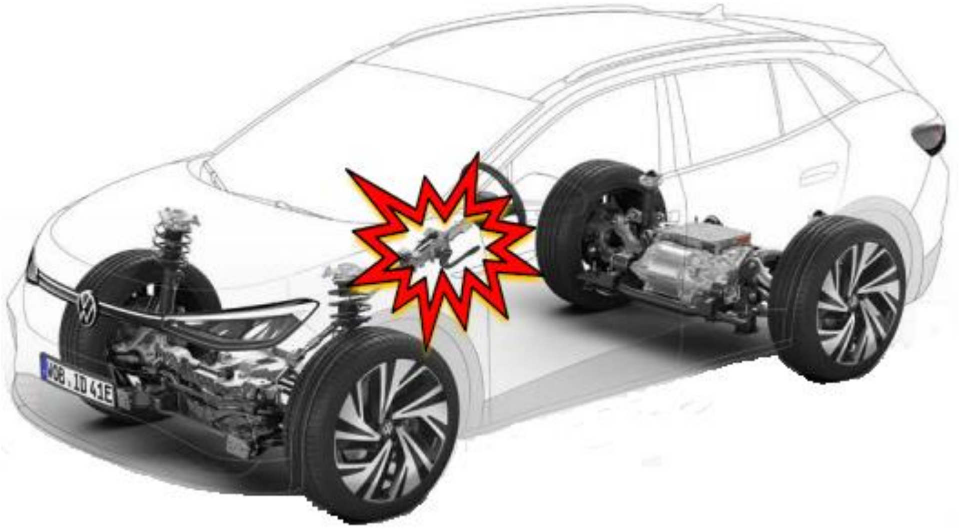


Fig. 69 Steering system

(Self Study Program 891213 The ID.4 New Model Overview, 2021)

Plan of the experiment

The research conducted during the experiment was divided into stages characterized below. A target of the attack was the steering gear control module in the electric car.

The possibility of taking control over the turning operation should be treated as the most serious threat, because it can easily lead to an accident, i.e., the threat to the health and life of traffic participants. It was assumed that the detection of the attack is possible by detecting anomalies in the control data contained in the transmitted CAN frames. Thus, it was necessary to log the signal values, and in fact individual bytes into the data fields of the transmitted frames. It was performed during the regular operation of the car as well as during the attack. Moreover, the scenario of the so-called regular operation was extended with additional data logged when using the driver assistance system called the lane assist. Dozens of trials and over 20 hours of tests performed on real electric car were carried out. The data values appearing on the CAN bus were collected and saved to files in 3 types of situations presented in Fig. 70:

- regular driving (the driver drives the vehicle without the lane assist active) - REGULAR_MODE
- driving with the lane assist system active - LANE_ASSIST_MODE
- driving when a successful attack was performed, and the steering gear control was taken over the vehicle - ATTACK_MODE

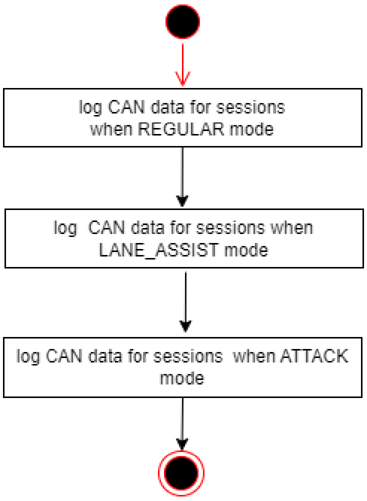

log CAN data for sessions when REGULAR mode
log CAN data for sessions when LANE_ASSIST mode
log CAN data for sessions when ATTACK mode

Fig. 70 CAN data logging sessions

According to the concept of the black box and owing the lack of access to the documentation containing the control signals of the tested vehicle, it was necessary to assume that among the data there are signals of the steering gear responsible for the control. Without knowing the exact signals, the full data fields of the frames under study, always arranged in the same order, were used as input. Having collected several gigabytes of data in the form of several dozen sessions, it was necessary to convert it to a format that would allow further data processing. For this purpose, the concept elaborated by the author of the thesis was elaborated. The concept is based on a map of bytes arranged in time with a resolution of 1 millisecond. The successive bytes are always clustered according to the CAN identifier in the same order, as shown in Fig. 71.

The bytes from the data fields of the selected CAN frames were linked together following the order: 0x40 (length = 8) + 0x86 (length = 8) + 0xFD (length = 8) + 0x116 (length = 8) + 0x176 (length = 8) + 0x31B (length = 8) + 0x65D (length = 8) + 0x303 (length = 24) + 0xFC (length = 48) + 0x102 (length = 48).

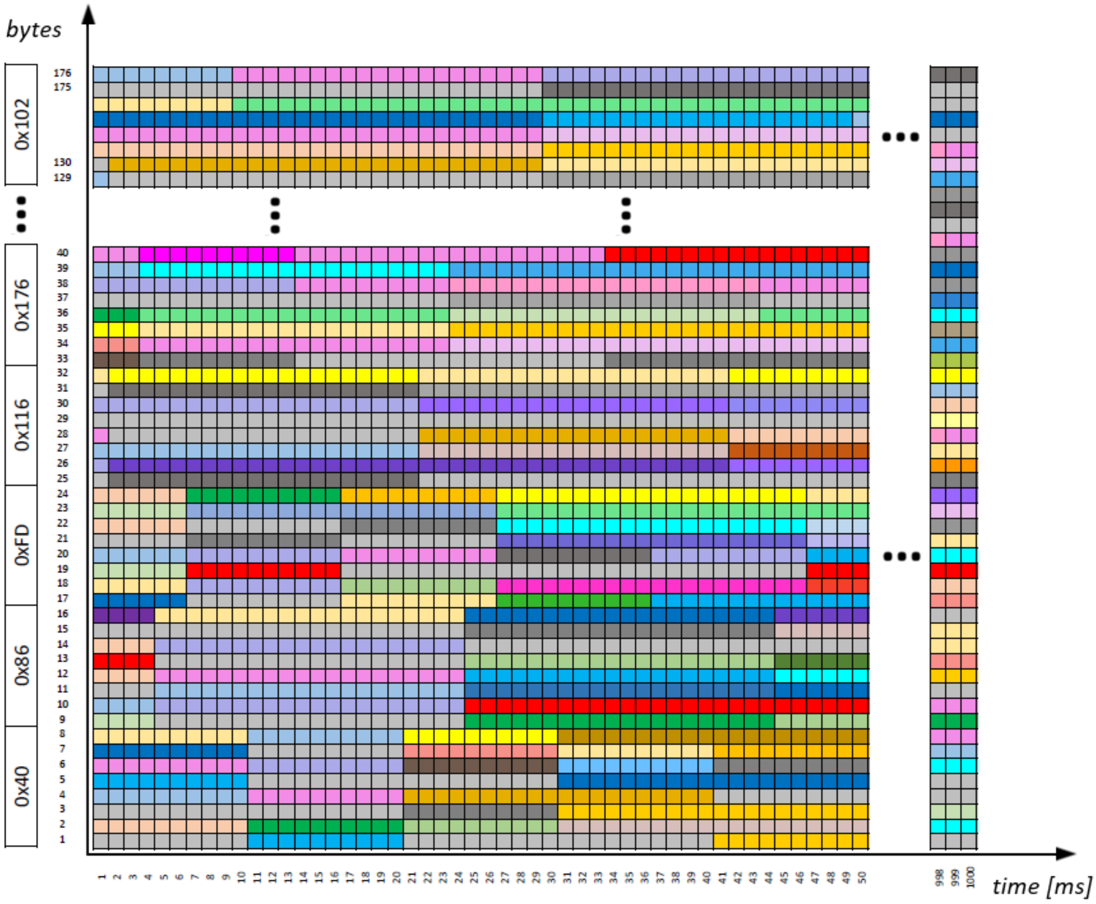


Fig. 71 A byte map concept with assigned color bytes representation for a single time window

According to the CAN protocol standard, frames are sent to the bus cyclically with a specific cycle time. The value of the cycle time is given in milliseconds and its value depends on the importance of the function performed by the signals included in one frame. The higher the priority of the transmitted information, the lower the value of the cycle time. Typical cycle time values range from ten to several thousand milliseconds. To obtain a time resolution of 1 millisecond, the collected data was processed using Python scripts in such way that the data bytes for subsequent milliseconds were duplicated with the data received in the last CAN frame. In addition, the logged data was prepared in such way that the data from all CAN frames for each identifier were saved in a separate file. At the same time, data consistency was ensured, i.e., their synchronization over time. Moreover, a fixed time interval was set for the duration of a single session of about 5 minutes. The concept of preparing data obtained from login processes is presented in detail in Fig. 72.

