Scientific Journal of the Military University of Land Forces
ISSN: 2544-7122 (print), 2545-0719 (online)
2024, Volume 56, Number 1(211), Pages 77-96
DOI: 10.5604/01.3001.0054.4255

# Cybersecurity of autonomous vehicles – threats and mitigation

**Artur Szymonik**

General Tadeusz Kościuszko Military University of Land Forces, Wrocław, Poland,
e-mail: artursz85@gmail.com

INFORMATION

**Article history:**

Submited: 6 November 2023

Accepted: 13 February 2024

Published: 31 March 2024

## ABSTRACT

The aim of this article is to draw attention to the growing problem of cybersecurity in the field of autonomous vehicles. A notable aspect is the use of autonomous vehicles to enhance the quality of decision-making processes as well as flexibility and efficiency. The implementation of new solutions will lead to improvements not just in transportation and delivery, but also in warehouse management. The growing demand for autonomous solutions, both in the industry and in the daily life of an average consumer, necessitates efforts to ensure their safe operation and use. The present literature review synthetically describes the history of the development of autonomous vehicles and machines. The standards and norms that should be met by products allowed for use as well as threats to cybersecurity, along with examples, are presented herein. The analysis of the collected materials leads to the conclusion that with the development of new technologies and the growth in the importance of autonomous solutions, the number of threats and the importance of systems securing the functioning of devices in cyberspace are increasing. Research on the problem also leads to the conclusion that legal systems do not fully keep up with technological developments, resulting in a lack of normative acts regulating this matter.

**KEYWORDS**

safety, cybersecurity, autonomous vehicles, AI

## Introduction

Many technologies have recently been developed by integrating the Internet of Things (IoT) with autonomous vehicles, aiming to offer efficient transport solutions and create intelligent systems. Such technologies are connected to the cloud, enabling fast information exchange. The integration of autonomous vehicles with other devices is called V2X. M. Muhammad and G.A. Safdar developed the following five definitions describing the connection of vehicles with different objects: vehicle – vehicle (V2V); vehicle – roadside (V2R); vehicle – infrastructure (V2I); vehicle – personal devices (V2P) and vehicle – sensors (V2S) (Muhammad, Safdar, 2018). According to the authors, all types of connections require solutions based on constant access to the internet, enabling uninterrupted information exchange between different areas of intelligent transport.

Solutions in the field of autonomous vehicles (AVs) result from technological progress in the field of transport and logistics. Thanks to built-in systems, AVs can identify the environment, location and space in which they are located. Moreover, as a rule, they are operated without human intervention or control (Leminen et al., 2022). Their system consists of radars, lidars, GPS and vision systems, among others. According to a report by McKinsey & Company, AVs will account for 15% of the automotive market sales by 2030. For this reason, the largest manufacturers in the industry, such as Ford, Volvo or Toyota, have announced the sales of AVs in the coming years (Rauniyar et al., 2018). The solutions being developed are intended to reduce traffic jams, increase efficiency and safety, save money and improve the mobility of children, elderly and disabled people. The primary goals for AVs include the following:

- increasing road safety by striving for the complete elimination of accidents and road incidents;
- optimising traffic efficiency and fluidity (transmitting data about traffic jams, accidents, among others), controlling speed;
- support in driving a vehicle, including stability control, automatic breaks, cruise control, fuel consumption optimisation;
- remote monitoring and operation support;
- enabling data acquisition anywhere and anytime without manual control;
- aiming to reduce malfunctions based on data generated by vehicles;
- reducing pollutant emissions;
- developing sustainable supply chains (Perussi et al., 2019).

The following chapters will focus on the brief history and levels of autonomous solutions.

## 1. Brief history and levels of autonomous vehicles

The most influential events in the history of autonomous driving are summarised below:

- 1980s
  - A robotic van developed by Mercedes-Benz, equipped with sensors, cameras and neural networks for steering controls, was able to run without a human driver at a speed of 63 km/h (39 mph) on traffic-free streets;
  - Carnegie Mellon University was one of the pioneers in using neural networks for controlling vehicles.
- 1994
  - A vehicle developed by Daimler-Benz, called VaMP, was able to travel 998 kilometre (620 miles) on a highway without human interventions.
- 1995
  - As part of Carnegie Mellon University's Navlab project, a semi-autonomous car was developed that was able to travel almost 5000 kilometres (3107 miles) using autonomous steering;
  - A re-engineered autonomous S-Class Mercedes-Benz was able to complete an almost 1600 kilometre (994 miles) journey across Europe.
- 1996
  - The ARGO project, developed by the University of Parma, Italy, was able to complete an almost 2000 kilometre (1243 miles) journey on highways using stereo-vision technology.
- 1998
  - Toyota was the first automaker to introduce laser-based Adaptive Cruise Control.
- 2004
  - During the DARPA Grand Challenge, a competition that took place in the desert, AVs had to complete a 241 kilometres (150 mile) route. Unfortunately, none of the 15 finalists were able to complete the course, and the $1 million prize went unclaimed.

