CENTER OF AUTOMOTIVE MANAGEMENT

Prof. Dr. Stefan Bratzel

Automotive Cyber Security

White Paper

A study in cooperation with Cisco Systems

Version 1.01 (Status as of: December 20, 2023)

Table of Contents

Executive Summary

This white paper argues that cyber security is set to be one of the biggest multiple challenges facing the automotive industry in the coming years. For automotive companies, the topic of "cyber security performance" is becoming an indispensable "hygiene factor".

With the increasing digitalization and networking of vehicles and the trends towards electromobility and autonomous driving, the need for an effective cyber security policy is increasing. At the same time, however, customer requests for "connected vehicles" and "connected services" are generating enormous competitive and time-to-market pressure, which can push the cyber security aspects into the background. In addition, the implementation of automotive cyber security is very demanding and complex: Essentially, it covers the entire product life cycle of the vehicle from the development and production through to vehicle use and must be secured in a complex value chain with distributed responsibility in a large supplier and partner network.

New regulatory requirements for cybersecurity in motor vehicles (UN R155 (15) / Regulation (EU) 2018/858) must be adopted by manufacturers in the EU from July 2022 for all new vehicle types and, from July 2024, for all existing vehicle types. The implementation of the various standards is necessary, but at the same time has far-reaching consequences and is costly for the industry.

The meta-analysis carried out on cyber-attacks on vehicles and companies in the automotive industry lays bare the urgency and the rapidly increasing risks. Evaluations of the previous points of attack on cyber security of the automotive industry internationally reveal that the quantity and quality of attacks has increased significantly in recent years. The supply chain and the complex supplier landscape are considered a major weak point and represent central points of attack with a high probability of occurrence and often also a high level of damage. A "deep dive" on electromobility highlights that the charging infrastructure for electric vehicles is one of the most vulnerable cyber security areas. The charging ecosystem is extremely complex due to its various market participants and essentially offers many points of attack for cyber criminals. Overall, the analysis of the cyber-attacks reveals that awareness in the industry regarding the hazards and risks is still significantly underdeveloped.

The development of a high level of "cyber security performance" in automotive companies requires great efforts and must be continuously monitored. The companies located at different levels and stages of the value chain in the industry differ significantly with regard to the quality of the design and implementation of cyber security programs. This white paper proposes a model for the empirical assessment of the cyber security performance of automotive companies. The "4C" model combines relevant cyber security performance criteria in four dimensions: Competencies, Cooperations, Culture & Organization and Cyber Strategy. It is argued that the fulfillment of these cyber security criteria is an important prerequisite for high performance quality of cyber security and thus for the long-term success in the companies.

1.Introduction

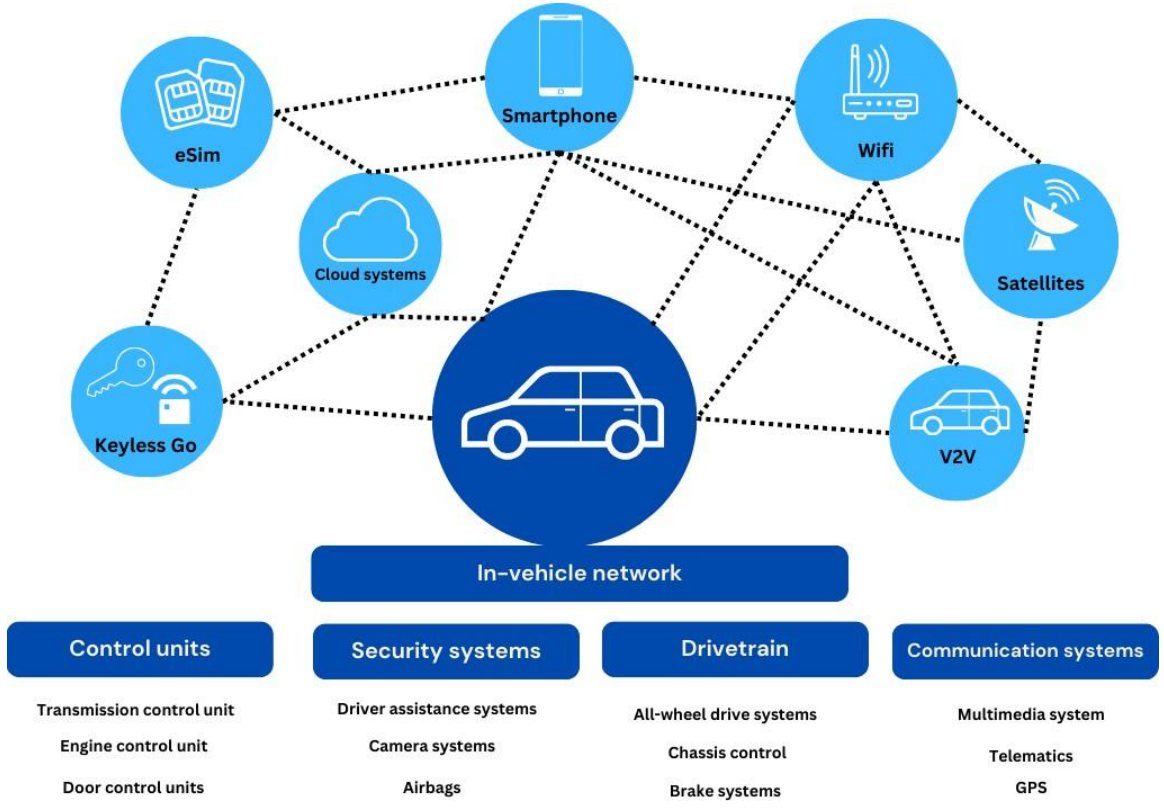
Challenges of cyber security in the automotive industry

In the automotive industry, with the increasing digitalization and networking of vehicles as well as the trends towards electromobility and autonomous driving, the need for an effective cyber security policy in companies is also increasing. The number of connected vehicles alone increased from 330 million in 2018 to around 775 million in 2023 (Juniper Research, cited in: Global Automotive Cyber Security Report 2022, p. 7). Based on the data and platform economy, digitalization in the mobility economy is penetrating the entire value chain of the companies involved (Bratzel/Böbber 2023, p. 18 ff.). Connected vehicles represent a central future innovation and value creation pool for the automotive industry with which they want to generate added value for their customers e.g. by means of connected services, over-the-air (OTA) software updates or autonomous driving.

This significantly increases the risk of cyber-attacks. The collection and processing of large amounts of data from various players in the vehicle ecosystem creates many points of attack through numerous sensors and control devices in the vehicle (infotainment, V2X, charging) that are networked with the outside world, as well as in the backend servers of automobile manufacturers and suppliers. With electromobility and the increasing networking of vehicles (vehicle-to-x communication), the number of interfaces of the vehicle and of the automotive ecosystem is increasing. As a result, the possibilities for attacks increase exponentially (charging infrastructure, SIM, WLAN, Bluetooth, USB, radio key, diagnostic interface, etc.). Accordingly, automobile manufacturers are not only confronted with the cyber security of their own vehicle, but also of the entire value creation network. For automobile manufacturers, reducing potential points of attack conflicts with the goal of further networking the vehicle and offering networked services and autonomous driving.

Accordingly, there is a need for all players in the vehicle ecosystem, i.e. manufacturers, system suppliers, SMEs as well as other players in the (charging) ecosystem, to counter the threat of cyber risks through appropriate strategies and processes.

Fig. 1: Attack Points of the Connected Vehicle



Source: CAM based on Vosseler et al. (2021), p. 4

Definition of cyber security in the automotive industry

Automotive cyber security encompasses the vehicles including the digital ecosystem and the entire product life cycle.

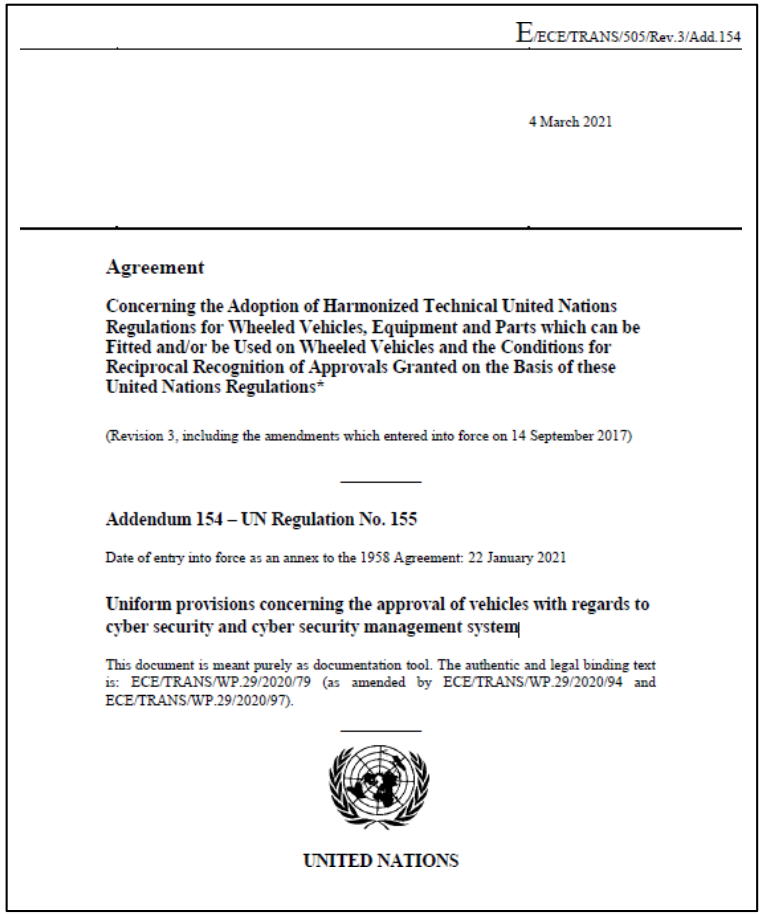
Cyber-attacks can have a significant impact on the safety of drivers, passengers, and other road users. Cyber security governance is required to ensure that automobile manufacturers can protect their **vehicles from cyber-attacks.**

However, as the vehicles are networked with the backend servers of automobile manufacturers, with the external infrastructure (e.g. charging ecosystems) or the customer's home or end devices, cyber security **encompasses the entire digital ecosystem with many companies involved.** Cyber security is not only limited to the use phase of vehicles, but affects the entire product life cycle, i.e. vehicle development, production, and vehicle use.