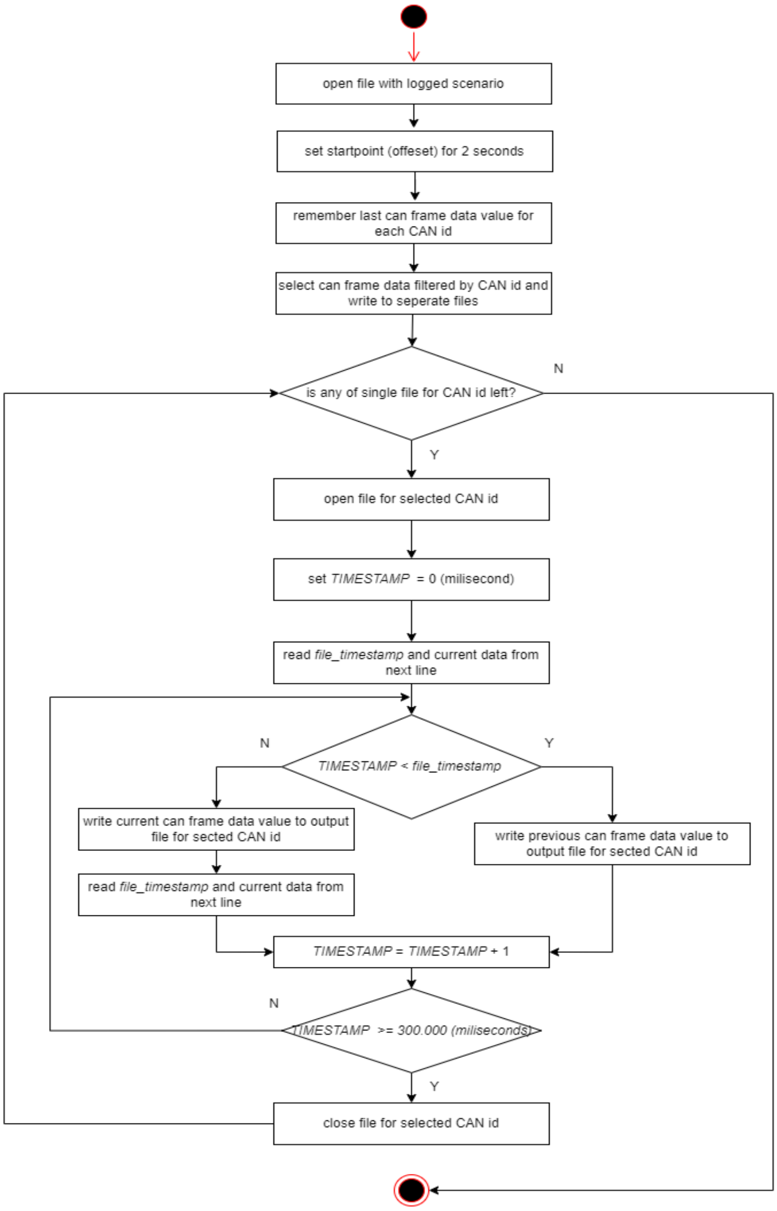

open file with logged scenario
set startpoint (offeset) for 2 seconds
remember last can frame data value for each CAN id
select can frame data filtered by CAN id and write to seperate files
is any of single file for CAN id left?
N
Y
open file for selected CAN id
set TIMESTAMP = 0 (milisecond)
read file_timestamp and current data from next line
N
Y
TIMESTAMP < file_timestamp
write current can frame data value to output file for sected CAN id
write previous can frame data value to output file for sected CAN id
read file_timestamp and current data from next line
TIMESTAMP = TIMESTAMP + 1
N
TIMESTAMP >= 300.000 (miliseconds)
Y
close file for selected CAN id

Fig. 72 Diagram of concept of preparation of separate files for each CAN id data with resolution of 1 millisecond

The next stage of the experiment was the use of artificial intelligence approach to search for anomalies. It was done after the CAN messages were recorded and processed with the use of Python scripts. Theoretically, having data logged during the regular operation of the vehicle, it is possible to train the neural network and detect the moment of occurrence of an anomaly understood as a sign of an ongoing attack on the vehicle.

For this purpose, deep learning algorithms were used, considering the time dependencies between the processed data. The anomaly detection tests using the network were carried out in 2 cases:

- the neural network was trained using data from the regular driving. The electric car was driven by a driver without the lane assist active. The detailed algorithm is presented in Fig. 73
- the neural network was trained using data from regular driving when the electric car was driven by a driver with the lane assist system active. The detailed algorithm is presented in Fig. 74.

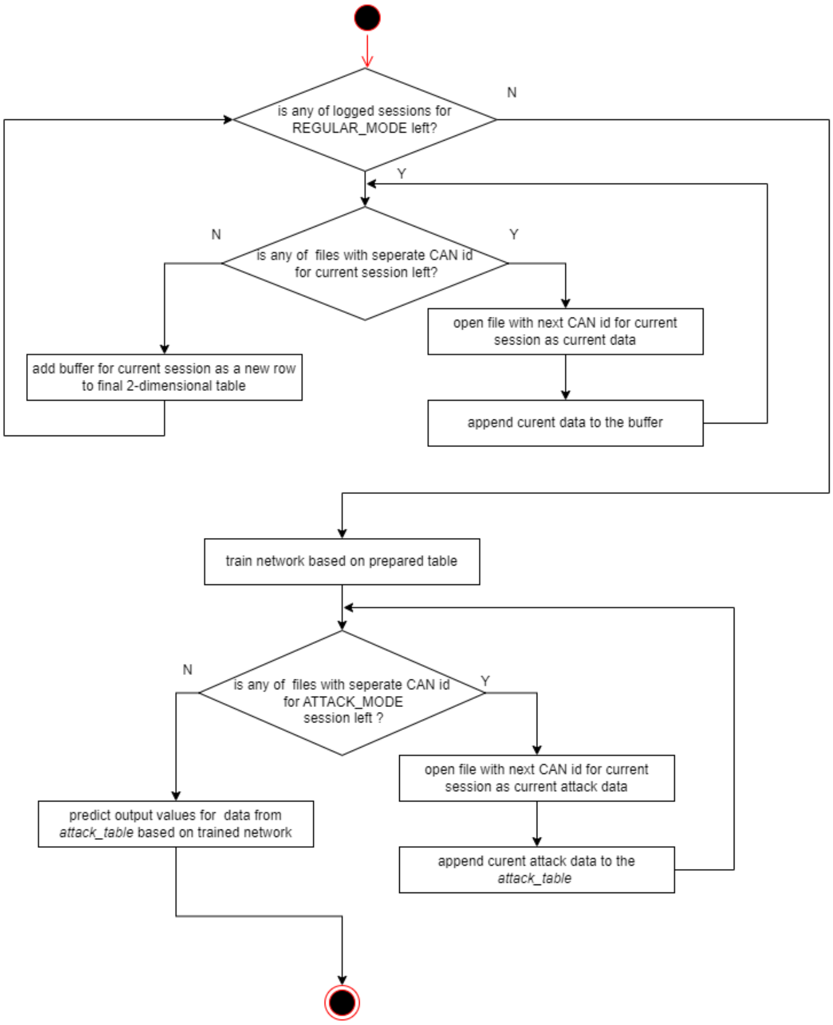

is any of logged sessions for REGULAR_MODE left?
N
Y
is any of files with seperate CAN id for current session left?
N
Y
open file with next CAN id for current session as current data
append curent data to the buffer
add buffer for current session as a new row to final 2-dimensional table
train network based on prepared table
is any of files with seperate CAN id for ATTACK_MODE session left ?
N
Y
open file with next CAN id for current session as current attack data
append curent attack data to the attack_table
predict output values for data from attack_table based on trained network