- 2005
  - The second DARPA Grand Challenge took place in a desert environment with the assistance of maps. Five teams managed to finish the course, with Stanford University's modified Volkswagen named Stanley emerging as the winner;
  - BMW started working on autonomous driving.
- 2007
  - Carnegie Mellon University won the third DARPA Grand Challenge, also known as the Urban Challenge, with their autonomous robotic SUV named Boss.
- 2009
  - Google began developing its self-driving car.
- 2010
  - In September 2010, Audi sent an autonomous version of its TTS sports car to navigate to the top of Pike's Peak without a driver. The car was guided only by computers and GPS and reached speeds of up to 72 km/h (45 mph);
  - VisLab, a research group at the University of Parma, conducted the first intercontinental autonomous challenge in 2010. The challenge, called the VisLab Intercontinental Autonomous Challenge (VIAC), involved four AVs navigating with minimal human intervention on an almost 16,000 kilometre (9942 miles) trip from Parma, Italy, to Shanghai, China;
  - *The Stadtpilot project*, developed by the Institute of Flight Guidance at the Technische Universität Braunschweig, was one of the first in the world to demonstrate the ability of driving autonomously in real urban traffic scenarios.
- 2011
  - General Motors developed the *Electric Networked-Vehicle* (EN-V), which is an autonomous urban car. The EN-V is a two-seat electric concept car that can be driven normally or operated autonomously;
  - A self-driving car named *The Spirit of Berlin*, created by the Freie Universität Berlin, successfully navigated the city streets, obeying traffic signals and roundabouts, from the Internationales Congress Centrum to the Brandenburg Gate. *The MadeInGermany* vehicle was also tested to handle traffic, traffic lights and roundabouts.
- 2012
  - Volkswagen tested its Autopilot system, which was capable of driving autonomously on highways at speeds of up to 129 km/h (80 mph);

  - Google's self-driving car passed its first driving test on public roads in Nevada.
- 2013
  - VisLab, a research group at the University of Parma, conducted a successful autonomous urban test;
  - Daimler R&D's S-Class drove autonomously for 100 km using stereo vision and radars. The car was able to navigate through complex traffic situations, including roundabouts and intersections, without any human intervention;
  - The Nissan Leaf, an all-electric car, was granted a license to drive on Japanese highways with semi-autonomous features;
  - The Mercedes S-Class had several autonomous driving features, including autonomous steering, lane keeping and parking. The car was equipped with a variety of sensors, including cameras, radars, and ultrasonic sensors, which enabled it to detect other vehicles and obstacles on the road.
- 2014
  - The Navia shuttle, developed by Induct, became the world's first commercially available self-driving vehicle.
- 2015
  - Volvo announced that it will commence working on autonomous driving;
  - Tesla released AutoPilot via a software update;
  - Uber teamed up with Carnegie Mellon University to develop autonomous cars;
  - Delphi Automotive successfully completed the first-ever coast-to-coast journey in the US using automated driving technology.
- 2016
  - Legal concerns were raised following the first fatal accident involving a Tesla AutoPilot in Florida;
  - Velodyne LiDAR and Ford Motor Company announced a partnership to develop the next generation of R&D cars;
  - Singapore became the first country to launch a self-driving taxi service, thanks to nuTonomy.
- 2017
  - Apple was said to be conducting research on 3D laser scanners for use in self-driving cars;

  - Velodyne announced the launch of VLS-128, a high-performance LiDAR sensor with 128 laser beams, the best resolution, and the widest field of view among self-driving vehicles in the world;
  - Waymo completed over 3 million kilometres (2 million miles) of fully autonomous driving on public roads;
  - The Audi A8 was the first production car to offer Level 3 autonomy, which meant that the driver did not need to supervise things at all, so long as the car stayed within guidelines. That meant driving no faster than 60 km/h (37 mph), which is why Audi called the feature AI Traffic Jam Pilot.
- 2018
  - Waymo and Jaguar Land Rover announced a long-term strategic partnership to develop the world's first premium self-driving electric vehicle;
  - An Uber self-driving car struck and killed a pedestrian in Tempe, Arizona, raising legal concerns.
- 2019
  - Twenty-nine US states passed laws permitting autonomous cars;
  - Subaru and Toyota announced the extension of their 14-year collaboration to develop new vehicles for the new era.
- 2020
  - Regulation (EU) 2019/2144 was established in 2019 and implemented in 2022 within the European Union (EU), specifically for automated and fully automated vehicles;
  - In June 2020, the UNECE WP.29 GRVA formulated a regulation concerning SAE Level 3;
  - In October 2020, Tesla launched a "beta" version of its "Full Self-Driving" software to a select group of testers in the US.
- 2021
  - Honda started leasing a limited edition of 100 Legend Hybrid EX sedans in Japan, which were equipped with the newly approved Level 3 automated driving equipment. This equipment, known as the "Traffic Jam Pilot" driving technology, received safety certification from the government of Japan and legally allowed drivers to divert their attention from the road;
  - Mercedes-Benz was granted approval in Germany for a Level 3 Automated Lane Keeping System (ALKS) self-driving technology that met the legal requirements of UN-R157.

- 2022
  - Mercedes-Benz initiated the sale of its Drive Pilot system in Germany; the system was capable of functioning at SAE Level 3 autonomy;
  - With the support of Yamaha Motor and TIER IV, in December 2022, eve autonomy launched “eve auto”, a commercial service that offered autonomous transportation with electric work vehicles. This was the first service in Japan to achieve SAE Level 4 autonomy, and it was deployed at nine locations, including three Yamaha Motor factories;
  - Robotaxis from Cruise received permission from the California Public Utilities Commission to operate on the streets of San Francisco;
  - Baidu and Pony.ai were given permission to start a robotaxi service with no driver behind the wheel in April 2022 in China (*Autonomous Vehicle Trends 2023 and Milestones From 2022*, 2022);
  - Arbe partnered with Veoneer to develop a 4D imaging radar for AVs (*Veoneer partners with Arbe to Expand the Boundaries of High-Performance Perception-Level Automotive Radars*, 2022).
- 2023
  - The “Road Traffic Act” in Japan was amended to permit Level 4 autonomy, which meant that vehicles could drive themselves without human intervention under certain conditions;
  - California approved the Mercedes-Benz Level 3 autonomous driving system for public roads (Walz, 2023).