Cyber **security** in the automotive industry refers to the techniques and measures that are used to **prevent and defend against cyber attacks on vehicle systems, networks and data**. This includes the implementation of security measures, compliance with security standards, the monitoring of data traffic and the provision of security solutions. These measures are primarily aimed at ensuring the security of vehicles and the underlying systems and protecting the integrity of the data.

"*Cyber security* means the condition in which road vehicles and their functions are protected from cyber threats to electrical or electronic components." (UNECE 2021: 4)

Fig. 2: UN Regulation No. 115



E/ECE/TRANS/505/Rev.3/Add.154

4 March 2021

Agreement

Concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations*

(Revision 3, including the amendments which entered into force on 14 September 2017)

Addendum 154 – UN Regulation No. 155

Date of entry into force as an annex to the 1958 Agreement: 22 January 2021

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

This document is meant purely as documentation tool. The authentic and legal binding text is: ECE/TRANS/WP.29/2020/79 (as amended by ECE/TRANS/WP.29/2020/94 and ECE/TRANS/WP.29/2020/97).

UNITED NATIONS

Source: UNECE (2021)

Aim of the study and methodological approach

The aim of the study is to analyze the status and the challenges of cyber security in the automotive industry and to make a reliable comparison of the performance and quality of cyber security management in automobile companies. In addition to increasing *awareness* of the topic, the indirect long-term goal is to *improve the cyber security* of vehicles and automobile companies. The multi-year study series is supported by Cisco Systems.

The following key questions are to be addressed:

- What is the **status of implementation of cyber security management** (UNECE WP.29 R155/R156 and ISO/SAE 21434)?
- What are **the challenges** of automotive cyber security ? What are the critical areas of action (vehicle, backend, etc.)?
- What are the **quality/performance characteristics** of cyber security or cyber security management?
- What dimensions and **criteria** are useful **for evaluating the performance** of automotive cyber security?

The first section of this white paper examines the **state of practice** in the area of automotive cyber security.

- The initial focus will be on the standards and the regulatory environment of the connected vehicle ecosystem.
- Then, the empirical results on CS incidents and attacks in the automotive industry will be discussed.
- There then follows a discussion, in a deep dive, on the cyber security of the automotive charging ecosystem.
- Lastly, the central challenges and starting points of cyber security will be summarized.

In the second section, approaches and **criteria for evaluating the quality of cyber security in automotive companies** are developed.

- First, the "4C" model is presented as a heuristic evaluation approach that addresses the following dimensions of cyber security performance: Competencies, Cooperations, Culture & Organization, Cyber Strategy
- On the basis of the model, the first elements of a survey concept with corresponding criteria and indicators are then presented.

Methodologically, the study is based on a comprehensive literature analysis of empirical studies on cyber security in the automotive industry. In addition, expert discussions were held with high-ranking representatives of automobile manufacturers, suppliers and associations. The results were also reflected upon in expert workshops.

CENTER OF AUTOMOTIVE MANAGEMENT

2. State-of-Practice – Cyber security in the automotive industry

2.1 Standards and regulation for the connected vehicle ecosystem

The regulatory environment of automotive cyber security

The topic of cyber security has been accompanied by a multitude of laws, regulations and standards, most of which complement each other.

At the highest legislative level, especially in Europe, are the UNECE regulations. These include the UNECE R-155 for cyber security and the R-156 for software updates. They prescribe, among other things, the implementation of management systems and relevant processes for securing legal requirements. Similar initiatives exist in China and the USA, although UNECE R- 155/156 does not apply in these countries.

The UNECE regulations are further defined by national laws (e.g the German national legal framework for implementation of SAE L4 applications).

In addition there are norms and standards that offer standardized, specified development frameworks, artifacts and processes which need to be implemented in a security-related development (ISO 21434 Cyber Security or ISO 20077 Extended Vehicle).

The laws must be integrated into the development of security-related customer functions and must be considered and designed across the entire digital software life cycle. The entire end-to-end (E2E) impact chain must be considered. (cf. McKinsey 2022; P3 2022: 20-22)

Table 1: Overview of Relevant (National) Rules and Regulations

(National) Rules & Regulations	Product Safety, (National) Rules & Regulations Liability & Quality
UNECE is currently the central topic for homologation and approval. A UNECE certification is a basic requirement for approval in Europe and Asia/Pacific (excluding USA China). The following UNECEs are particularly relevant for autonomous driving : - Uniform Provisions Concerning the Approval of: Vehicles with Regard to Steering Equipment (R.79-01) - Cyber Security MS (R.155) - Software Update SUMS (R.156) - Automated Lane Keeping Systems (R.157)	Product safety includes all design measures and activities that prevent harm or risk to people or property. The ultimate goal is to produce robust and safe products. Relevant regulations are: - Functional Safety (**ISO 26262**) - SOTIF (**ISO/PAS 21448** or UL 4600)
Germany currently allows autonomous driving functions up to SAE level 4 (general vehicle approvals were given up to SAE L2 ; as of: 02/21) **US registration regulations** and laws for autonomous driving functions **vary from state to state** (max. SAE L4) – **UNECE does not apply** **China** currently allows prototype testing up to SAE L3 & SAE L4 – an adapted ICV legislation with an expanded V2I approach will, however, come into force this year – **UNECE does not apply**	Product security describes the ability to protect and defend the use of cyber- physical networks against external manipulation and attacks. Automotive-related regulations are: - **ISO 27001** Information Security - **ISO 21434** Automotive Cyber Security - **ISO 20077** Extended Vehicle - **ISO 15408** Evaluation Criteria for IT Security - **ISO/TR 4804** Safety and Cyber Security for automated driving systems - Software Updates etc.
	The automotive industry also requires broad coverage of additional standards : - Quality Management **ISO 900x/IATF 16949** - Process Maturity **ISO 15504/ASPICE** - Energy Management/Environmental Management (e.g. **ISO 50001/14001**)

Source: P3 (2022), p. 21; CAM

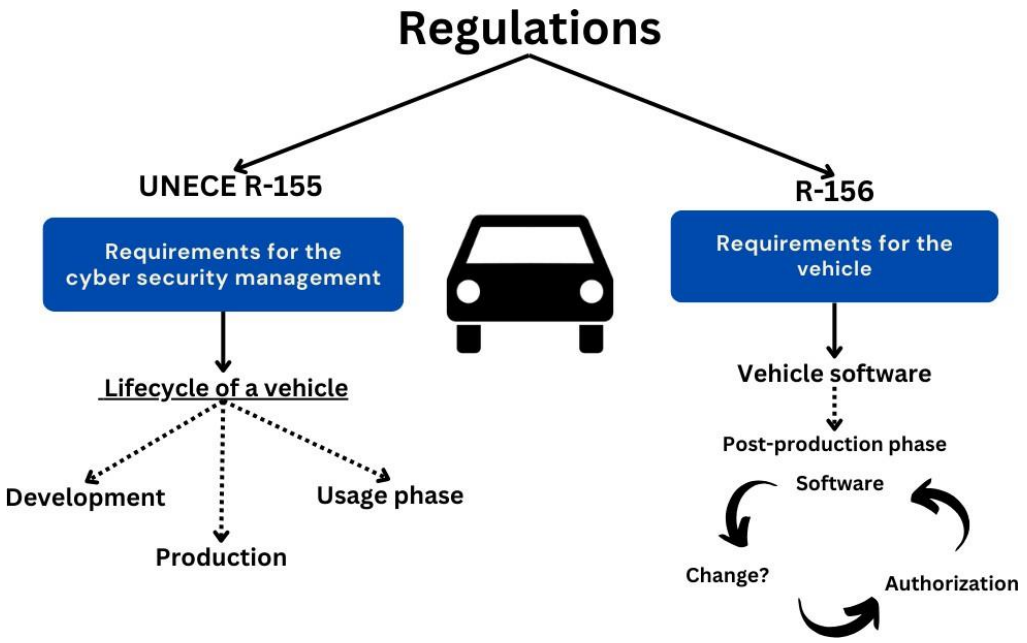
Standards and regulation for the connected vehicle life cycle

An important step of a uniform approach to addressing cyber security risks are the UNECE regulations adopted in year 2021 UNECE R-155 (Cyber Security and Cyber Security Management System), UNECE R-156 (Software Update Management System) and the standard ISO/SAE 21434 of the International Organization for Standardization. Neither of them provides specific solutions and precise processes, but emphasizes by way of their guidelines that CS hazards and risks must be taken into account in vehicle development, production and throughout the life cycle of the vehicle.