Fig. 73 Detailed diagram of learning algorithms for REGULAR_MODE

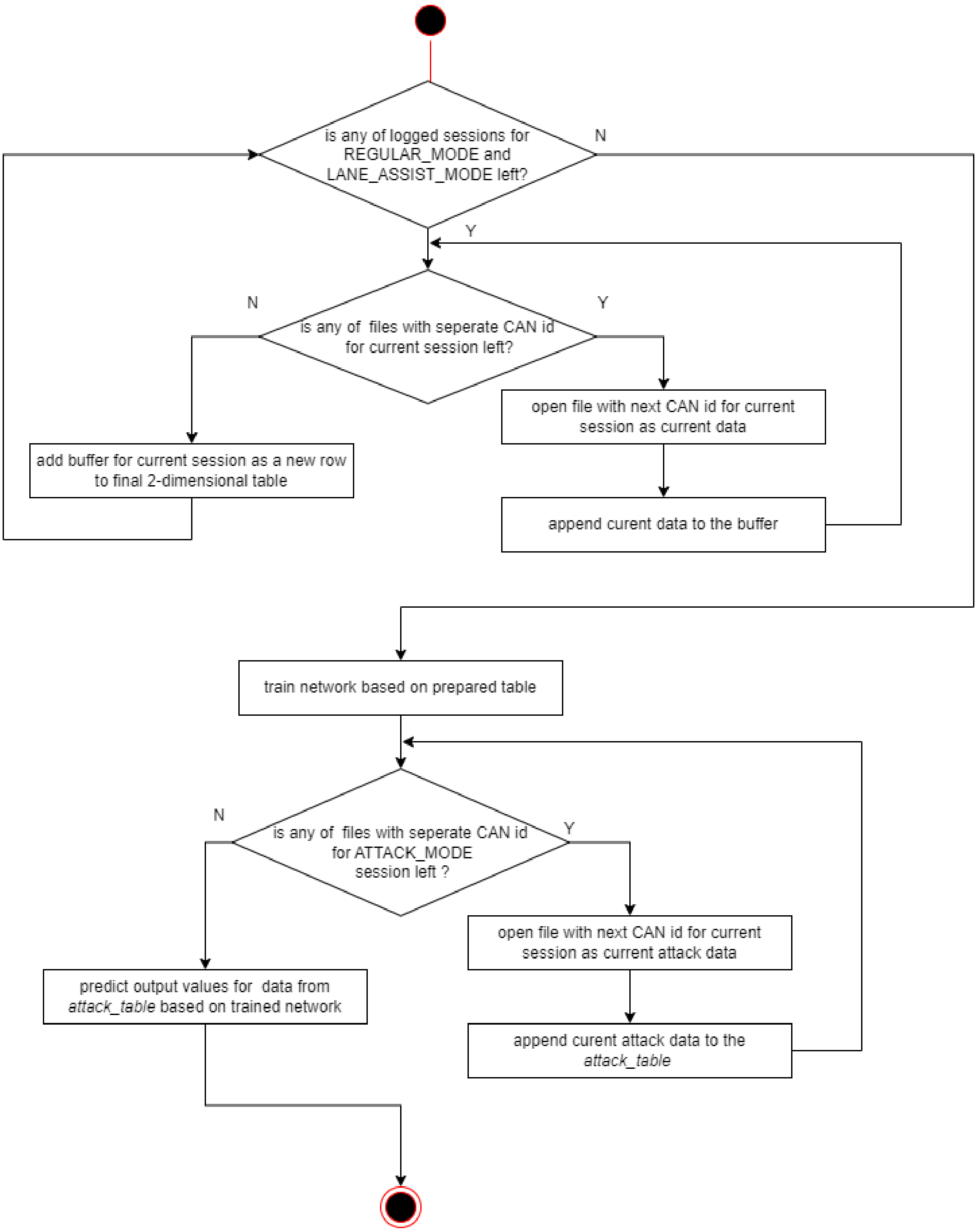

is any of logged sessions for REGULAR_MODE and LANE_ASSIST_MODE left?
N
Y
N
is any of files with seperate CAN id for current session left?
Y
open file with next CAN id for current session as current data
add buffer for current session as a new row to final 2-dimensional table
append curent data to the buffer
train network based on prepared table
N
is any of files with seperate CAN id for ATTACK_MODE session left ?
Y
open file with next CAN id for current session as current attack data
predict output values for data from *attack_table* based on trained network
append curent attack data to the *attack_table*

Fig. 74 Detailed diagram of learning algorithms for REGULAR_MODE and LANE_ASSIST_MODE

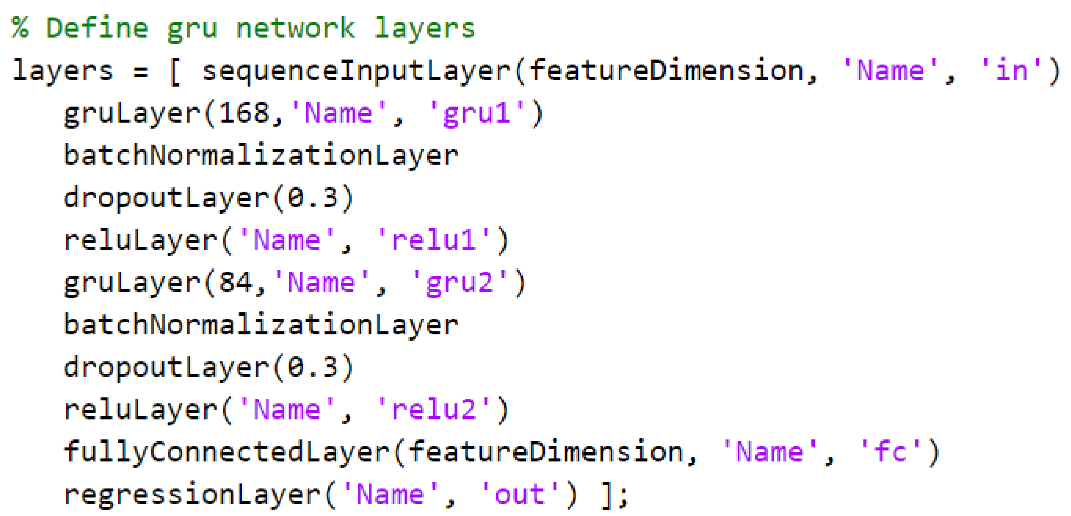
Real data logged during various modes of vehicle operation were used to carry out the experiment. At first a proper preparation and adjustment in terms of both the data format and time synchronization to the proposed original byte map concept were performed. As the result tens of gigabytes of data were obtained. The main problem that arose was the choice of a data analysis method that can work in case of such large amount of input data. It is important to mention that the data is time dependent. The main goal of this part of experiments was to detect the attack on the basis of identification of anomalies present in the data. In the experiment the method using the autoencoders was implemented.

Considering the type of processed data, the fact that they are very large amounts of bytes sent cyclically every millisecond, and the defined lengths of the data field in the CAN frames (for each CAN frame identifier), it is assumed that there are some repeating data patterns. It is the main reason the application of the deep neural learning method was chosen. The calculations were conducted with the use of a specialized engineering tool MATLAB with the deep learning toolbox. The main idea of deep learning as well as some kinds of neural networks were characterized in Chapter 2.4. of the thesis. In the selected algorithm 3 types of recursive layers were available for deep learning with time series and sequence data:

- **LSTM layer** – long short-term memory layer, learns long-term relationships between sequential data and time periods
- **BILSTM layer** – bidirectional long short-term memory layer, the LSTM layer learns bidirectional long-term relationships between sequential data and time periods
- **GRU layer** – gated recurrent unit layer, learns the relationship between sequential data and time periods

Since the amount of data to be processed is very large (tens of gigabytes), and having access to limited computing power, the GRU layer was used in the experiment. It is faster than the model with LSTM layer due to its structure.

It was assumed that the number of input units in the input layer was 168. This resulted from the number of bytes that were included in a single line of the byte map. According to the principle of operation of the autoencoder (incomplete) network, the next layer should contain a reduced number of neurons (because the encoding process is taking place), therefore the second GRU layer was limited to 84, which was half the number in the first GRU layer. In the final step, at the time of decoding, a fully connected layer was created with the number of input neurons equal to 168, i.e., the original size was reached. The exact layers used in the model are shown in Fig. 75.



```
% Define gru network layers
layers = [ sequenceInputLayer(featureDimension, 'Name', 'in')
   gruLayer(168,'Name', 'gru1')
   batchNormalizationLayer
   dropoutLayer(0.3)
   reluLayer('Name', 'relu1')
   gruLayer(84,'Name', 'gru2')
   batchNormalizationLayer
   dropoutLayer(0.3)
   reluLayer('Name', 'relu2')
   fullyConnectedLayer(featureDimension, 'Name', 'fc')
   regressionLayer('Name', 'out') ];
```

Fig. 75 Layers implemented in autoencoder concept

Research environment / test bench

The test setup was a real electric car with minor modifications to the connections at the central gateway to connect additional devices. For logging data from the CAN bus, as in the case of other experiments, a standard PCAN-USB PRO device available on the market was used. To perform the attacks and to take over control and the twisting function, i.e., in practice an electronic module responsible for the steering gear control the MicroDAQ E2000 device working in bridge mode was used. The method of connecting to the gateway is presented in Fig. 76.

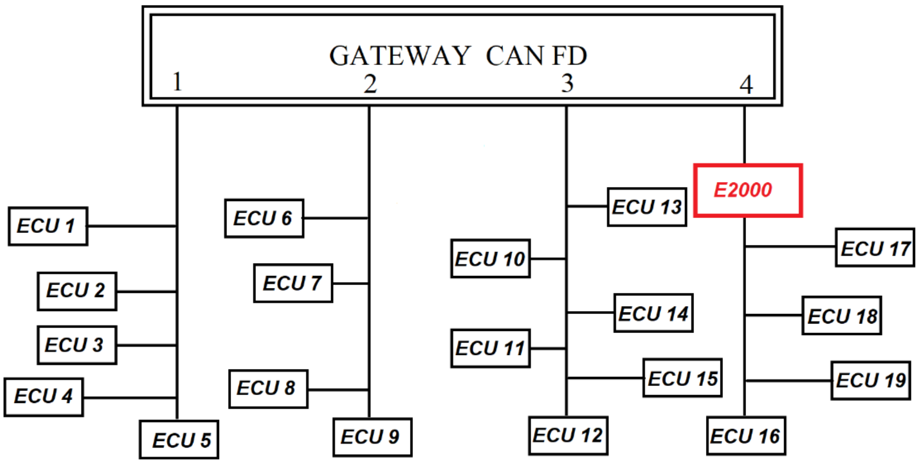


Fig. 76 Diagram of the system under test with bridge module marked in red

The requirements that the Microdaq E2000 test device was supposed to meet were very high. They are especially important in terms of time required to process a full CAN FD frame. This device was used to attack the steering gear module by replacing the original content of the CAN frames with frames that were previously recorded during the operation of the lane assist system. Thanks to this, it was possible to take control of the steering gear system on a real car vehicle. The tests one carried out, caused no error detection by a car system. To attack the control system, a device operating in the bridge mode or sending information in the CAN frames from input to output in both directions were used. It what was shown in Fig. 77.