In 2019, the International Society of Automotive Engineers (SAE) created a universal standard that defined six levels of driving automation, from no driving automation (level 0) to full driving automation (level 5) (Fig. 1):

- Level 0 – No Driving Automation;
- Level 1 – Driver Assistance;
- Level 2 – Partial Driving Automation;
- Level 3 – Conditional Driving Automation:
  - BMW’s 7 Series was set to become the next car to achieve Level 3 autonomy, with the technology expected to be available in the second half of 2022,
  - Stellantis, a global automaker, tested its Level 3 autonomous driving technology, Highway Chauffeur, on public roads in Italy in 2021. The company used Maserati Ghibli and Fiat 500X prototypes equipped with Highway Chauffeur, which could take over the driving task under certain conditions. Stellantis aimed to launch cars with Level 3 capability by 2024,

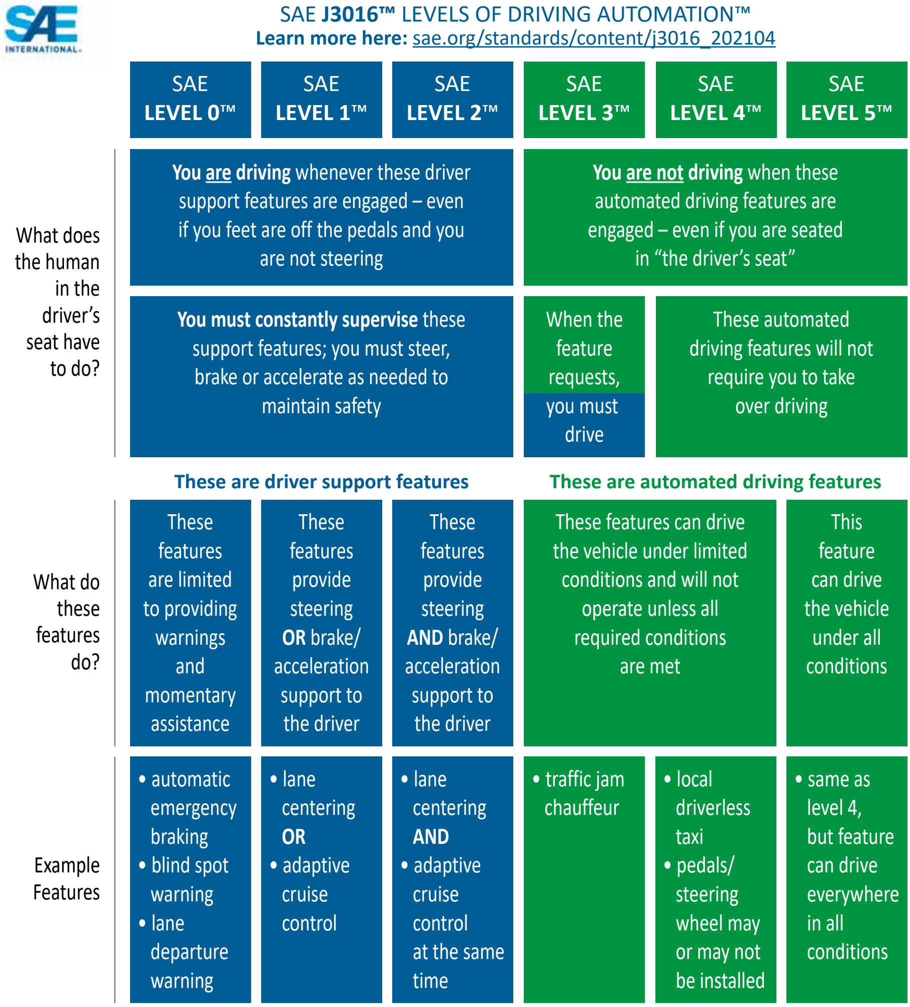
  - In 2022, Polestar, a subsidiary of Volvo Cars, announced that it would be incorporating Level 3 autonomous driving technology in its Polestar 3 SUV, which was the successor to the Volvo XC90. The system was to utilise technologies from Luminar Technologies, Nvidia and Zenseact,
  - Bosch and Volkswagen Group subsidiary CARIAD announced a partnership to develop a standardised software platform for mass production of vehicles up to SAE Level 3, with plans to explore targets for Level 4 systems,
  - To launch its Level 3 self-driving Genesis G90 in Korea soon, Hyundai Motor Company has been working on enhancing the cybersecurity of its connected cars. Level 3 autonomy means that a car can handle most driving situations, but the driver must be ready to intervene when needed,
  - 2022, Honda started working on the development of advanced Level 3 self-driving technology to function at any speed below legal limits on highways by 2029, with the aim of eliminating traffic deaths involving the company's vehicles,
  - 2023, Drive Pilot, a Level 3 autonomous driving system from Mercedes-Benz, got the green light in Nevada and set to seek approval in California by mid-2023. The system, which can take over the driving task on highways, was to be offered as an optional feature for some models in the US market in the latter half of 2023;

– Level 4 – High Driving Automation (*AV Development Continues, Level 5 Autonomy Coming Soon to Consumer Cars*, 2021):