The UN Regulation for Automotive Cyber Security is an international standard created by the World Forum for Harmonization of Vehicle Regulations (WP.29). It defines cyber security technical requirements for vehicles and systems. The UNECE R-155 and R-156 are mandatory requirements for the homologation of vehicles in more than 50 countries. Similar regulations are expected to follow in the other core markets, USA and China, which have not signed up to the UN regulation. The UNECE regulation has divided the automotive cyber security into two sub-areas :

- The UNECE R-155 outlines requirements for an automobile manufacturer's Cyber Security Management System (CSMS). The entire **life cycle of a vehicle** is taken into account from development, through to production and the use phase. The OEMs must also take into account compliance with the CS-related measures of their automobile supplier.
- The R-156 Regulation focuses on the **vehicle software** in the post-production phase, i.e. software approved in production must be re-approved, if changes are made that affect the vehicle's security.

Fig. 3: UN Cyber Security Regulations



"*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to treat risk.

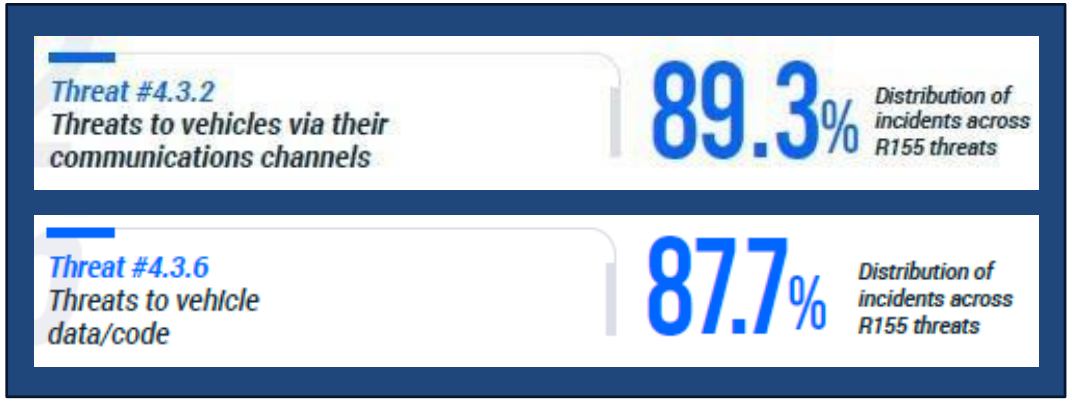
Source: CAM based on Zastrow (2022)

Levels of threats/vulnerabilities

The UNECE Regulation for Automotive Cyber Security identifies various areas of threats and vehicle vulnerability. These refer, among other things, to attacks on the backend servers, communication channels, connectivity, software updates and vehicle data (cf. p. 12).

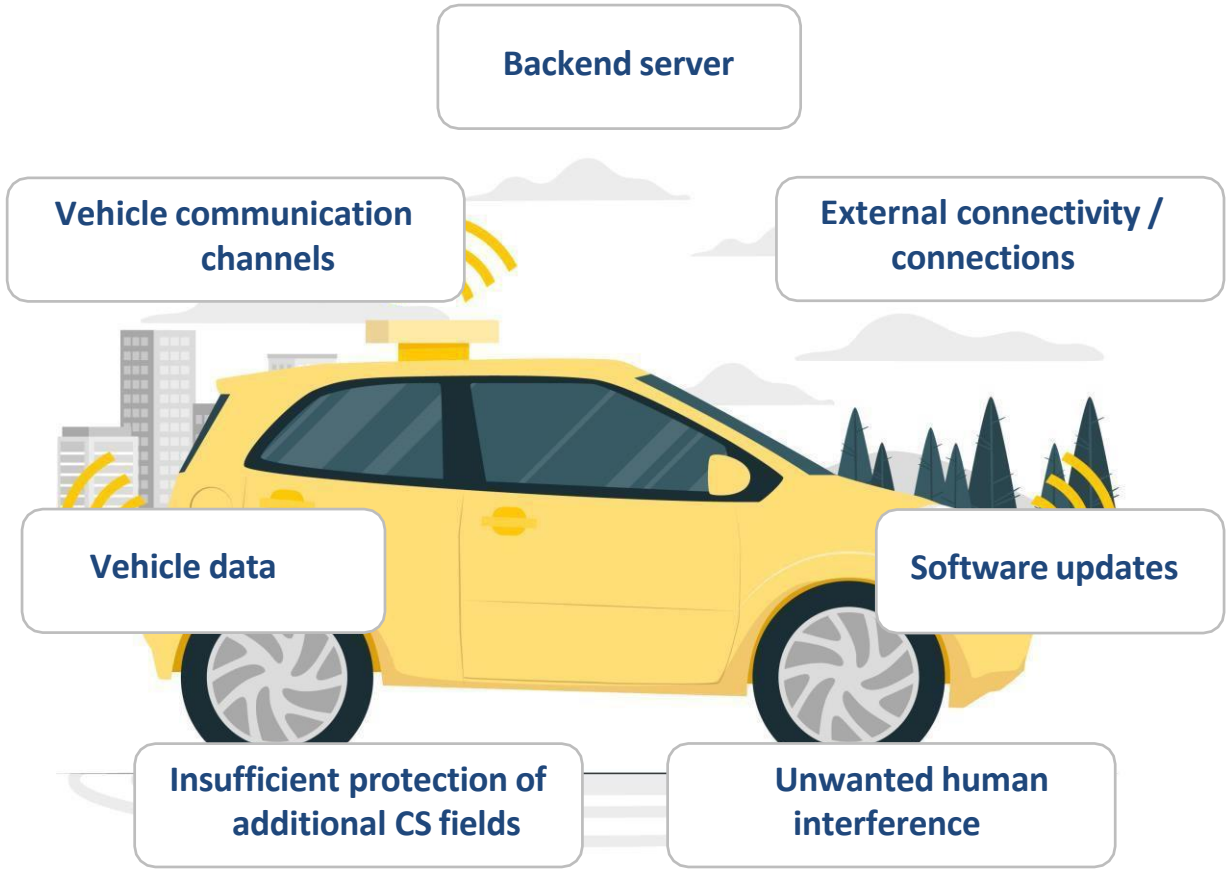
The empirical analysis of CS incidents in the automotive industry in 2020/2021 reveals that around 90% of attacks take place via the **communication channels of the vehicle** and in the area of **vehicle data** (cf. p. 21).

These incidents can have a significant impact on the confidentiality, integrity and availability of data and information. Ensuring information security according to the general principles (cf. ISO 27001) is therefore also the remit of cyber security management.



Source: Upstream (2022)

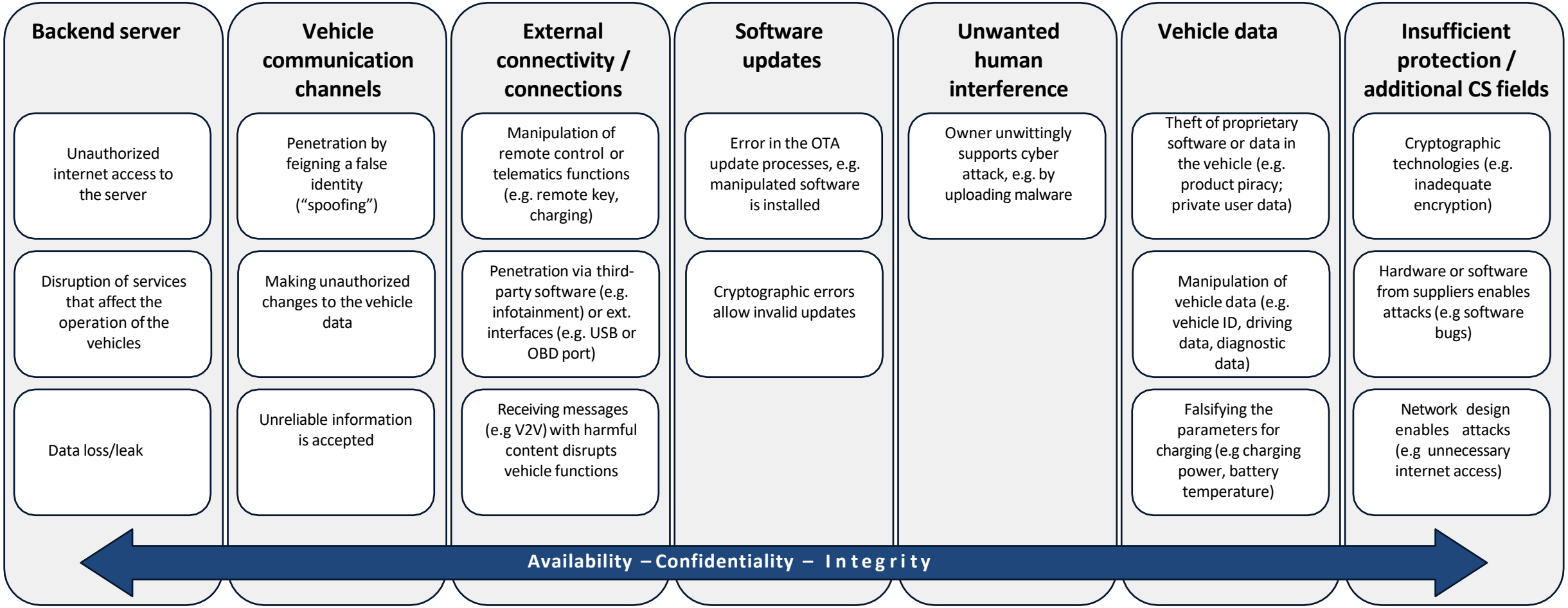
Fig. 4: Threat areas for cyber security attacks according to UNECE R-155



Source: CAM, compilation based on UNECE R-155

Automotive cyber security: levels of threats/vulnerabilities according to UNECE R-155

Fig. 5: Examples of threats/vulnerability according to UNECE R-155



Source: CAM, compilation based on UNECE R-155, Appendix 5

Obligations of cyber security according to the UNECE regulation

The regulatory requirements for cybersecurity in motor vehicles in accordance with the UNECE regulation UN R155 (15) and Regulation (EU)2018/858 have been mandatory for manufacturers to implement on all new vehicle types since July 2022. In **July 2024,** all **new and existing vehicle types** will be subject to UN R155 type approval for cyber security.