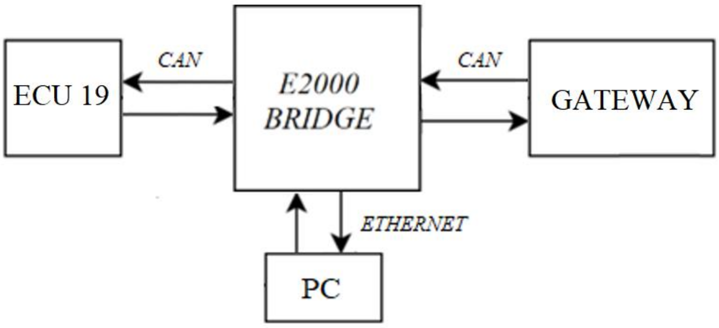


Fig. 77 Detailed diagram of the logical connections of the MicroDAQ E2000 device

In addition, for a specific CAN frame responsible for twisting (ID=0x303), the content of the data field was replaced with values sent via the Ethernet interface from the application on the PC computer. To control the steering wheel, a pad (for computer games) was used, which was connected to the computer via Bluetooth. A complete set of devices is shown in Fig. 78.

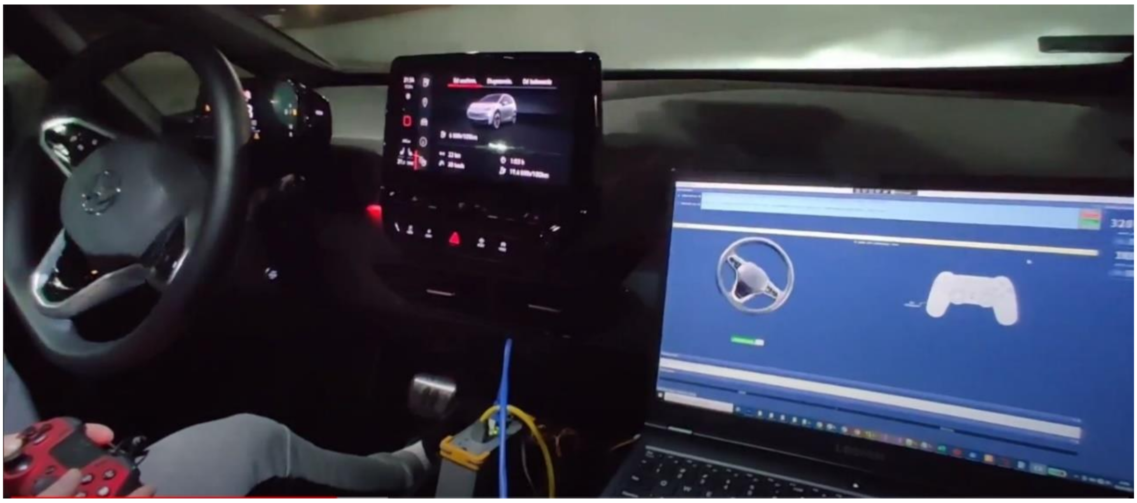


Fig. 78 Set of devices to take control of the steering gear system: MicroDAQ E2000 as a bridge, pad, notebook with PC application

The developed software allowed to set the desired turning values with the appropriate direction and momentum, while reading the current position of the steering wheel from the Microdaq E2000 device. It was presented in a graphical form.

Verification tests

Having collected data from the CAN bus in cases where the car was used in the so-called a regular mode, i.e., the car is driven by a human without the lane assist active and in the mode with the lane assist activated, the collected data after processing using Python scripts were implemented to train the neural network. The proposed byte map model, i.e., arrange subsequent bytes of data fields of CAN frames always in the same order. They are trained with the network of the GRU-AE type. This training was divided into 2 stages. In the first stage, the data collected during a regular driving, i.e., without the lane assistant system active was used. The important factor that caused the steering wheel to move was the driver's intentional maneuver. As can be seen in Fig. 79, it was possible to notice an anomaly that arose during the ongoing attack, i.e., taking control over the turning function of the car. However, the obtained difference between the signal indicating the occurrence of the anomaly and the signal at the output of the network for the correct case is not significant. One may conclude that there is necessary to use more training data while riding to get bigger value of residua.

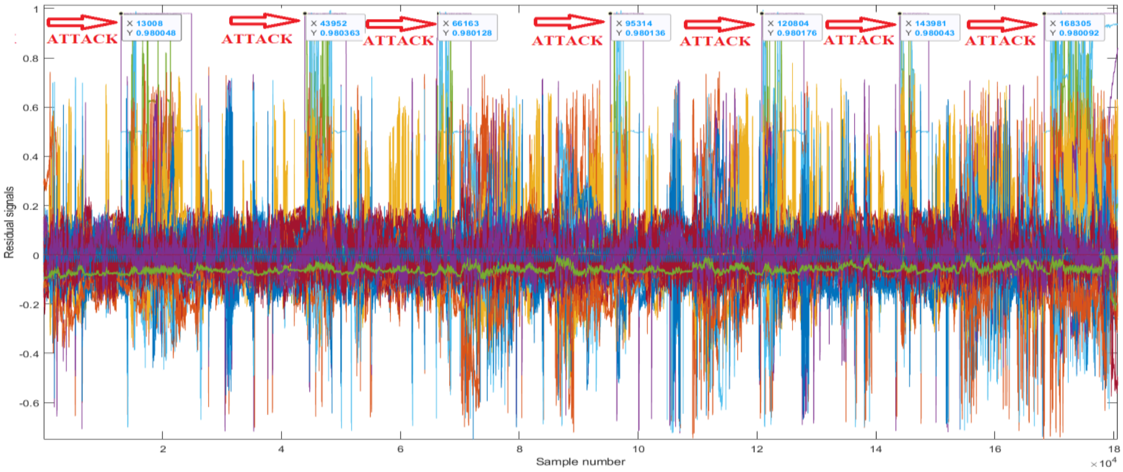


Fig. 79 Anomaly (attack) detection with the DNN GRU-AE trained without lane assist (Gajdzik, Timofiejczuk, Gnacy-Gajdzik, & Przystałka, 2023)

In the second stage of the research, the data collected while driving was used when both the driver and the lane assistant system were responsible for turning the car. As can be seen in Fig. 80, it was possible to notice the anomaly that arose during the ongoing attack, i.e., taking control over the turning function of the car. The obtained difference between the signal indicating the occurrence of the anomaly and the signal at the network output for the correct case was so significant that it was easy to distinguish between the correct signal and the anomaly, or to indicate precisely and without doubt the moment of the attack.

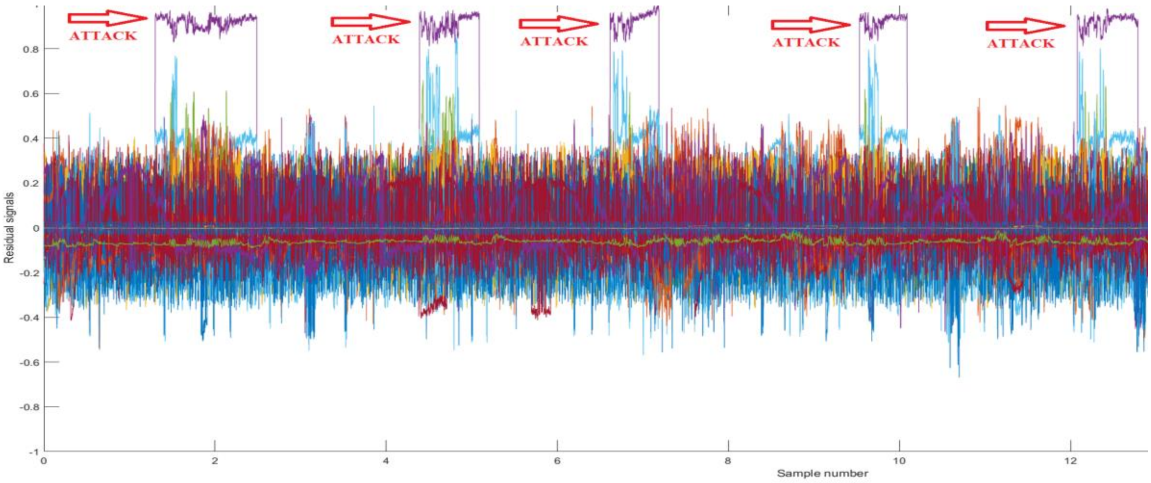


Fig. 80 Anomaly (attack) detection with DNN GRU-AE trained with lane assist (Gajdzik, Timofiejczuk, Gnacy-Gajdzik, & Przystałka, 2023)

At this point, it should be stressed that the experiment proved that it is possible to successfully attack a modern electric car and take control over it. In the event of taking control over such key control systems as braking, accelerating, or turning described in this part of the thesis. Since the attacks of these types are very dangerous, it is so important to continue research aimed at increasing security in cars. Considering results of previous experiments, it is clearly visible that the application of methods based on artificial intelligence, and especially learning significantly increases the possibility of the attack detection and especially the attack that are more complicated

Conclusions

Throughout the experiment, a planned sequence of activities was carried to detect anomalies. It was assumed that the detection of the anomaly may constitute information about an ongoing attack on the car. Data was logged from the CAN bus directly connected with the steering gear system. The experiments were performed when driving in the regular mode and with the lane assistant system active. In addition, data from the CAN bus was logged during the attack consisting in taking control over the turning function in the car. For this purpose, a real cyberattack scenario was carried out using an additional Microdaq E2000 device operating in the bridge mode and controlled from a computer application via Ethernet bus. It was proven that it is possible to successfully attack a modern electric car and take control over it in a way imperceptible to the vehicle control system. Having collected data from the buses while driving in predefined test cases, the data was converted in such a way that it was possible to process them further. Maintaining consistency and time synchronization and a resolution was equal to 1 millisecond. This value resulted from the proposed concept of a byte map, i.e., successive CAN frames connected as data fields with a resolution of 1ms (concept presented in Fig. 71). The files obtained for each CAN frame identifier in sessions with the regular driving (without the attack) were used to train the neural network. Then, an attempt was made to detect the anomaly by inputting the data logged during the ongoing attack.