  - Vehicles that can drive themselves without any human intervention or supervision are being used by Cruise and Waymo to provide self-driving taxi services in a few US cities,
  - In 2020, Toyota was testing its TRI-P4 autonomous driving technology, which has Level 4 capability, with public demonstration rides using the Lexus LS (fifth generation). The company also operated a potentially Level 4 autonomous driving service using its e-Palette vehicles around the Tokyo 2020 Olympic Village in August 2021,
  - In 2020, the new S-Class from Mercedes-Benz came with the Intelligent Park Pilot, a Level 4 AVP system that could park a car without a driver. This was the first system of its kind in the world to be commercially available, but it can only work where the law allows it,
  - In 2021, Honda began testing its Level 4 autonomous driving technology in Japan as part of its collaboration with Cruise and General

Motors to launch a mobility service business. At the World Congress on Intelligent Transport Systems, Honda revealed that it was testing its Level 4 self-driving technology on Legend Hybrid EX vehicles that had been modified for this purpose,

- In 2022, General Motors and Cruise requested permission from the National Highway Traffic Safety Administration to manufacture and launch a self-driving vehicle, the Cruise Origin. The vehicle is unique in that it does not have any human controls such as steering wheels



SAE **J3016™** LEVELS OF DRIVING AUTOMATION™
**Learn more here:** sae.org/standards/content/j3016_202104

| | SAE **LEVEL 0™** | SAE **LEVEL 1™** | SAE **LEVEL 2™** | SAE **LEVEL 3™** | SAE **LEVEL 4™** | SAE **LEVEL 5™** |
|---|---|---|---|---|---|---|
| What does the human in the driver's seat have to do? | **You are driving** whenever these driver support features are engaged – even if you feet are off the pedals and you are not steering | | | **You are not driving** when these automated driving features are engaged – even if you are seated in "the driver's seat" | | |
| | **You must constantly supervise** these support features; you must steer, brake or accelerate as needed to maintain safety | | | When the feature requests, you must drive | These automated driving features will not require you to take over driving | |
| | **These are driver support features** | | | **These are automated driving features** | | |
| What do these features do? | These features are limited to providing warnings and momentary assistance | These features provide steering **OR** brake/ acceleration support to the driver | These features provide steering **AND** brake/ acceleration support to the driver | These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met | | This feature can drive the vehicle under all conditions |
| Example Features | • automatic emergency braking<br>• blind spot warning<br>• lane departure warning | • lane centering **OR**<br>• adaptive cruise control | • lane centering **AND**<br>• adaptive cruise control at the same time | • traffic jam chauffeur | • local driverless taxi<br>• pedals/ steering wheel may or may not be installed | • same as level 4, but feature can drive everywhere in all conditions |

Fig. 1. Levels of vehicles' autonomy

Source: *SAE Levels of Driving Automation™ Refined for Clarity and International Audience* (2021).

or brake pedals. The collaborators were expected to begin production in late 2022 at the General Motor's Factory Zero in Detroit,
  - In 2022, Honda announced the collaboration with Cruise and General Motors to launch a self-driving vehicle mobility service in Japan. In September 2022, a prototype of the Cruise Origin designed for Japan was completed and began testing,
  - In 2023, the HOLON Mover, a self-driving shuttle that runs on electricity and can go up to 290 kilometres (180 miles) with one charge, was unveiled by HOLON, a new brand from the Benteler Group, at the CES 2023 in Las Vegas. The company claims that the vehicle is the first Level 4 shuttle in the world that meets the automotive standard. The HOLON Mover is planned to be produced in the US by the end of 2025;

– Level 5 – Full Driving Automation:
  - As defined by the SAE, Level 5 means that the vehicle is fully autonomous and can handle all driving tasks without any human intervention in all driving conditions and environments. As of now, there are no vehicles with Level 5 of autonomy.

## 2. Regulations and standards

In the fast-changing automotive sector, the relationship between safety and security has become vital. In July 2022, the European Commission announced that it was willing to allow robots to take over driving duties. The Vehicle General Safety Regulation, which takes effect at present, mandates a range of advanced driver assistant systems that are expected to improve road safety. The regulation establishes the legal basis for the authorisation of automated and fully driverless vehicles in the EU. The new safety measures are expected to save over 25,000 lives and prevent at least 140,000 serious injuries by 2038, thereby protecting passengers, pedestrians and cyclists throughout the EU.

With the General Safety Regulation, the European Commission has created the legal framework for automated and connected vehicles. The EU is a leader in the field, as it is preparing to introduce technical rules for the approval of fully driverless vehicles. The European Commission believes that these rules will enhance public confidence, foster innovation and strengthen the competitiveness of Europe's car industry. The Executive Vice-President of the European Commission for a Europe Fit for the Digital

Age, Margrethe Vestager, has said that technology can help make cars safer. She also mentioned that the new advanced and mandatory safety features would further reduce the number of casualties. The European Commission is taking measures to ensure that its rules allow for the safe introduction of autonomous and driverless vehicles in the EU, with a framework that prioritises people's safety. The European Commission's new vehicle safety legislation, which came into effect on 6 July 2022 (European Commission, 2022), aims to improve road safety and establish a legal framework for the approval of automated and fully driverless vehicles in the EU. It requires the implementation of numerous sophisticated driver aid systems to enhance the road safety. For all road vehicles (i.e. cars, vans, trucks and buses), the new measures include:

– intelligent speed assistance;
– reversing detection with camera or sensors;
– attention warning in case of driver drowsiness or distraction;
– event data recorders as well as an emergency stop signal.