In order to minimize the numerous threats, the UNECE Regulation (UNECE WP.29 R155) requires automobile manufacturers to have in operation a **Cyber Security Management System** (CSMS). It must demonstrate that the processes of the CSMS take appropriate account of security. This results in **obligations to define organizational processes, responsibilities and governance of risk management.**

At the same time, a **comprehensive reporting obligation** is required, which must be submitted to the licensing authorities or to the technical service at least once a year. This should also outline the results of **monitoring of cyber attacks** and the counter-measures introduced. In addition, according to Art. 33 (1) GDPR, there **is an obligation to report** if, firstly, there is a personal data breach and, secondly, if this breach results in a significant risk for the data subjects.

The requirement, which will apply from July 2024, poses major technical and economic challenges for automobile manufacturers. For example, in response, Volkswagen has already announced that the VW Up! will be discontinued from the summer of 2024 without a direct successor. The reason cited is the high costs of developing a new electronics architecture, which would not be economically viable (cf. Ecomento 2023). Porsche also has to withdraw the Macan from the market prematurely due to inadequate compliance with regulations in the EU. In the USA and China, the countries that together account for around two thirds of Macan sales and in which the UN R155 does not apply, the vehicle will continue to be offered for sale (cf. Wittich 2023).

Fig. 6: Examples of Vehicles Affected by UN R155

Volkswagen e-Up!

Image source: Volkswagen

Porsche Macan

Image source: Porsche

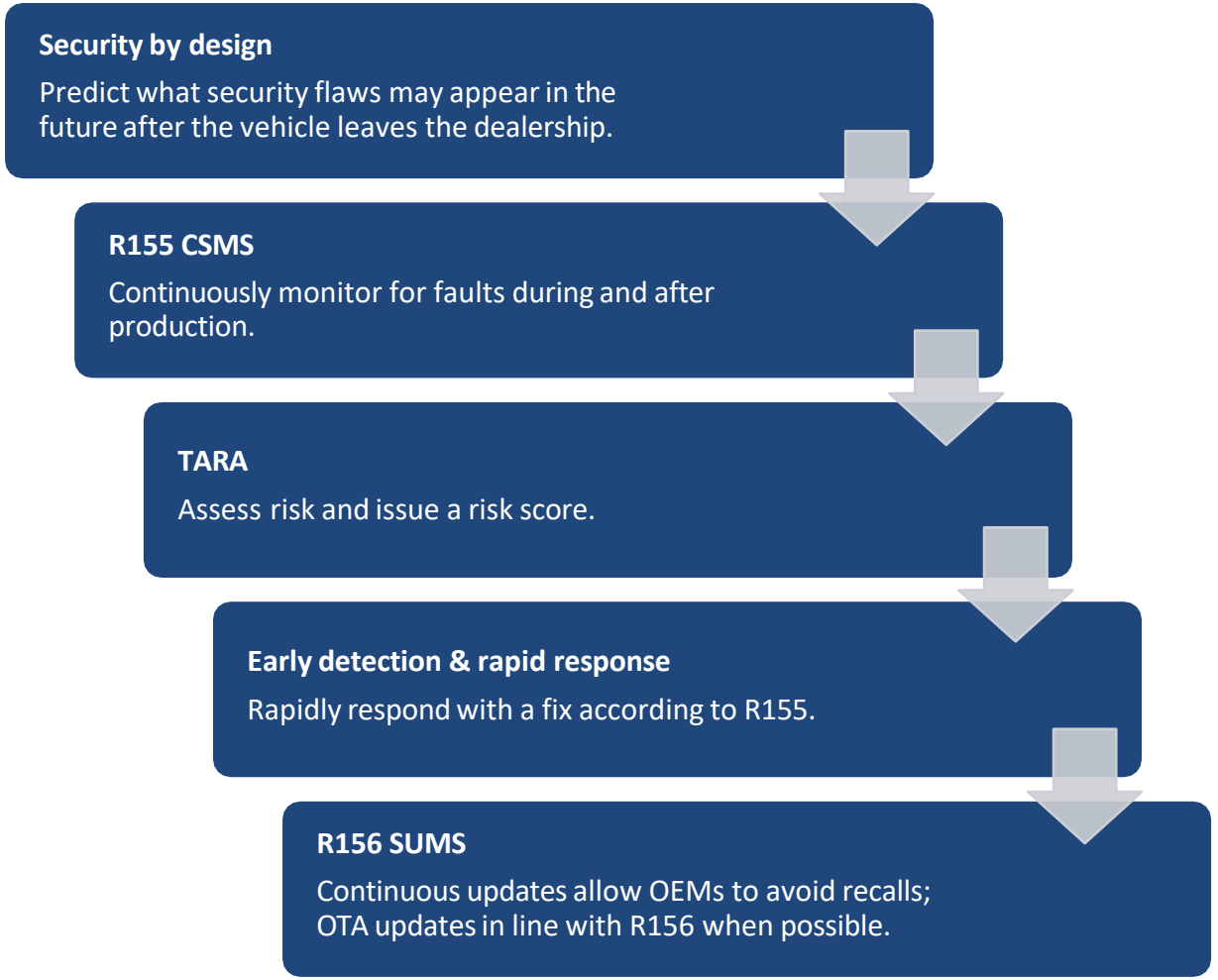
Standard ISO/SAE 21434 as a methodology for cyber risk assessment

In August 2021 the **ISO/SAE 21434 "Road Vehicles Cyber Security Engineering"** standard was published. This standard is aimed at vehicle manufacturers and defines a framework for the implementation of cyber security requirements in the development of vehicles. It provides concrete guidance for the fulfillment of the certification for the UN Regulation R155. A key differentiator between UNECE WP.29 R155 / R156 Regulation and **ISO/SAE 21434** is that ISO/SAE provides a comprehensive methodology on how OEMs and tier suppliers **calculate the risk of weak points**. The standard provides a structured cyber security framework that establishes cyber security as an integral part of engineering across the entire life cycle.

"The activities in product development, in accordance with the standard, are controlled on the basis of a risk assessment. This requires measures for organizational anchoring. Although processes are required, the norm only describes the task of a process and leaves the design of the process to the companies. Specific technologies or solutions are not proposed." (…) (Wikipedia 2023)

"The standard ISO/DIS 24089 "Road Vehicles – Software Update Engineering" is currently in development. (…) The ISO 24089 is intended to support the implementation of the regulatory requirements under the UNECE Regulation UN R156. This standard also provides for an explicit consideration of cybersecurity risks in the entire update process." (BSI (2022), p. 23)

Fig. 7: ISO/SAE 21434, R155 and R156 in Practice



Source: CAM based on Upstream (2022), p. 17

Integrated perspective important in the development process

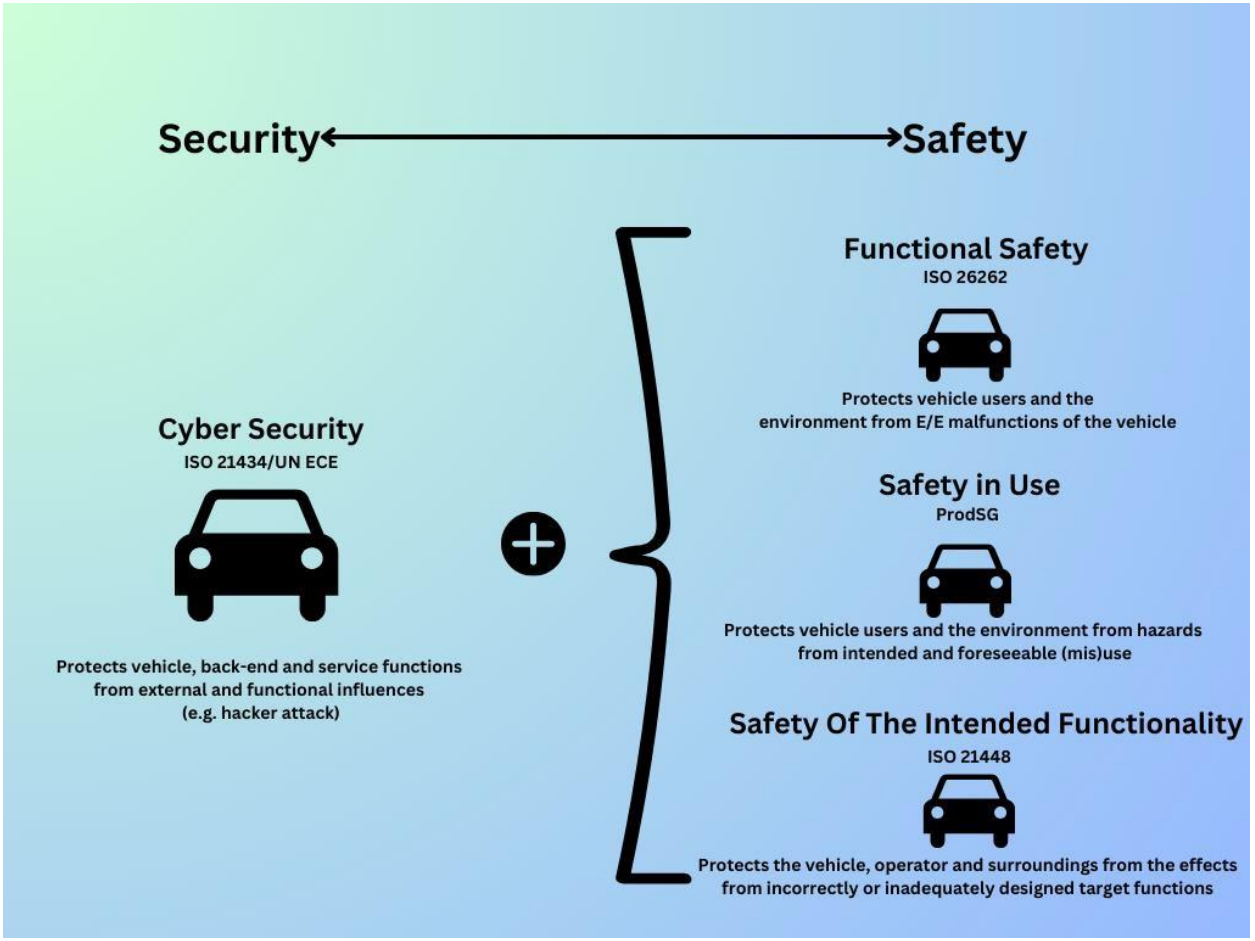
The development processes for cyber security (Security) in accordance with ISO 21434 and functional safety (Safety) in accordance with ISO 26262 (and ideally for safety in use and SOTIF according to ISO 21448) must be closely interlinked to effectively achieve the common goal of a safe E/E-system and overall product. It is therefore important to take an **integrated approach *in the development process*** to achieve a safe E/E-system and overall product.