3.5 Summary of experiments and verification tests. Proposed approaches to car protection

During the experimentation outlined in Chapter 3, innovative cyberattack protection methods were developed. These solutions were tailored to meet the specific requirements of the automotive sector, which include:

- the production of certain modules in extremely high quantities, reaching millions of units, where their impact on human safety is indirect, such as internal ambient lighting
- the existence of modules directly accountable for crucial vehicle operations, such as braking, acceleration, or steering

To address these distinct needs, the author categorized the solutions into two groups: cost-effective approaches and advanced functionalities, both of which leverage deep neural networks.

To detect the attack, an autoencoder deep neural networks using the GRU as an anomaly detection tool was used. The comparison between compression of the source data, and then their decompression, considering time dependencies, showed that it was possible to detect the attack. It was also proven that it is possible to detect the attack by training the deep neural network using data collected during the regular driving without the lane assistant system active. However, the difference between the expected value at the network output and the anomaly was not significant (see Fig. 79). It should be also stressed that if the network was additionally trained with the data collected while driving with the lane assistant system active, the difference was significant (see Fig. 80). The experiment proved that it is possible to detect attacks with 100% effectiveness thanks to the use of deep neural networks and thus prepare the appropriate scenario at the vehicle level that would be able to prevent such situations or at least minimize their effects.

3.5.1 Lost-cost solutions

In the automotive industry, where the manufacturing volume is counted in millions of pieces, the special emphasis is put on the lowest possible production cost of a single module. Therefore, even though there exist the effective encryption methods using dedicated hardware, they are usually not implemented in systems that control critical functionalities in vehicles. Implementing such methods and devices increase the cost of a car. It is the reason in most cases, data on buses is transmitted openly, creating risk of improper use. Considering the expectations to decrease costs and to ensure the security of a car, one requires simple encryption methods to be used. Such approaches were elaborated within the PhD project and are presented below. They are results of experiments described in the previous chapter of the thesis.

Time-window concept

The concept assumes adding some information to the data field of the CAN frame. It is known as a timestamp which checks the validity of the transmitted data. As the timestamp, the current value of time counted from the start of the entire system, is used. Its initial value is determined by a special CAN frame, which is sent through the device controlling the remaining modules at the system startup. Then it is synchronized every specified time (e.g., 10 seconds). By default, the timestamp uses 1 byte (which means that smaller amount of data can be sent in one single CAN frame), but it can be easily extended to 2 bytes. The idea as well as the verification results are characterized in (Gajdzik, Timofiejczuk, & Sebzda, 2021) and discussed in the chapter 3.1 in “Time-window concept for internal ambient light devices” experiment. The verification tests have proven the effectiveness of this method. It was stated that 100% effectiveness is not possible to be obtained. However, the method significantly minimizes the probability of a successful attack. The shorter the time window and the greater the number of bits allocated to the lifetime counter, the higher the effectiveness of the described method. Assuming the following assumptions:

- 16 bits is used for life time counter
- time window value is set to 100 milliseconds
- sending CAN frames is possible with resolution 1 millisecond.

The probability of conducting a successful frame replay attack is close to 0%.

$$P_{SA} = \frac{1}{65536} * \frac{100ms}{1ms} = 0{,}15\%$$

P_{SA} – **P**robability of **S**uccessful **A**ttack

which translates into a protection effectiveness of 99.85%.

XOR concept

The basis of this concept is a reference to the way the logical function XOR (Exclusive-OR) works. In case a byte value is XORed twice with the same argument, the result is limited to the initial value. In other words, the sender of the frame performs the *byte[x] XOR key* operation (where x is the index of the data field from the CAN frame). As the result the encrypted information is obtained. The recipient performs the same *byte[x] XOR key* operation and thus obtains the original data value. However, during the transmission, they are simply encrypted. Detailed information as well as verification results on this approach is presented in the chapter 3.3 characterizing the experiment "Car blinker masking cyber-attack" and described in (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021).

Double bits negation concept

The concept is an extended version of the "Time-window concept". The approach is based on the double negation of bits in each byte of the transmitted frame, for which the corresponding bits of the argument value of this operation are equal to 1. In other words, for the bits that correspond to the value 1 in the argument, a bitwise negation is performed, and the rest of the bits is unchanged. The operation is performed twice. In the first step the value of the operand is the key, and in the second step the value of the operand is related to the time window. The 8-bit key value is stored in the non-volatile memory of each ECU connected to the CAN bus. The receiver of the frame performs the reverse process, i.e., the first negates using the value of the time window as an argument, and then the key stored in the non-volatile memory. Tab. 7 shows the next steps of the proposed elementary encryption algorithm.

Tab. 7 Example application of the proposed encryption

Value	Hexadecimal value	Binary value
original byte	0x7D	01111101
key (mask for negation)	0xC3	**11**0000**11**
encrypted byte – step 1	0xBE	10111110
time window	0xF1	**1111**0001
final encrypted byte	**0x4F**	01001111

3.5.2 Concept of CAN bus burglary protection module supported by artificial intelligence-based algorithms

The results of the research presented in the thesis has proved that it was possible to take control of various Electronic Control Units (ECUs). Even such critical functionality as the steering, which should be especially protected. Since an effective attack on the electronic executive module is possible and the same time the cost of the vehicle cannot significantly increase a CAN bus burglary protection module was proposed. The approach uses artificial intelligence algorithms to detect anomalies during the analysis of CAN bus traffic. The main assumption of the approach is that each detected anomaly may indicate an ongoing attack.

The proposed concept is a compromise between maintaining low module production costs and effective detection of the attack. With the use of the elaborated solution, it is possible to react and avoid taking control over some vehicle modules. It should be stressed that the improvement of the existing transmission architecture basing on CAN buses with an additional supervisor module requires additional costs due to the large number of CAN interfaces and high computing power. However, it is still a viable solution, considering that the number of electronic control modules in a contemporary car is between 100 and 200. The architecture of the elaborated concept is presented in Fig. 81.

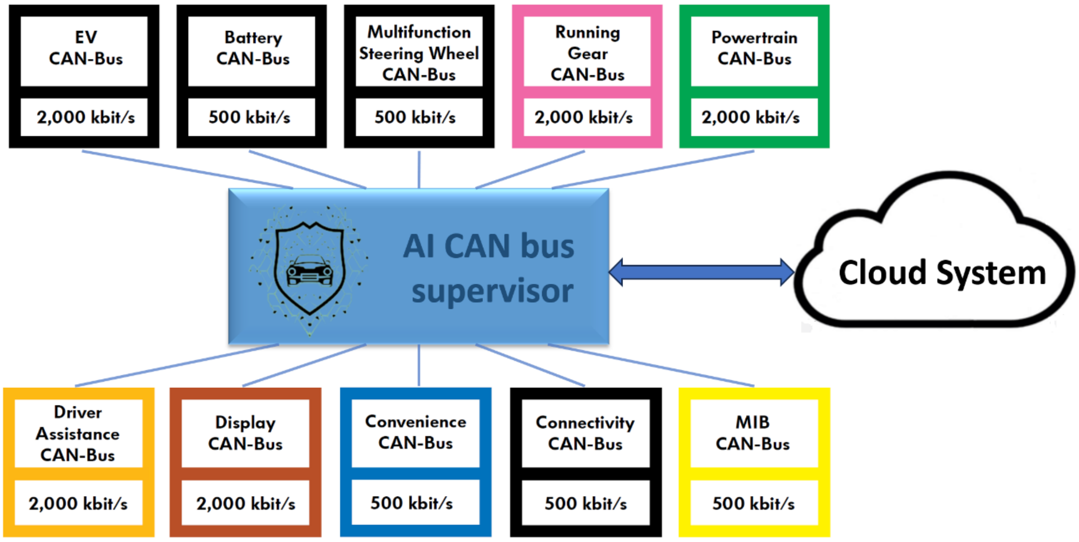


Fig. 81 Concept of CAN bus burglary protection module following the Industry 4.0 idea

The concept of the module elaborated as the result of the PhD project assumes the implementation of deep learning algorithms based on the auto-encoder model and the proprietary method of byte maps received from the CAN bus. Detailed description and verification of the approach were presented in the chapter 3.4 characterizing experiment "Detection of cyber-attack to steering gear by Artificial Intelligence". The approach was also described in (Gajdzik, Sternal, Timofiejczuk, & Przystałka, 2021). The verification tests showed that a properly trained neural network was able to detect any attempt to attack the steering control system in the car.

The biggest problem was encountered during the process of training the neural network. Despite the high computing power and a dedicated graphics card with an independent RAM memory of 24 GB, more than 20 hours of training were needed to train the network. Since the supervisory module that would be able to learn on the fly in a reasonable time and support several or several dozen CAN bus interfaces, the approach came out to be too expensive. Considering current state of IT development, it is possible to take advantage of approaches related to the "Industry 4.0". The author also elaborated a concept basing on connection the burglary protection module to the cloud system. As a result, all calculations and operations that require many available resources are performed in the cloud. The architecture of such system is shown in Fig. 82.