In the EU, the law requires that all new vehicles have advanced driver assistant systems that can help prevent accidents and protect people on the road, whether they are inside or outside the vehicle. These new safety measures are expected to save over 25,000 lives and avoid at least 140,000 serious injuries by 2038.

Thierry Breton, the European Commissioner for Internal Market, has stated that the new legislation will ensure that the above-described technology improves citizens' daily lives. The legislation is to guarantee a predictable and safe framework for the automotive industry to continue rolling out innovative technology solutions while maintaining its global competitiveness.

Cars and vans must have features including systems that keep them in their lane and brakes that work automatically. Buses and trucks must have technologies that can effectively detect blind spots, warn of possible crashes with pedestrians or cyclists and check the tire pressure. At present, the rules are to affect new vehicle types, and from 7 July 2024, they will apply to all new vehicles. Until 2029, some of the new measures will be extended to include different types of road vehicles.

The European Commission intends to establish technical regulations for autonomous and interconnected vehicles, with an emphasis on automated vehicles taking over the driver's role on highways (Level 3 automation) and completely AVs such as city shuttles or robotaxis (Level 4 automation). The imminent regulations will harmonise the EU laws with the new UN standards on Level 3 automation and introduce new EU technical laws for completely AVs. The first global regulations of this nature will set up a thorough evaluation of the safety and readiness of fully automated vehicles prior to their introduction to the EU market. They will encompass protocols for testing, stipulations for cybersecurity, regulations for data recording, as well as the supervision of safety performance and the obligations for incident reporting by producers of entirely AVs (European Commission, n.d.). The updated General Safety Regulation, enacted in November 2019, aims to enhance the safety of vehicles and roads, considering that research indicates the contribution of human error in 95% of accidents. Since its inception, the Regulation has been complemented by a range of corresponding enforcement regulations that address the various driver assistance initiatives introduced by the Regulation. Along with the proposal for the revised General Safety Regulation, the Commission also published the EU's strategy on automated mobility, which outlines the EU actions to support the deployment of connected and automated mobility systems (European Commission, 2022).

In addition to the described regulations, car manufacturers follow certain standards when developing software and/or hardware for the automotive industry.

The international ISO 26262 standard for functional safety in road vehicles offers a comprehensive framework for handling the safety of electrical and electronic systems. It assists automotive manufacturers and suppliers throughout the development process by ensuring that potential hazards arising from system malfunctions are identified and resolved. By adopting ISO 26262, companies can systematically analyse risks, implement safety measures and conduct rigorous testing and validation to achieve an acceptable level of functional safety (International Organization for Standardization, 2018).

Given the growing connectivity and complexity of modern vehicles, cybersecurity has become a pressing issue. The advent of connected cars, autonomous driving systems and overtheair updates has broadened the scope for potential cyber threats. Unauthorised access, data breaches and remote manipulation of vehicle systems pose substantial risks to both driver safety and privacy. Consequently, it is crucial to establish robust cybersecurity measures to safeguard against malicious activities and potential compromises of the vehicle's electronic systems (Fig. 2).

ISO 26262, the international standard for functional safety in road vehicles, primarily focuses on functional safety. However, it also includes

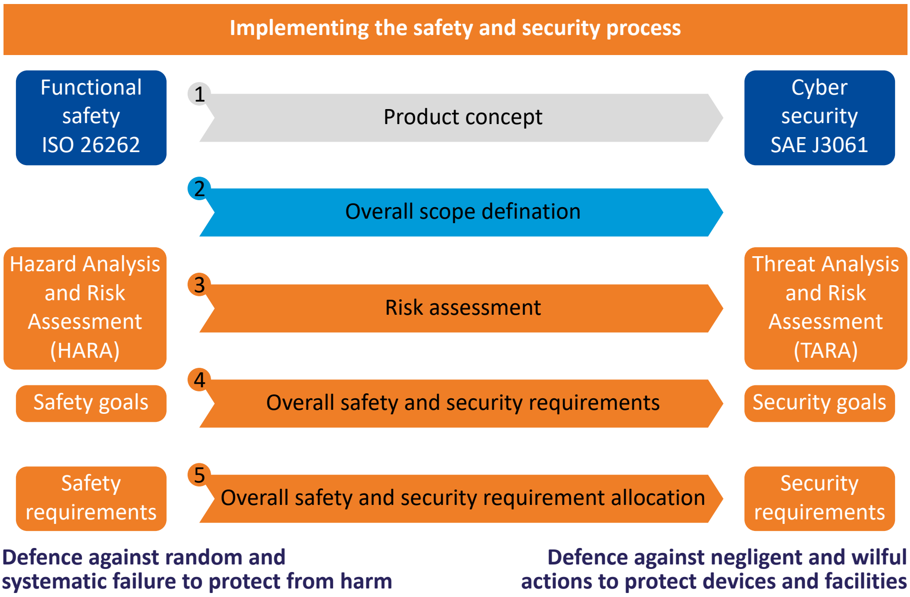

Implementing the safety and security process
Functional safety ISO 26262
1
Product concept
Cyber security SAE J3061
2
Overall scope defination
Hazard Analysis and Risk Assessment (HARA)
3
Risk assessment
Threat Analysis and Risk Assessment (TARA)
Safety goals
4
Overall safety and security requirements
Security goals
Safety requirements
5
Overall safety and security requirement allocation
Security requirements
Defence against random and systematic failure to protect from harm
Defence against negligent and wilful actions to protect devices and facilities

Fig. 2. Implementation of a safety and security process

Source: (Rangappla, 2023).