- **SECURITY** (Cyber Security ISO 21434/UNECE): Protects vehicle, backend and service functions from external and functional influences (e.g. hacker attacks)

  +

- **SAFETY (Functional Safety** ISO 26262): Protects vehicle users and the environment from E/E-malfunctions of the vehicle
- **Safety in use** (ProdSG): Protects vehicle users and the environment from hazards arising from intended and foreseeable misuse
- **Safety Of The Intended Functionality** (**SOTIF)** (ISO 21448 (CD)): Protects the vehicle, operator, and the environment from the effects of incorrectly or inadequately designed target functions

Fig. 8: Relevance of the Perspective in the Development Process



Source: CAM based on P3 (2022), p. 27

ISO/SAE 21434: Threat analysis and risk assessment

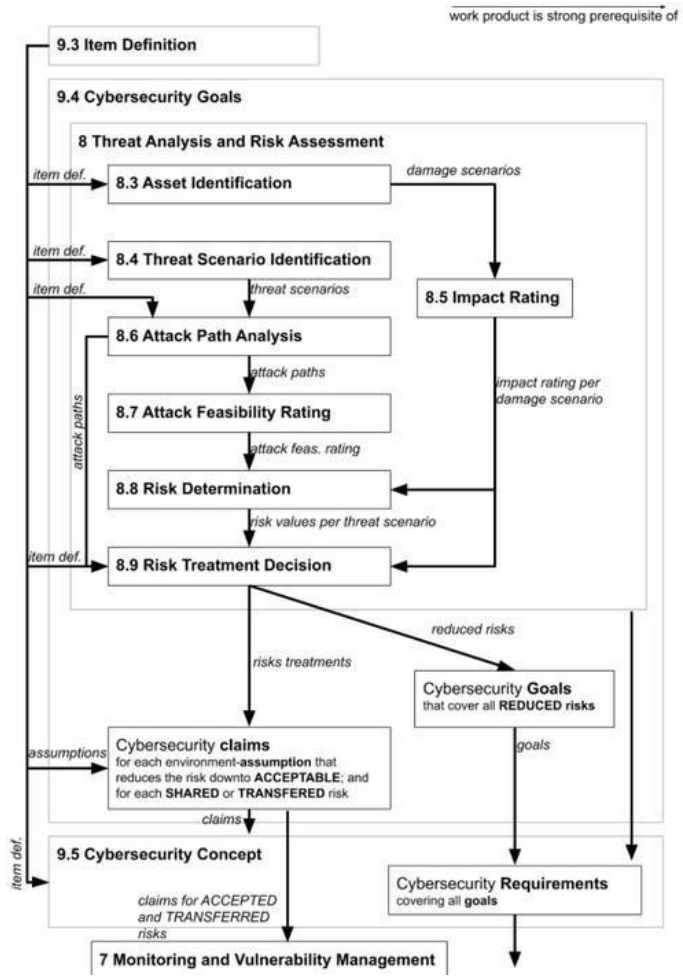
The technical risk assessment concerns the **severity of the potential impact** and the **probability of occurrence**, with a distinction being made between Hazard and Risk Analysis (HARA) and the Threat And Risk Analysis (TARA).

A central point of ISO/SAE 21434 ("Road Vehicles Cyber Security Engineering") is accordingly **threat analysis and risk assessment**. ISO 21434 distinguishes three types of product phases: Concept phase, development phase and operational phase. The main part of identifying cyber security targets is invoking the TARA (Threat And Risk Analysis) (Chapter 8).

The main steps in conducting a ISO/SAE 21434-compliant threat analysis and risk assessment are (in the order of an idealized linear execution) (cf. itemis SECURE (2023)):

- Item definition (Section 9.3)
- Asset identification (Section 8.3)
- Identification of threat scenarios (Section 8.4)
- Damage assessment (Section 8.5)
- Attack path analysis (Section 8.6)
- Assessing the feasibility of an attack (Section 8.7)
- Risk determination (Section 8.8)
- Risk treatment decision (Section 8.9)
- Cyber security objectives [RQ-09-07]
- Cybersecurity claims [RQ-09-08]
- Cybersecurity concept (Section 9.5)

Fig. 9: Threat analysis ISO/SAE 21434



Source: itemis SECURE (2023)

Risks and points of attack in the product life cycle of the automotive industry

Automotive cyber security essentially covers the product life cycle of the vehicle from development and production through to vehicle use.

The different phases of the product life cycle harbor different points of attack and risks:

1. Development
High importance and CS risks due to broad attack options and many vulnerabilities, including in the supplier network

2. Production
Medium importance and CS risks

3. Vehicle use
Very high importance and CS risks

Fig. 10: Risks in the product life cycle of the automotive industry

Development

High importance/risks +++

- Development enables access to hardware and software of a vehicle (wide attack options; potentially high number of affected vehicles/high extent of damage)
- Vehicle development favors vulnerabilities (e.g. encryption, errors in the code, software from third-party providers)
- Good security of development areas at OEMs / broad testing/iteration processes
- Risk of targeted information gathering on vehicle attack points for later attacks
- Central security of corporate networks

Production

Medium importance/risks ++

- Physical access to vehicles and/or their control devices by unauthorized persons (targeted manipulation)
- Unintentional errors: e.g. attacks via open vehicle interfaces in production (OBD software, importing of malware)
- Installation of manipulated components/control devices
- Regulation/standards for software is intended to ensure that only homologated software is installed (see UNECE R-156)

Vehicle use

Very high importance/risks ++++

- Duration of Software updates for CS vehicle fleets has still not been clarified
- Identifying vulnerabilities, e.g. using public sources, e.g. the CVE database of the National Institute of Standards and Technology
- Establishing organizations/structures for vehicle monitoring
- Attacks via the numerous communication interfaces (cellular, Wi-Fi, etc.) and applications (V2X)
- Typical points of attack:
  - Backend server
  - Vehicle communication Interfaces
  - SW update procedure
  - External connectivity
  - Vehicle data/code
  - Lack of system security
  - Unintentional human action
- Due to the variant diversity and software updates in the life cycle, the number of vehicle configurations in the field increases exponentially and makes CS more difficult

Source: CAM based on P3 (2022), p. 14-18

2. State-of-Practice – Cyber security in the automotive industry

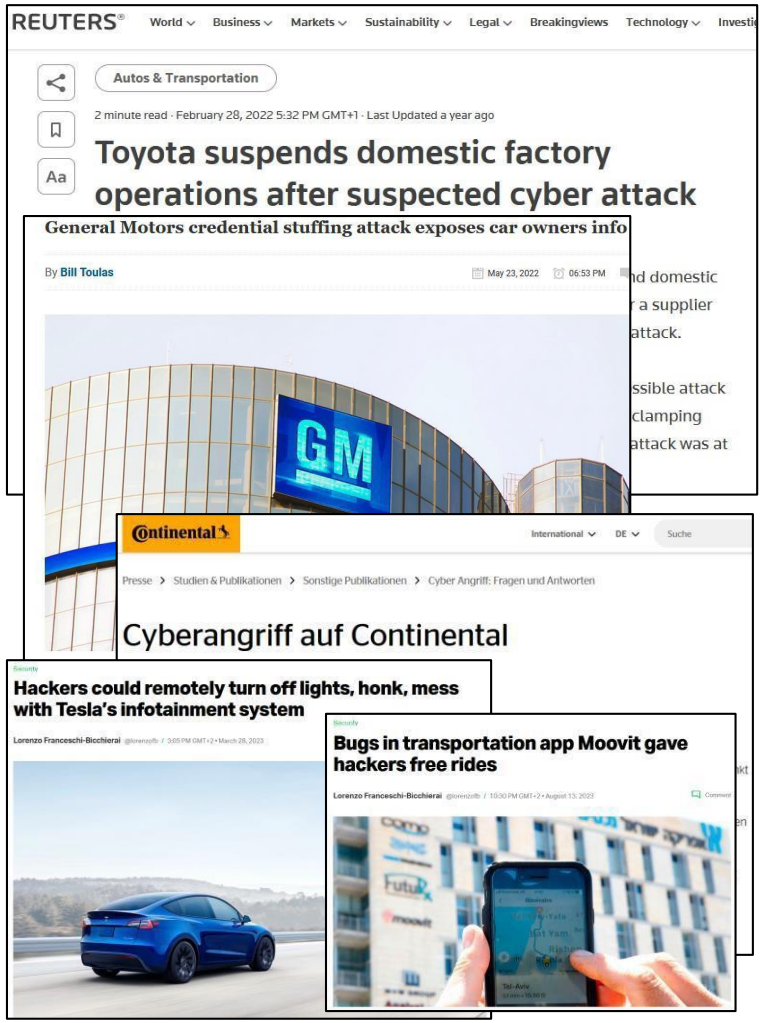
1. Standards and regulation for the connected vehicle ecosystem
2. Empirical surveys on CS incidents and attacks in the automotive industry