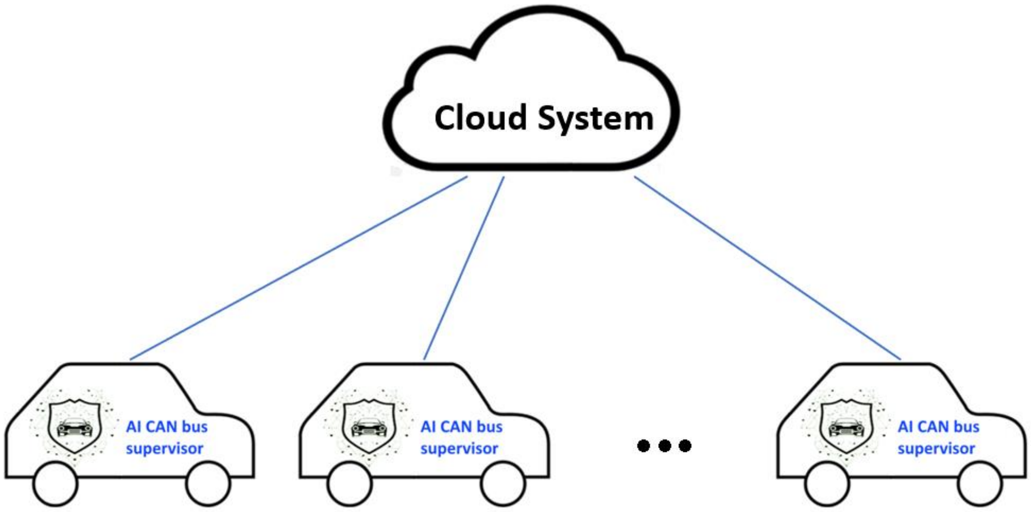


Fig. 82 Concept of cars connected to cloud system following the Industry 4.0 ecosystem

The module implemented in each vehicle sends pre-processed data to the cloud system, where the training process takes place. It is required that the data are pre-processed because of its original large size. There are several advantages of this approach. The most significant one is that all vehicles are equipped with the latest model of data collected obtained based on all active vehicles. It is enough that a single vehicle is attacked with a hitherto unknown method and thanks to the cloud learning and the distribution of the trained model to supervisory modules in cars, each car is resistant to this new type of the attack. It makes it possible to be resistant to hitherto unknown type of threat. Therefore, the presented concept is an intelligent self-learning model that is able to effectively detect unknown types of threats.

Chapter 4

Conclusions and plan of further research

The goal of this research conducted within the PhD project was to elaborate approaches to minimize threats in embedded car systems which control electronic modules. In the first part of the thesis a review of potential treats and exemplary attacks were discussed. The author identified hazards in contemporary cars in scope of cybersecurity and performed a series of experiments aimed at attacking some embedded car systems. The results of these experiments were bases for proposing original solution to the undertaken problem.

A contemporary car is understood as an intelligent mechatronic vehicle integrated with a management system consistent with different aspects of the “Industry 4.0” concept.

During the research, it has been proved that in a contemporary electric car it is possible to take control of the following control modules in the vehicle: interior ambient lighting, blinker, and steering function.

The author of the thesis proposed 2 different approaches to the topic of protection against attacks:

- low-cost solutions that include 3 approaches to increase the security level of transmission between ECUs in the vehicle, thus minimizing chances of conducting a successful attack
- advanced detection system of anomalies that may indicate an ongoing attack, which uses deep learning and neural network for analysis. In the "Detection of cyber-attack to steering gear by an artificial intelligence-based approach" experiment's verification tests, it was demonstrated that employing the suggested model based on auto-encoder concept and deep neural networks one achieves 100% detection rate for the attack. It can therefore be assumed that the deep neural network trained on data containing new types of threats is able to detect them with a very high probability, even close to 100%. With this aspect, the author proposed a vehicle-integrated information exchange system between them and the cloud system, which is pre-processing data from all active vehicles. Considering the fact that the training process of the deep neural network takes place in the cloud system, it is enough that if a new type of attack is carried out on even one car, all vehicles will become resistant to it. It can be stated that the presented concept

follows the idea of Industry 4.0, which integrates various technologies in one ecosystem. Connecting vehicles to the cloud system are the goal of further analyzes and tests.

It should be stressed that the solutions presented as the result of the thesis are universal. The research problem concerns cyberattacks on electronic control modules in vehicles. However, nowadays a very large number of industrial processes is automated and there is increasing danger to perform an effective attack on such structures. The methods developed within the PhD project can be also implemented in other branches of the industry. In each case when, electronically controlled mechanical systems are maintained, communication processes are performed. Contemporary devices are mechatronic systems connected to each other constituting a network. The advantage is the mutual communication and control. However, it should be also stressed that taking control over such systems or at least destabilizing their regular operation is possible. The spectrum of areas where such an attack may occur is wide and growing day by day. From another side, it is strong desire to automate as many industrial processes as possible. It accelerates manufacturing and increases profits. Taking into account factories, examples are production lines or logistics centers operating as automated warehouses for goods. In addition, it should be also mentioned the rapidly growing branch of private smart-home applications.

Owing new technologies, as well as user demands and their safety, the maintenance of mechatronic systems is a big challenge. The difficulty is that in case of the regular safe operation of such systems, it is necessary to provide on-demand diagnostics in real time. Such approaches, operating in real time are additional entries of potential attacks.

The proposed concepts of the cyber-security modules are responses to these types of threats. The idea of its operation, presented in the thesis, is based on the continuous analysis of real, correct signals (i.e., when it was assumed that an attack is not underway). One of the approaches is based on application of artificial intelligence algorithms, and especially neural networks were implemented. The crucial aspect in this case is continuous monitoring of transmission and the goal is to detect anomalies, which are understood as a potential possibility of an ongoing attack. It is obvious that depending on the technologies and buses used, the communication interfaces should be adapted. One of the biggest advantages of the presented approach is the fact that a continuous self-learning process is possible to be implemented. The presented concept of burglary protection modules supports the Original Equipment Manufacturers (OEMs), who expect the following procedures:

- to protect their products against cyber-attacks by real – time detection of anomalies in the network traffic on vehicle buses
- to pursue vertical integration in building their own cybersecurity hardware – software integrated stacks by providing a complete component
- to use artificial intelligence to protect vehicles against cyber-attacks by delivering trusted, reliable, and efficient AI algorithms
- to respond immediately to security incidents by real – time embedded modules connected to the cloud
- to discover a new or potential vulnerability in which their vehicles are attacked by malicious hackers by delivering trusted reliable and efficient AI algorithms embedded in real time approaches connected to cloud

Bibliography

Advanced Driver Assistance Systems (ADAS). (2023). Retrieved 08 23, 2023, from https://www.chipsaway.biz/blog/advanced-driver-assistance-systems-adas

Aliwa, E., Rana, O., Perera, C., & Burnap, P. (2021). Cyberattacks and countermeasures for in-vehicle networks. *ACM Computing Surveys (CSUR)*, 1-37.

Andrade, R., Santos, M., Justo, J., Yoshioka, L., Hof, H.-J., & Kleinschmidt, J. (2023). Security architecture for automotive communication networks with CAN FD. Retrieved from https://www.sciencedirect.com/science/article/pii/S016740482300113X

Aries, K. (2021, 6 4). *What Is V2V Technology?: V2V vs V2I vs V2X Technology Systems*. Retrieved 08 02, 2023, from https://www.verizonconnect.com/resources/article/connected-vehicle-technology-v2v-v2i-v2x/

Asfa, I. (2023). *Parts of a car and their functions explained*. Retrieved 08 28, 2023, from https://engineerine.com/parts-of-a-car/

Autoencoders. (2023). Retrieved from https://www.mathworks.com/discovery/autoencoder.html

Babaghayou, M., Labraoui, N., Ari, A., Ferrag, M., & Maglaras, L. (2020). The Impact of the Adversary’s Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles. *2020 5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM)*, (pp. 1-6). doi:10.1109/SEEDA-CECNSM49515.2020.9221839

Bosch, R. (1991). *Specification version 2.0. Published by Robert Bosch GmbH (September 1991)*. Retrieved 08 28, 2023, from http://esd.cs.ucr.edu/webres/can20.pdf

Buttigieg, R., Farrugia, M., & Meli, C. (2017). Security issues in controller area networks in automobiles. *2017 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, (pp. 93-98). doi:10.1109/STA.2017.8314877

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., . . . Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *20th USENIX security symposium (USENIX Security 11)*, (pp. 77-92).

Choi, J., & Jin, S.-i. (2019). Security Threats in Connected Car Environment and Proposal of In-Vehicle Infotainment-Based Access Control Mechanism. *Advanced Multimedia and Ubiquitous Engineering,* (pp. 383–388).

D'Andrada, L., Araujo-Filho, P., & Campelo, D. (2020). A Real-time Anomaly-based Intrusion Detection System for Automotive Controller Area Networks. *Brazilian Symposium on Computer Networks and Distributed Systems.* Retrieved from https://api.semanticscholar.org/CorpusID:234531030

Das, S., Bhowmik, S., & Giri, C. (2017). Design of asynchronous semantic preamble listening for semantic sensor network to avoid early overhearing. *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET),* (pp. 420-424). doi:10.1109/WiSPNET.2017.8299790

Desnitsky, V., & Kotenko, I. (2014). Expert Knowledge Based Design and Verification of Secure Systems with Embedded Devices. *Availability, Reliability, and Security in Information Systems* (pp. 194–210). Springer International Publishing.