several provisions that overlap with cybersecurity considerations. These synergies can be leveraged to create a comprehensive safety and security strategy for automotive systems. For instance:

- **Risk Analysis** is a crucial aspect of both ISO 26262 and cybersecurity frameworks. ISO 26262 primarily focuses on safety hazards, while cybersecurity frameworks identify vulnerabilities and threats. By integrating these two risk assessment processes, a holistic approach can be adopted to identify potential hazards and security weaknesses.
- **System Design**: ISO 26262 emphasises functional safety across the system's lifecycle, while cybersecurity practices focus on secure design principles. Aligning these design processes helps mitigate safety risks associated with cyber threats, such as unauthorised system access or manipulation.
- **Testing and Validation**: ISO 26262 requires comprehensive testing and validation of safety-related systems. Manufacturers can identify vulnerabilities and validate the effectiveness of security measures alongside safety functions by incorporating cybersecurity testing methodologies (Rangappla, 2023).

Another standardisation document followed by manufacturers in the automotive industry is ISO/SAE 21434:2021 Road vehicles – Cybersecurity engineering which addresses cybersecurity in the road vehicle industry. It specifies engineering requirements for cybersecurity risk management throughout the lifecycle of electrical and electronic (E/E) systems in road vehicles, including their components and interfaces. The document defines a framework that includes requirements for cybersecurity processes and a common language for communicating and managing cybersecurity risk. It is applicable to series production road vehicle E/E systems, including their components and interfaces, the development or modification of which began after the publication of this document. However, it does not prescribe specific technology or solutions related to cybersecurity (International Organization for Standardization, 2021).

## 3. Examples of threats to autonomous mobile robots

There is a good reason for all the regulations and safety standards mentioned in the previous chapter, as AVs relying on the newest technologies are potentially exposed to cyber-attacks. Some of the many ways of gaining access to an AV are listed below (Harris, 2022):

- remote access via the Internet;
- remote access via Bluetooth;
- inserting a backdoor into a self-driving car via the maker of the vehicle (supply chain);
- planting a specialised device into a vehicle;
- interfering with the sensors of a vehicle.

A good example showing what a cyberattack can look like is an experiment in which two hackers hijacked a Jeep and disabled it on a highway (WIRED, 2015). Hackers were able to take over the steering and all other functions of the car, leaving the driver without any real influence on the car's behaviour. It was a very spectacular demonstration of what can happen, but it was just an experiment. Other examples of cybersecurity breaches include the following:

- hacker disabling more than 100 cars in Austin, Texas (Poulsen, 2018);
- the release of information about loopholes in Tesla Model S systems by Marc Rogers and Kevin Mahaffey in 2015 (Zetter, 2015);
- opening the door of the Tesla Model X using a drone by Ralf-Philipp Weinmann and Benedikt Schmotzle in 2020, exposing flaws in Tesla's security.

Those are just a few instances of possible threats that might occur in the future if manufacturers do not put more emphasis on the security systems in their vehicles before they reach the last level of autonomy.

In addition to the recommendations already mentioned, there are several significant challenges that researchers can tackle to help achieve security objectives in future AVs.

The theft of data is a serious and growing problem that affects various sectors. In 2020, the average cost of a single data breach was about $3.86 million (Upstream Security, 2021). The large volumes of data that future AVs collect and use can make them vulnerable to data theft, which can have different impacts on safety, security and economy depending on the type and severity of the breach. Such thefts can expose the data of individual users as well as the data of vehicle original equipment manufacturers which are their intellectual property. For example, attackers can use stolen user information to launch more effective socially engineered attacks. The source material covers the topics of security, trust and privacy in AVs in depth (Muhammad, Alhussein, 2022). The automotive domain needs to use techniques such as the confidentiality, integrity, availability (CIA) and distributed immutable ephemeral (DIE) models to protect the data and privacy of future AVs. AI algorithms can perform better than traditional methods in detecting intrusions and assisting drivers in AVs, but they can also be fooled by malicious attacks that are designed to trick them (Eykholt et al., June 18-23, 2018). As vehicles become more connected, it is anticipated that DDoS attacks (where communication between vehicles is blocked) and Sybil attacks (where a vehicle operates with multiple identities) will become more prevalent. These attacks can confuse AI algorithms and potentially cause failure across vehicle subsystems. Recent model inversion attacks, which attempt to reconstruct training data from model parameters, have also become a growing concern (Chen et al., October 10-17, 2021). Automakers' proprietary data used to train AI models is at risk due to adversarial attacks. As new and scalable learning methods, such as federated learning in data centre environments, emerge, it becomes more crucial to have AI algorithms that are secure and robust against adversarial attacks. The source material provides a comprehensive review of adversarial attacks on AI/ML algorithms in connected and autonomous vehicles (CAVs), as well as the methods to defend against them and the open challenges that remain (Qayyum et al., 2020).

Semiconductor integrated circuit (IC) components in vehicles need to have secure supply chains, as they are made in different parts of the world.

Any weakness in the supply chain that affects any component of the vehicle can have disastrous effects on AVs. The need for RSUs and 5G infrastructure to enable intelligent transportation systems makes this issue even worse. The source material discusses the main concerns about the IC supply chain and a technique to hide the logic of the ICs to protect them (Shamsi et al., 2019). Some techniques that can help secure the supply chain are digital watermarking, IC fingerprinting and IC metering. These techniques can help identify the origin and authenticity of the IC components.