Cyberattacks on the automotive industry: Examples internationally (1)

- Using a **meta-analysis,** studies regarding cyberattacks on vehicles and companies in the automotive industry are evaluated below. Examples of current cyberattacks on automobile companies demonstrate the **urgency and importance** of the topic. At the same time, the evaluations also reveal the **previous points of attack** on the cyber security of the automotive industry internationally.
- Conclusions on cyber attack trends in the automotive-industry and the challenges derive from the meta-analysis.
- Current examples on the automotive industry from 2022/2023 show that the entire industry is affected:

  - After a supplier of plastic parts and electronic components was hit by a suspected cyber attack, **Toyota** was forced briefly to suspend operations at its Japanese factories in February 2022 and was unable to build around 13,000 cars as planned.
  - The US manufacturer **General Motors** announced that it had been a victim of a cyber attack in April 2022 in which some customer data was exposed, and hackers were able to redeem reward points for gift cards.
  - Automobile supplier **Continental** was also targeted by cyber criminals in the summer of 2022. The investigation into the incident showed that the attackers were also able to steal a subset of data from affected IT systems despite established security precautions.
  - In March 2023, a cyber attack on **Tesla** was reported, in which hackers were able to remotely dial into a vehicle and perform various functions. These included operating the horn, opening the trunk, switching on the low beam and manipulating the infotainment system.
  - In August 2023, software vulnerabilities in the multi-modal mobility app **Moovit (Intel)** meant that security researchers were able to access numerous registration data (including e-mail, credit card) from various user accounts and exploit them for free rides.

Fig. 11: Current Examples of Cyber Attacks (2022/23)

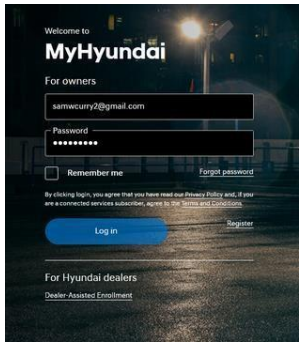


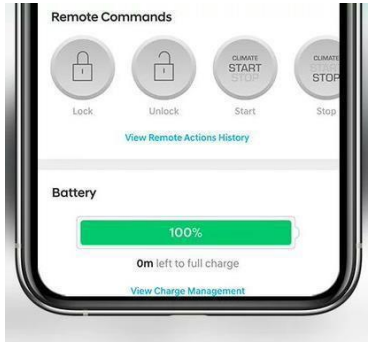
Cyberattacks on the automotive industry: Examples internationally (2)

Hackers use vulnerabilities to gain access to **vehicles, customer data** and **backend infrastructure** of automobile manufacturers. A group of "benign hackers" led by the security researcher, Sam Curry, sought out vulnerabilities in the APIs of telematics ECUs of vehicles of various manufacturers and discovered the following, among others:

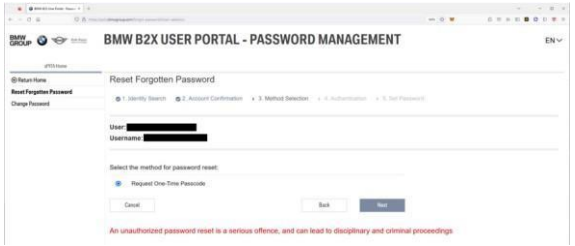
- **Kia, Honda, Infiniti, Nissan, Acura:**
  - Fully remote locking, unlocking, engine start, engine stop, precision locating, headlight flash and horn of vehicles using only the VIN number
  - Fully remote take over of accounts and disclosure of personal data via the VIN number (name, telephone number, e-mail address, address)
  - Ability to exclude users from the remote control of their vehicle and change owner.
- **Mercedes-Benz:**
  - Access to hundreds of business-critical internal applications via improperly configured SSO, including...
    - Multiple Github instances behind SSO
    - Company-wide internal chat tool, option to join virtually any channel
    - SonarQube, Jenkins, various build servers
    - Internal cloud provisioning services for the management of AWS instances
    - Internal vehicle-related APIs
    - Remote Code Execution on multiple systems
    - Storage leaks, leading to disclosure of employees'/customers' personal data, access to accounts
- **More automobile manufacturers with vulnerabilities:**

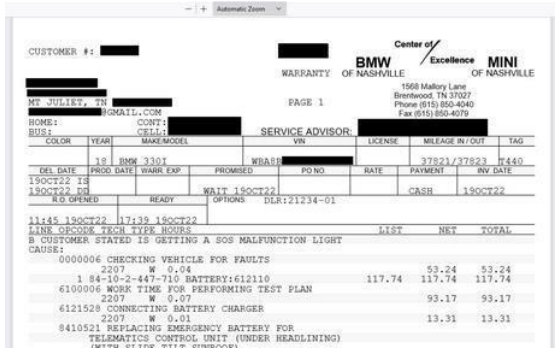
HYUNDAI GENESIS





"If we could do this, it would be full account and **full vehicle takeover** for all remotely enabled Hyundai (and, later we learned Genesis) vehicles. (...) After putting everything together, we reported the issue to Hyundai and worked with them to confirm the fix.





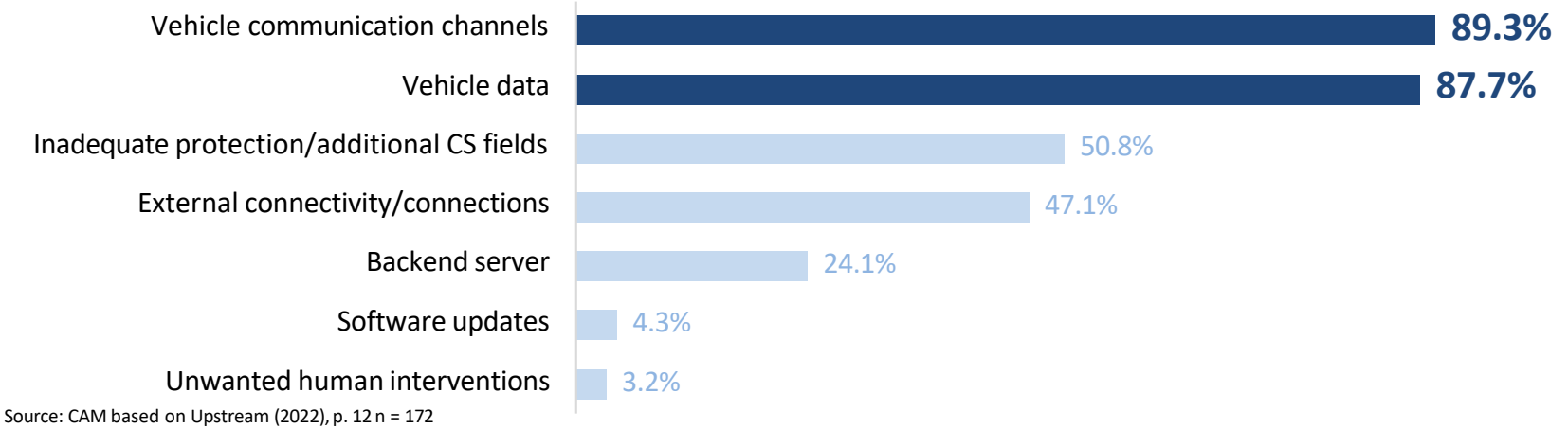
"With our level of access, there was a huge amount of functionality we could've performed against BMW and Rolls Royce **customer accounts and customer vehicles**. We stopped testing at this point and reported the vulnerability. The vulnerabilities reported to BMW and Rolls Royce have since been fixed."

Source: CAM based on Curry (2022)

Cyberattacks on the automotive industry: critical threat areas

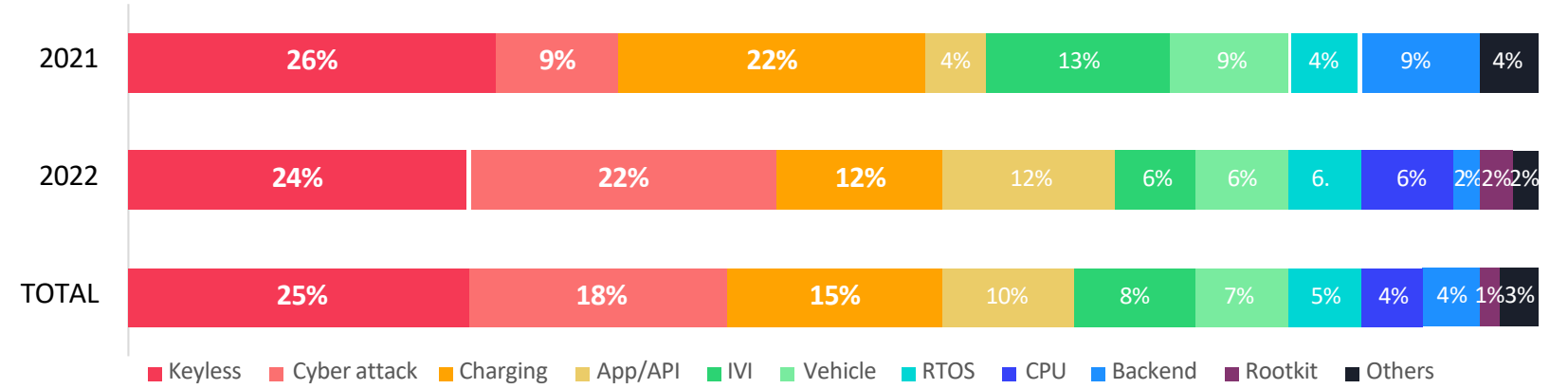
- Upstream's research team analyzed publicly reported automotive cyber incidents that occurred in 2020 and 2021 and classified them into the seven threat categories according to Appendix 5 of UNECE-R155. Some incidents fall into more than one threat category. According to the report, **communication channels (89.3%)** and **vehicle data (87.7%)** are most frequently affected by cyber attacks.
- Cyber attacks are also receiving increased attention in the media. According to a study by VicOne, which analyzed media reports on security issues in the automotive industry between the beginning of 2021 and June 2022, the importance of **cyber attacks** more than doubled from 9% to 22%. Although **keyless systems** (25%) and **charging stations** (15%) are also receiving increased attention. Subsequent investigations identify **three particularly critical areas**:
  - **Charging stations for electric vehicles**
  - **Cloud APIs**
  - **Keyless entry systems**