(2019). *Development and Evaluation of Vehicle to Pedestrian (V2P) Safety Interventions.* Retrieved 08 02, 2023, from https://www.roadsafety.unc.edu/research/projects/2017r7/

Fahami, H., Zamzuri, H., Mazlan, S., & Zulkarnain, N. (2013). The Design of Vehicle Active Front Steering Based on Steer by Wire System. *Advanced Science Letters*, 61-65. doi:10.1166/asl.2013.4706

Falch, M. (2022). *CAN FD Explained - A Simple Intro [2023]*. Retrieved from https://www.csselectronics.com/pages/can-fd-flexible-data-rate-intro

Forest, T., & Jochim, M. (2011). On the Fault Detection Capabilities of AUTOSAR's End-to-End Communication Protection CRC's. *SAE Technical Papers*. doi:10.4271/2011-01-0999

Gajdzik, M. (2023). Metodyka wykrywania i rozpoznawania sygnałów sterujących na magistralach CAN w nowoczesnych pojazdach samochodowych. *Materiały Konferencji Młodych Naukowców nt.: Analiza zagadnienia, analiza wyników - wystąpienie młodego naukowca - Edycja V, 28-29.01.2023, Kraków*, (p. 43).

Gajdzik, M., Sternal, K., Timofiejczuk, A., & Przystałka, P. (2021). A Glimpse into the Low-Cost Protection Method Dedicated for Electric Cars. *2021 5th International Conference on Control and Fault-Tolerant Systems (SysTol).* IEEE. doi:10.1109/SysTol52990.2021.9595347

Gajdzik, M., Timofiejczuk, A., & Sebzda, W. (2021). Zastosowanie metody okien czasowych do zabezpieczenia danych podczas transmisji magistralą can w pojazdach samochodowych. *Metody komputerowe - 2021 : Studencka konferencja naukowa, Gliwice, wrzesień 2021*, (pp. 37–40).

Gajdzik, M., Timofiejczuk, A., & Sebzda, W. (2022). Zastosowanie metody programowych punktów testowych z możliwością wstrzykiwania informacji do pełnej diagnostyki elektronicznych modułów sterujących w pojazdach samochodowych. *Metody komputerowe - 2022. Studencka konferencja naukowa, Gliwice, czerwiec 2022*, (pp. 21-24).

Gajdzik, M., Timofiejczuk, A., Gnacy-Gajdzik, A., & Przystałka, P. (2023). Detection of Cyber Attacks in Electric Vehicles Using a Deep Neural Network. (pp. 144–153). Springer Nature Switzerland.

Garnaev, A., & Trappe, W. (2022). A Sophisticated Anti-Eavesdropping Strategy. *IEEE Wireless Communications Letters*, 1463-1467. doi:10.1109/LWC.2022.3174573

Giannopoulos, H., Wyglinski, A., & Chapman, J. (2017). Securing Vehicular Controller Area Networks: An Approach to Active Bus-Level Countermeasures. *IEEE Vehicular Technology Magazine*, 60-68. Retrieved from https://api.semanticscholar.org/CorpusID:28250361

Gillela, M., Prenosil, V., & Ginjala, V. (2019). Parallelization of Brute-Force Attack on MD5 Hash Algorithm on FPGA. *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)*, (pp. 88-93). doi:10.1109/VLSID.2019.00034

Gnacy–Gajdzik, A., Gajdzik, M., Przystałka, P., & Sternal, K. (2022). A Model-Based Approach for Testing Automotive Embedded Systems – A Preliminary Study. *Intelligent and Safe Computer Systems in Control and Diagnostics* (pp. 340–351). Springer International Publishing.

Greenberg, A. (2015). *Hackers Remotely Kill a Jeep on the Highway—With Me in It.* Retrieved 08 31, 2023, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Halim, Z., Kalsoom, R., Bashir, S., & Abbas, G. (2016). Artificial intelligence techniques for driving safety and vehicle crash prediction. *Artificial Intelligence Review,* 351-387. doi:10.1007/s10462-016-9467-9

Hartwich, , F., & Bosch , R. (2012). *CAN with Flexible Data-Rate, CAN in Automation.* Retrieved from https://www.cancia.org/fileadmin/resources/documents/proceedings/2012_hartwich.pdf

Hubaux, J., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. *IEEE Security & Privacy*, 49-55. doi:10.1109/MSP.2004.26

ISO 14229-1:2020 Road vehicles — Unified diagnostic services (UDS). (2020).

ISO/SAE 21434:2021. (2021). Retrieved from https://www.iso.org/standard/70918.html

J3061_202112: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - SAE International. (2021). Retrieved from https://www.sae.org/standards/content/j3061_202112/

Jadoon, A., Wang, L., Li, T., & Zia, M. (2018). Lightweight Cryptographic Techniques for Automotive Cybersecurity. *Wireless Communications and Mobile Computing*. doi:https://doi.org/10.1155/2018/1640167

Kabil, A., Rabieh, K., Kaleem, F., & Azer, M. (2022). Vehicle to Pedestrian Systems: Survey, Challenges and Recent Trends. doi:10.1109/ACCESS.2022.3224772

Kang, T., Song, H., Jeong, S., & Kim, H. (2018). Automated Reverse Engineering and Attack for CAN Using OBD-II. 1-7. Retrieved from https://api.semanticscholar.org/CorpusID:116880418

Kengo Oka, D. (2021). Overview of the Current State of Cybersecurity in the Automotive Industry. In *Building Secure Cars: Assuring the Automotive Software Development Lifecycle* (pp. 1-21). doi:DOI: 10.1002/9781119710783.ch1

Khandelwal, S. (2016, 09 20). *Hackers take Remote Control of Tesla's Brakes and Door locks from 12 Miles Away*. Retrieved from https://thehackernews.com/2016/09/hack-tesla-autopilot.html

King, C., & Klinedinst, D. (2016, 05 23). *Vehicle Cybersecurity: The Jeep Hack and Beyond*. Retrieved from https://insights.sei.cmu.edu/blog/vehicle-cybersecurity-the-jeep-hack-and-beyond/

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., . . . Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy*, (pp. 447-462). doi:10.1109/SP.2010.34

Koyama, T., Shibahara, T., Hasegawa, K., Okano, Y., Tanaka, M., & Oshima, Y. (2019). Anomaly Detection for Mixed Transmission CAN Messages Using Quantized Intervals and Absolute Difference of Payloads. *Proceedings of the ACM Workshop on Automotive Cybersecurity*. Retrieved from https://api.semanticscholar.org/CorpusID:85519054

Lee, H., Jeong, S., & Kim, H. (2017). OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame. *2017 15th Annual Conference on Privacy, Security and Trust (PST),* (pp. 57-5709). doi:10.1109/PST.2017.00017

Lendave, V. (2021). Retrieved 08 30, 2023, from https://analyticsindiamag.com/lstm-vs-gru-in-recurrent-neural-network-a-comparative-study/

Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. *IEEE Network*, 50-58. Retrieved from https://api.semanticscholar.org/CorpusID:10505056

Long Short-Term Memory (LSTM). (2023). Retrieved 08 04, 2023, from https://d2l.ai/chapter_recurrent-modern/lstm.html

Luo, F., Zhang, X., & Hou, S. (2021). Research on Cybersecurity Testing for In-vehicle Network. *2021 International Conference on Intelligent Technology and Embedded Systems (ICITES),* (pp. 144-150). doi:10.1109/ICITES53477.2021.9637070

Making the Connection with Vehicle to Network (V2N). (2022). Retrieved 08 04, 2023, from Making the Connection with Vehicle to Network (V2N): https://blog.rgbsi.com/connection-with-vehicle-to-network-v2n

Martínez-Cruz, A., Ramírez-Gutiérrez, K., Feregrino-Uribe, C., & Morales-Reyes, A. (2021). Security on in-vehicle communication protocols: Issues, challenges, and future research directions. *Computer Communications*, 1-20. doi:https://doi.org/10.1016/j.comcom.2021.08.027

Miyata, H. (2018). Digital Transformation of Automobile and Mobility Service. *2018 International Conference on Field-Programmable Technology (FPT),* (pp. 1-5). doi:10.1109/FPT.2018.00012

Muir, A. (2023). *Replacing a handbrake cable*. Retrieved 08 06, 2023, from https://www.howacarworks.com/brakes/replacing-a-handbrake-cable

Ndonda, G., & Sadre, R. (2017). A low-delay SDN-based countermeasure to eavesdropping attacks in industrial control systems. *2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN),* (pp. 1-7). doi:10.1109/NFV-SDN.2017.8169840

Nowdehi, N. (2019). Automotive Communication Security Methods and Recommendations for Securing In-vehicle and V2X Communications. Retrieved from https://api.semanticscholar.org/CorpusID:210140864

Nowdehi, N., Lautenbach, A., & Olovsson, T. (2017). In-Vehicle CAN Message

Authentication: An Evaluation Based on Industrial Criteria. 1-7. Retrieved from https://api.semanticscholar.org/CorpusID:46783086

Rae, A., & Wildman, L. (2003). A taxonomy of attacks on secure devices. *Proceedings of the Australia Information Warfare and Security Conference 2003*, (pp. 251-264).