Recently, researchers have investigated the application of WiGig networks that utilise the IEEE 802.11ad multiple gigabit wireless system (MGWS) standard operating at a frequency of 60 GHz for communication within vehicle networks. The capacity to facilitate high-speed data transfer and accommodate applications with minimal latency has the potential to revolutionise both in-vehicle networking and forthcoming autonomous driving applications. A recent study (Nino et al., October 28-31, 2020) illustrates the potential of employing IEEE 802.11ad millimetre wave (mmWave) for communication among ECUs within a vehicle, with an observed worst-case throughput approximating 300 Mbps. Blockchain technology represents another ground breaking innovation that could potentially transform the landscape of future self-driving vehicles. The blockchain's distributed ledger offers precise and concurrent access to various data types, such as traffic details and enhanced vehicle tracking data for carpooling applications. An all-encompassing strategy that utilises blockchain to address the security and privacy concerns in AVs has been previously examined (Gupta at al., 2020). Given that these technologies are still nascent in the automotive field, it is crucial to evaluate them thoroughly by identifying potential weaknesses and investigating security measures to bolster security (Kukkala et al., 2022).

## Conclusion

The present article delves into the significant cyber-attacks that have transpired in the automotive sector in the last ten years. It also showcases cutting-edge solutions that utilise AI and suggests a strategic plan for the development of secure AVs. The strategic plan underscores crucial technical and regulatory matters that require attention, in addition to the unresolved challenges that persist. The fundamental components of the cybersecurity roadmap and the unresolved challenges underscore the essential issues that must be tackled to resolve the cybersecurity dilemma in upcoming AVs. As shown herein, future vehicles will face complex and evolving security challenges across their entire infrastructure. Therefore, it is essential to design vehicles with cybersecurity in mind, using the best practices discussed in the present work. Additionally, robust hardware and software solutions as well as proactive threat intelligence will play a key role in achieving the security objectives needed to protect vehicles from sophisticated attacks.

Despite the obvious need for high-level cybersecurity measures, there are deficits in legal regulations regarding this matter. In addition to developing norms and standards, it would be worthwhile to create an appropriate legal framework and institutional frameworks for the authorities responsible for maintaining the desired level of cybersecurity. The establishment of preventive measures and prosecution of cybercriminals are also important. This article aims to draw attention to the area of cybersecurity for vehicles and autonomous machines, which in recent years has undergone very dynamic development and is likely to become one of the most important security issues in the near future.

## References

*Autonomous Vehicle Trends 2023 and Milestones From 2022*. (2022). https://www.geospatialworld.net/prime/autonomous-vehicle-trends-2023-milestones-2022/

*AV Development Continues, Level 5 Autonomy Coming Soon to Consumer Cars*. (2021). https://www.arrow.com/en/research-and-events/articles/av-development-continues-level-5-autonomy-coming-soon-to-consumer-cars

Chen, S., Kahla, M., Jia, R., Qi, G.J. (October 10-17, 2021). *Knowledge-Enriched distributional model inversion attacks* [article]. 2021 IEEE/CVF International Conference on Computer Vision (ICCV). Montreal, Canada.

European Commission. (n.d.). *Internal Market, Industry, Entrepreneurship and SMEs*. Retrieved October 10, 2023 from: https://single-market-economy.ec.europa.eu/sectors/automotive-industry/vehicle-safety-and-automatedconnected-vehicles_en

European Commission. (2022). *New rules to improve road safety and enable fully driverless vehicles in the EU*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4312

Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T., Song, D. (June 18-23, 2018). *Robust physical-world attacks on deep learning visual classification* [article]. IEEE/CVF Conference on Computer Vision and Pattern Recognition. Salt Lake City, USA.

Gupta, R., Tanwar, S., Kumar, N., Tyagi, S. (2020). Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review. *Computers & Electrical Engineering, 86*. https://doi.org/10.1016/j.compeleceng.2020.106717

Harris, J.R. (2022). *Can Driverless Vehicles Be Hacked?*. https://www.hlmlawfirm.com/blog/can-driverless-vehicles-be-hacked/

International Organization for Standardization. (2018). *Road vehicles – Functional safety – Part 1: Vocabulary*. (ISO Standard No. 26262-1:2018) https://www.iso.org/obp/ui/en/#iso:std:68383:en

International Organization for Standardization. (2021). *Road vehicles – Cybersecurity engineering*. (ISO/SAE 21434:2021) https://www.iso.org/obp/ui/en/#iso:std:70918:en

Kukkala, V.K., Thiruloga, S.V., Pasricha, S. (2022). *Roadmap for Cybersecurity in Autonomous Vehicles*. https://www.researchgate.net/publication/358143292_Roadmap_for_Cybersecurity_in_Autonomous_Vehicles

Leminen, S., Rajahonka, M., Wendelin, R., Westerlund, M., Nyström, A. (2022). Autonomous vehicle solutions and their digital servitization business models. *Technological Forecasting and Social Change*, *185*. https://doi.org/10.1016/j.techfore.2022.122070

Muhammad, G., Alhussein, M. (2022). Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. *IEEE Consumer Electronics Magazine, 11*(6), 49-55. https://doi.org/10.1109/mce.2021.3089880

Muhammad, M., Safdar, G.A. (2018). Survey on existing authentication issues for cellular-assisted V2X communication. *Vehicular Communications*, *12*, 50-65. https://doi.org/10.1016/j.vehcom.2018.01.008

Nino, R., Nishio, T., Murase, T. (October 28-31, 2020). *IEEE 802.11ad Communication Quality Measurement in In-vehicle Wireless Communication with Real Machines* [article]. *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. New York, USA.