Fig. 12: Frequency of Cyber Incidents According to the Categories of WP.29 R155 (2020-2021)



Source: CAM based on Upstream (2022), p. 12 n = 172

Fig. 13: Frequency of Safety Topics in Automotive News by Category (2021-2022)



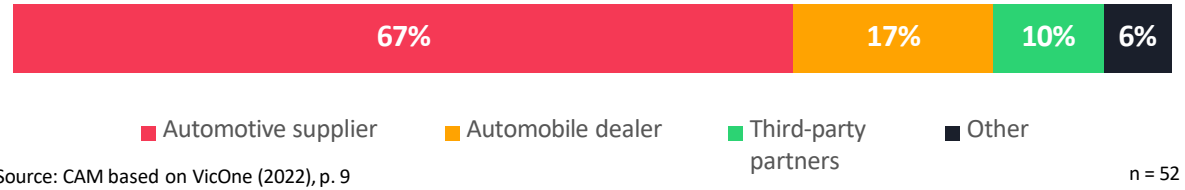
Source: CAM based on VicOne (2022), p. 3

n = n/a

Cyberattacks on the automotive industry: supply chain/suppliers as a point of attack

- Cyber attacks in the automotive industry are not exclusively limited to large, established manufacturers, but are increasingly affecting supplier companies, automobile dealers and other players along the value chain. An analysis of 52 significant security incidents between January and June 2022 revealed that **automotive suppliers are at the center of** around two thirds (**67%**) **of cyber attacks.**
- The EU study by Enisa (2021), which analyzed cross-industry (not automotive-specific) attacks on supply chains, evaluated 24 attacks in Europe from January 2020 to the beginning of July 2021 and came to the following conclusions:
  - 50% of the attacks were attributed to Advanced Persistent Threats (APT) groups known to the security community.
  - 42% of the analyzed attacks could not be assigned to a specific group.
  - 62% of attacks on customers took advantage of their **trust in their suppliers**.
  - In 62% of cases, **malware** was used **as an attack technique.** When looking at the targeted assets, the attackers in 66% of the incidents focused on the code of the suppliers in order to compromise targeted customers.
  - Around 58% of supply chain attacks were aimed at **accessing data,** (predominantly customer data, including personal data and intellectual property) and around 16% were aimed at accessing individuals.

Fig. 14: Frequency of Cyber Incidents in the Value Chain (Jan-Jun 2022)



Source: CAM based on VicOne (2022), p. 9

n = 52

Fig. 15: Classification of Attacks on the Supply Chain

Suppliers		Customers	
Attack techniques to disrupt the supply chain	Supplier assets as target of attack on the supply chain	Attack techniques to compromise customers	Customer assets as target of attack on the supply chain
• Malware Infection • Social engineering • Brute force attack • Exploitation of software vulnerabilities • Open Source Intelligence (OSINT)	• Existing software • Software libraries • Code • Configurations • Data • Processes • Hardware • People	• Trusting relationship [T1199] • Drive-by compromise [T1189] • Phishing [T1566] • Malware infection • Physical attack or modification • Falsification	• Data • Personal data • Intellectual property • Software • Processes • Bandwidth • Finances

Quelle: CAM according to Enisa (2021), S. 7

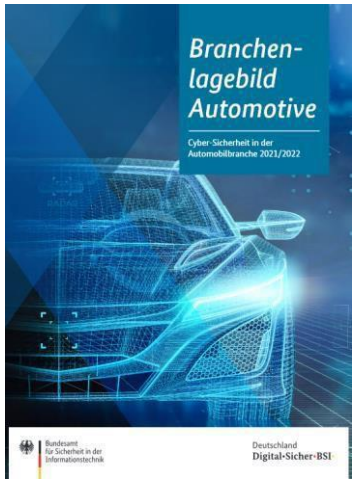
Cyberattacks on the automotive industry: BSI studies 2022/23

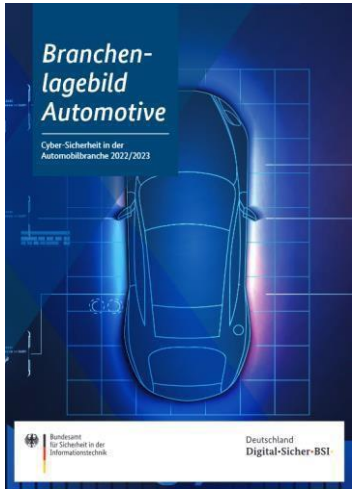
The German Federal Office for Security and Information Technology (BSI) also investigated the cyber attacks on the automotive industry in studies, on the one hand in the reporting period July 2021 to June 2022 and July 2022 to June 2023. As a result, the BSI continues to view **ransomware (attacks)** and **data leaks** as the greatest operational threats to cybersecurity, particularly for the IT systems of automobile manufacturers and their suppliers. The following deficits have been noted:

- In the case of ransomware incidents in particular, **failures in prevention** often come to light. Poorly maintained systems, missing, outdated or unverified software backups, weak administrator passwords, missing network segmentation etc., have a high and immediate potential for damage.
- **Employee behavior** also plays a key role. Some attacks now appear so deceptively real by using legitimate names and e-mails that they are difficult to detect. Raising employee awareness would help here.

The BSI also emphasizes other core areas of cyber security:

- **Supply chain**: Threat primarily from pro-Russian hacktivism attacks. There were some incidents in the reporting period that led to production downtime or disruptions to suppliers and IT service providers. A defense and technology company, which mainly supplies customers from the automotive sector, was the victim of two cyberattacks. Once again Ransomware was used.
- **IT security problems in vehicles or road traffic infrastructure:** The locking systems of vehicles (which are operated via radio keys) have inadequate rolling codes: Simple rolling codes are inadequate for effective protection. The locking systems (and immobilizers) must be secured with additional cryptographic mechanisms.
- **Cybersecurity for electric charging:** Attacks are expected to increase significantly with the growth phase of e-mobility.
  Attack surfaces are seen during the charging process in the authentication phase, billing or through insecure updates (cf. p. 25 ff.).
- **Transport infrastructure:** Facilities such as networked transport systems can wirelessly send status information in the surrounding area. These are particularly vulnerable because the systems, some of which were installed many years ago, were often installed without cybersecurity considerations.
- **Cyber security in production systems and processes:** With increasing networking and automation of production, the attack surface increases, as these systems can also be connected to the company network and service provider networks. The BSI emphasizes the establishment of comprehensive vulnerability management as well as the cyber security-oriented protection of service providers and remote services





2. State-of-Practice – Cyber security in the automotive industry

1. Standards and regulation for the connected vehicle ecosystem
2. Empirical surveys on CS incidents and attacks in the automotive industry
3. **Case study/Deep dive: Cyber security during charging and the charging infrastructure**

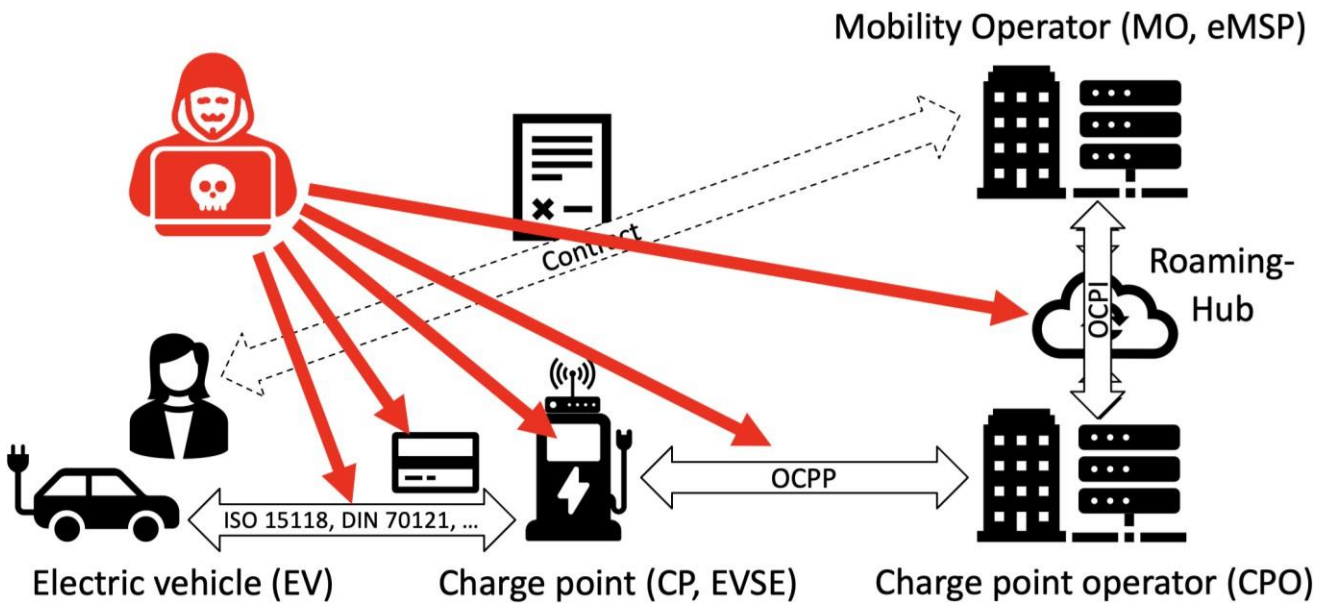
Case Study/Deep Dive: Cyber security during charging and the charging infrastructure*