Raikar, M., & Meena, S. (2021). SSH brute force attack mitigation in Internet of Things (IoT) network : An edge device security measure. *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC),* (pp. 72-77). doi:10.1109/ICSCCC51823.2021.9478131

Ruiz, J., Harjani, R., Mana, A., Desnitsky, V., Kotenko, I., & Chechulin, A. (2012). A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. *2012 20th Euromicro International Conference on Parallel, Distributed and Network-based Processing*, pp. 261-268. doi:10.1109/PDP.2012.36

Scalas, M., & Giacinto, G. (2019). Automotive Cybersecurity: Foundations for. *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS),* (pp. 1-6).

Self Study Program 891213 The ID.4 New Model Overview. (2021, 3). Retrieved 07 30, 2023, from https://static.nhtsa.gov/odi/tsbs/2021/MC-10189712-0001.pdf

Simacsek, B. (2019). *Can we trust our cars?* Retrieved from https://www.nxp.com/docs/en/white-paper/AUTOSECWP.pdf

Soja, R. (2014). *Automotive Security: From Standards to Implementation*. Retrieved 08 30, 2023, from https://www.nxp.com/docs/en/white-paper/AUTOSECURITYWP.pdf

Song, H., Kim, H., & Kim, H. (2016). Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. *2016 International Conference on Information Networking (ICOIN)*, (pp. 63-68).

Staggs, J. (2013). How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles. Retrieved from https://api.semanticscholar.org/CorpusID:42752899

Staron, M., & Durisic, D. (2017). AUTOSAR Standard. In *Automotive Software Architectures: An Introduction.* Springer International Publishing. doi:DOI: 10.1007/978-3-319-58610-6_4

Tariq, S., Kim, H., & Woo, S. (2020). CAN-ADF: The controller area network attack detection framework. *Computers & Security*. doi:https://doi.org/10.1016/j.cose.2020.101857

The course of studies in Mechatronics. (2023). Retrieved 08 20, 2023, from https://www.mechatronik.tu-darmstadt.de/fg_mec/studiengangmechatronik_mec/index.en.jsp

Tong, W., Hussain, A., Bo, W., & Maharjan, S. (2019). Artificial Intelligence for Vehicle-to-Everything: A Survey. *IEEE Access*. Retrieved from https://api.semanticscholar.org/CorpusID:59554672

(2020). *Upstream Security: 2020 Global Automotive Cyber security Report.* doi:https://doi.org/10.1016/S1353-4858(20)30005-2

Wang, J., Shao, Y., Ge, Y., & Yu, R. (2019). A Survey of Vehicle to Everything (V2X) Testing. *Sensors*. doi:10.3390/s19020334

Woo, S., Jo, H., & Lee, D. (2015). A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems*, 993-1006. Retrieved from https://api.semanticscholar.org/CorpusID:206740341

Wu, S., Jiang, Y., Luo, H., & Li, X. (2021). Deep learning-based defense and detection scheme against eavesdropping and typical cyber-physical attacks. *2021 CAA Symposium on Fault Detection, Supervision, and Safety for Technical Processes (SAFEPROCESS)*, (pp. 1-6). doi:10.1109/SAFEPROCESS52771.2021.9693596

Young, C., Svoboda, J., & Zambreno, J. (2020). Towards Reverse Engineering Controller Area Network Messages Using Machine Learning. *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, (pp. 1-6). doi:10.1109/WF-IoT48130.2020.9221383

Zou, Y., & Wang, G. (2016). Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. *IEEE Transactions on Industrial Informatics*, 780-787. doi:10.1109/TII.2015.2399691

List of figures

List of tables

Appendix

DATA BYTES	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D20	D21	-	-
BYTE INDEX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Fig. 83 Standard transmission data (all bytes)

DATA BYTES	CRC	MA IND	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D20	-
BYTE INDEX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Fig. 84 End-to-End protection data (all bytes)

DATA BYTES	CRC	MA IND	T_W	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12	D13	D14	D15	D16	D17	D18	D19	D20
BYTE INDEX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Fig. 85 Ent-to-End protection with time window data (all bytes)

Doctoral thesis – Summary

Identification and minimization of threats in embedded systems during the car vehicles maintenance, in accordance with Industry 4.0 concept

Author: MSc. Eng. Marcin Gajdzik

Supervisor: Ph.D. D.Sc. Eng. Anna Timofiejczuk, Associate Professor

Industry supervisor: Ph.D. Eng. Wojciech Sebzda

The main objective of this dissertation was to elaborate approaches allowing to minimize potential hazards of attacks in embedded systems in a car. A car is considered as an intelligent mechatronic vehicle integrated with the management system following several aspects of the "Industry 4.0" concept.

The PhD project was divided into research stages, presented in 4 experiments. The author focused his attention on various aspects regarding the possibility of eavesdropping, disruption or changing the content of frames during data transmission via the CAN bus.

Taking into account the current state-of-the-art in the CAN bus transmission in modern cars, a few concepts of attacks were prepared and tested. Each experiment consisted of 3 parts. In the first part the author focuses on checking whether it is possible to carry out an effective attack on the selected electronic control module. The second part is devoted to elaborating a solution increasing the level of security against the attack. In the third part of the experiments, the validation tests were carried out to confirm the effectiveness of the implemented security measures. It should be emphasized that it is not possible to obtain the security that gives a 100% guarantee, because even the most effective algorithms implemented in security cannot fully take into account new types of threats that are developing very quickly. The role of the author's original concepts presented in the thesis is to minimize the probability of a successful attack.

The dissertation resulted in the development of an innovative security concepts, taking into account contemporary expectations of the automotive industry. As the result of the PhD project a few concepts of relatively simple low-cost solutions were presented. There was also presented more advanced AI-based approach.

The overall results confirmed the high practical potential of developed concepts, which can be implemented in DRÄXLMAIER company. It should be stressed that the innovative burglary protection module supported by AI algorithms is especially interesting to be implemented. It can be successfully used for the development of new products of the company.

Praca doktorska - Streszczenie

Identyfikacja oraz minimalizacja zagrożeń w systemach wbudowanych przy eksploatacji samochodów zgodnie założeniami koncepcji "Przemysł 4.0"

Autor: Mgr inż. Marcin Gajdzik

Promotor: Dr hab. inż. Anna Timofiejczuk, prof. PŚ

Promotor wdrożeniowy: Dr inż. Wojciech Sebzda

Głównym celem rozprawy doktorskiej było opracowanie metod pozwalających na minimalizację potencjalnego zagrożenia wystąpienia ataków na systemy wbudowane w samochodzie. Współczesny samochód należy rozumieć jako inteligentny pojazd mechatroniczny zintegrowany z systemem zarządzania zgodnym z różnymi aspektami koncepcji „Przemysł 4.0”.

Całość pracy została podzielona na etapy badawcze, przedstawione w 4 eksperymentach. Autor skupił swoją uwagę na różnych aspektach związanych z możliwością podsłuchu, zakłócenia czy zmiany zawartości ramek podczas transmisji danych poprzez magistralę CAN. Biorąc pod uwagę aktualny stan wiedzy w zakresie transmisji magistrali CAN we współczesnych samochodach, przygotowano kilka koncepcji ataków, które można poddać testom. Każde doświadczenie składało się z 3 części. W pierwszej części eksperymentów autor skupia się na sprawdzeniu, czy możliwe jest przeprowadzenie skutecznego ataku na wybrany elektroniczny moduł sterujący. W drugiej części zaproponowano rozwiązanie zwiększające poziom zabezpieczenia przed takim atakiem. W trzeciej części eksperymentów przeprowadzono testy walidacyjne, mające na celu potwierdzenie skuteczności wdrożonych zabezpieczeń.

Należy podkreślić, że nie jest możliwe uzyskanie zabezpieczenia dającego 100% gwarancję, ponieważ nawet najbardziej efektywne algorytmy zaimplementowane w zabezpieczeniach nie są w stanie w pełni uwzględnić bardzo szybko się rozwijających nowych rodzajów zagrożeń. Rolą autorskich koncepcji przedstawionych w pracy jest minimalizowanie prawdopodobieństwa udanego ataku.

Kolejność i zakres eksperymentów zaplanowano w taki sposób, aby sprawdzić, czy możliwe jest przeprowadzenie skutecznego ataku na elektroniczny moduł wykonawczy, zwiększając poziom trudności w zależności od funkcjonalności, za jaką odpowiadał

atakowany ECU.

Efektem rozprawy doktorskiej było opracowanie innowacyjnych koncepcji zabezpieczeń, uwzględniających potrzeby przemysłu motoryzacyjnego. Zaprezentowano koncepcje stosunkowo prostych, tanich rozwiązań, jak również złożonych, opartych na algorytmach sztucznej inteligencji.

Wyniki otrzymane w ramach weryfikacji potwierdziły wysoki potencjał praktyczny zaimplementowanych propozycji, które można wdrożyć w firmie DRAEXELMAIER. Szczególnie innowacyjny moduł antywłamaniowy, wspierany algorytmami opartymi na zastosowaniach sztucznej inteligencji, może z powodzeniem zostać wykorzystany przy opracowywaniu nowych produktów firmy.