Perussi, J.B., Gressler, F., Seleme, R. (2019). Supply Chain 4.0: Autonomous Vehicles and Equipment to Meet Demand. *International Journal of Supply Chain Management, 8*(4). https://ojs.excelingtech.co.uk/index.php/IJSCM/article/view/2275

Poulsen, K. (2010). *Hacker Disables More Than 100 Cars Remotely*. https://www.wired.com/2010/03/hacker-bricks-cars/

Qayyum, A., Usama, M., Qadir, J., Al-Fuqaha, A. (2020). Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward. *IEEE Communications Surveys & Tutorials, 22*(2), 998-1026. https://doi.org/10.1109/comst.2020.2975048

Rangappla, V. (2023). *Harmonizing ISO 26262 and Cybersecurity: Driving Safety & Security in Automotive Systems*. https://www.linkedin.com/pulse/harmonizing-iso-26262-cybersecurity-driving-safety-vikram-rangappla/

Rauniyar, A., Hagos, D.H., Shrestha, M. (2018). A Crowd-Based Intelligence Approach for Measurable Security, Privacy, and Dependability in Internet of Automated Vehicles with Vehicular Fog. *Mobile Information Systems, 2018*. https://doi.org/10.1155/2018/7905960

*SAE Levels of Driving Automation™ Refined for Clarity and International Audience*. (2021). https://www.sae.org/blog/sae-j3016-update

Shamsi, K., Li, M., Plaks, K., Fazzari, S., Pan, D.Z., Jin, Y. (2019). IP protection and supply chain security through logic obfuscation: A systematic overview. *ACM Transactions on Design Automation of Electronic Systems*, *24*(6), 1-36. https://doi.org/10.1145/3342099

Upstream Security. (n.d.). *Upstream Security's 2021 Global Automotive Cybersecurity Report*. Retrieved October 10, 2023 from: https://upstream.auto/2021report

*Veoneer partners with Arbe to Expand the Boundaries of High-Performance Perception-Level Automotive Radars*. (2022). https://www.prnewswire.com/news-releases/veoneer-partners-with-arbe-to-expand-the-boundaries-of-high-performance-perception-level-automotive-radars-301643475.html

Walz, E. (2023). *California approves Mercedes-Benz Level 3 autonomous driving system for public roads*. https://www.automotivedive.com/news/mercedes-benz-level-3-autonomous-driving-in-california/652727/

WIRED. (2015, July 21). *Hackers remotely kill a jeep on a highway* [video]. YouTube. https://www.youtube.com/watch?v=MK0SrxBC1xs

Zetter, K. (2015). *Researchers Hacked a Model S but Tesla's Already Released a Patch*. https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/

## Cyberbezpieczeństwo pojazdów autonomicznych – zagrożenia i przeciwdziałanie im

**STRESZCZENIE** Celem artykułu jest zwrócenie uwagi na rosnący problem cyberbezpieczeństwa w dziedzinie pojazdów autonomicznych. Istotnym aspektem jest wykorzystanie pojazdów autonomicznych do poprawy jakości procesów decyzyjnych oraz zwiększenia ich elastyczności i efektywności. Wdrożenie nowych technologii poprawi nie tylko procesy transportowe i dostawy, ale także zarządzanie magazynami. Rosnące zapotrzebowanie na rozwiązania autonomiczne, zarówno w przemyśle, jak i w codziennym życiu przeciętnego konsumenta, prowadzi do konieczności zwiększenia wysiłków na rzecz zapewnienia ich bezpiecznej pracy i użytkowania. W przeglądzie literatury przedstawiono syntetycznie historię rozwoju pojazdów i maszyn autonomicznych, a także normy i standardy, jakie powinny spełniać produkty dopuszczone do użytku, a ponadto zagrożenia dla cyberbezpieczeństwa wraz z przykładami. Analiza zebranego materiału prowadzi do wniosku, że wraz z rozwojem nowych technologii i wzrostem znaczenia rozwiązań autonomicznych liczba zagrożeń oraz znaczenie systemów zabezpieczających funkcjonowanie urządzeń w cyberprzestrzeni wzrasta. Badania nad problemem prowadzą również do konkluzji, że systemy prawne nie nadążają za postępem technologicznym, co skutkuje brakiem aktów normatywnych regulujących przedmiotową kwestię.

**SŁOWA KLUCZOWE** bezpieczeństwo, cyberbezpieczeństwo, pojazdy autonomiczne, sztuczna inteligencja

### Biographical note

**Artur Szymonik** – Major, PhD, graduated with a master's degree in economics at the War Studies University and in law at the University of Warsaw. Since 2010, having completed his officer training course at the Military University of Land Forces in Wrocław, he has been a professional soldier. In the years 2010-2019, he held the following posts in succession: platoon commander, staff officer and company commander, then an expert in the Armaments Agency in the period 2020-2022 and in the Command of Warsaw Garrison in the years 2022-2023. Currently, an expert at the General Tadeusz Kościuszko Military University of Land Forces. Doctoral dissertation defended in 2022 in the field of social science in the discipline of security studies.

### ORCID

Artur Szymonik https://orcid.org/0000-0002-6308-2782

### Acknowledgement

No acknowledgement and potential funding was reported by the author.

### Conflict of interests

The author declared no conflict of interests.

### Author contributions

The author contributed to the interpretation of results and writing of the paper. The author read and approved the final manuscript.

### Ethical statement

The research complies with all national and international ethical requirements.