In various studies (see above) it has already become clear that the charging infrastructure for electric vehicles is one of the most vulnerable cybersecurity areas. The charging infrastructure is being developed parallel to the spread of electric vehicles under high pressure in order to ensure a wide distribution of charging stations. The implementation of cyber security is often given secondary priority or not treated at all. At the same time, the charging infrastructure is not a homogeneous system, but consists of parts that are operated by different players and their service providers, which must interoperate in order to enable charging processes and to be able to bill correctly (see graphic). These factors have made the charging infrastructure an easy target for attacks, which are not yet rampant due to the ability to control the potential for any damage. Attack scenarios for different parts of the charging infrastructure are shown below, and the respective impact is described.

- The charging infrastructure is not a homogeneous system, but consists of parts that are operated by different players and their service providers, which must interoperate in order to enable charging processes and to be billed correctly

  - The charging ecosystem with various market participants is complex and basically offers many points of attack:
    - Electric vehicle: network interface
    - EVCP: ISO 15118
    - Charging card
    - Charging station
    - CP-CPO: OCPP connection
    - CPO-MSP: OCPI connection

Fig. 16: Possible Attacks on the E-Mobility Ecosystem



Source: CAM/rt-solutions.de

* This 'deep dive' on the topic of "charging/charging infrastructure" was created in collaboration with Ralf Schumann and Georg Lukas from rt-solutions.

Deep dive: CS on charging/charging infrastructure

A distinction can be made between attack scenarios

1. for the **charging process**,
2. the **charging stations**,
3. the **charging network backend systems** and
4. for **hub providers for roaming.**

5. Attacks on the charging process

There are basically two aspects of the charging process that present an attack surface: The authorization (and thus payment) of the charging process and the communication between the vehicle and the charging station. The most common form of authorization is the contactless charging card from the vehicle owner's mobility provider (e.g. from the vehicle manufacturer or from a large electricity network operator). In contrast to contactless payment cards, it does not have any protective measures for securing the payment. Only the card's Unique ID (UID) is used and then transmitted in plain text between all participants in the ecosystem. It has been known since 2003 that these UIDs can be trivially copied (Westhues 2003) and was also demonstrated as far back as 2017 for e-charging cards (Dalheimer, Schwarzladen: Ladekarten manipulieren leicht gemacht (Scam Charging: Charging Card Manipulation Made Easy)). If you obtain someone else's foreign UID, you can clone it with a smartphone onto a blank card, or even simulate it directly with a smartphone, and carry out charging processes at the victim's expense until the fraud is detected in the next billing. This system was not supposed to be used in this way.

Charging processes via the app of the mobility provider or via billing with a payment method at the charging station do not have this problem, however they are inconvenient. Further, the mandatory introduction of payment terminals in new charging stations has been postponed until July 2024 (Charging Station Regulation Section 8 (4).)

The new Plug&Charge system based on the ISO 15118 standard promises to eliminate the need to register at the charging station securely by fitting the vehicle with a cryptographic certificate from the mobility provider and encrypting all connections. The system is highly complex (and therefore prone to errors and vulnerabilities), as there is a multi-level public key infrastructure (PKI) for each role and the provisioning of vehicles is permitted via various routes (Klapwijk & Driessen-Mutters, 2018). Furthermore, it is not available in most existing vehicles. As the system becomes more widespread, public documentation of various vulnerabilities is also expected.

The ISO 15118 standard also outlines the data connection between vehicle and charging station in direct current (DC) fast charging. This data connection is based on HomePlug AV, a method for data transmission via power lines, about which several attacks have already been documented that can be used to decrypt the connection and introduce false data (Dudek, 2019), in order to block a connection (Baker, Köhler, Strohmeier, & Martinovic, 2023) or hook into a third-party Plug&Charge session (Conti, Donadel, Poovendran, & Turrin, 2022). With special equipment, you could interrupt someone else's charging process, use the charging station at someone else's expense or, in the worst case, damage a nearby vehicle by introducing incorrect information about voltage and current intensity.

Charging costs of up to approx. 60 EUR can be obtained per process, but require the presence of one's own vehicle at the charging station during the entire attack. A large-scale attack on vehicles or the power grid is, however, therefore impractical, and many models have overvoltage protective fuses to prevent physical damage.

Deep dive: CS on charging/charging infrastructure

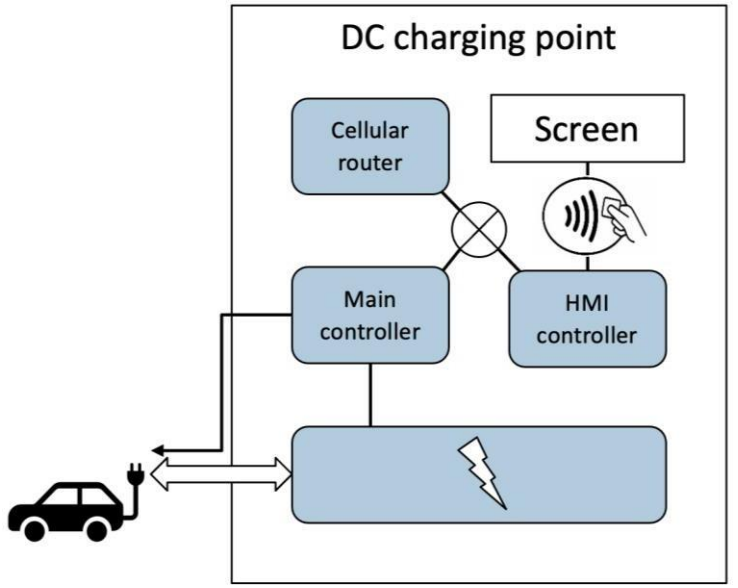
2. Attacks on charging stations

A charging station is tasked with identifying the users and authorizing the charging process, measuring the transmitted energy, and, in the case of DC charging stations also controlling the power during the charging process according to the requirements of the vehicle. For authorization and billing, a data connection with a server of the charging network operator is required, via which occupancy of the charging station and other live data are transmitted, and remote maintenance is enabled via a web interface. This connection is in most cases executed via cellular radio, and the access via a private APN (Access Point Name) which simulates a private cellular radio data network for the operator in which only the charging stations and the backend servers are located.
AC charging stations (alternating current) have less complex requirements and often come with a single controller that carries out all tasks.

DC charging stations are far more complex and have much larger enclosures with a full-size display, and often have three different controllers – one for the charging controller, a HMI (Human-Machine Interface) controller for the screen, and a dedicated cellular modem. Here, standard components from the production area with embedded Linux are often used, which enable rapid market entry thanks to rapid prototyping. A standard Ethernet network is used for the internal connection of the controllers. The enormous market pressure is even leading to some charging stations in some places being delivered with an open back door due to a lack of quality assurance (Johnson, 2023).

During product development, it is often assumed that both the internal network within the charging station and the connection to the backend server are reliable, i.e. that no attacks are to be expected from there. In practice, all that is needed are readily available tools and a few attempts to unlock a poorly guarded charging station without force, and to gain access to the internal systems. This gives access to the internal communication and for the most part poorly secured maintenance interfaces, via which customer UIDs can be read or manipulated firmware can be installed (Dalheimer, Schwarzladen III: Mit USB zum Profit, 2017 (Scam Charging III: With USB to Profit)). This type of manipulation is difficult to detect and can be used as a permanent "bug" to read additional customer data, to paralyze the controller of the charging station (with a time delay), or to attack the backend network and other charging stations. The same type of attack can also be carried out using the SIM card installed in the charging station, which accesses the APN network of the charging network operator.

Fig. 17: Typical Structure of a Charging Station



Source: CAM/rt-solutions

Deep dive: CS on charging/charging infrastructure

3. Attacks on charging network backend systems

While the backend servers are often not directly accessible from the internet, or have appropriate hardening, an attack through a charging station is not expected. In the summer of 2022 while a charging station security analysis was being conducted, the author managed to introduce, through a trivial attack, executable code into the operator's backend system, making it also possible to gain control over the backend system and all charging stations connected to it. The vulnerability was reported immediately to the developers but has still not been completely eliminated one year on.

In the worst-case scenario, the entire charging network of an operator or of a network can be sabotaged in one fell swoop in such a way that a total replacement of the controllers would be necessary, similar to the attack on the KA-Sat system in 2022 (Ermert, 2022).

And often it is not even necessary to exploit weak points because the charging stations are operated by a few integrators with the (publicly documented) standard passwords of the manufacturer in order to facilitate troubleshooting.

3. Hub attacks

The rapidly growing number of charging network operators (Charge Point Operators, CPO) and mobility providers (Mobility Operators, MO) has made it necessary to establish central structures for brokering charging processes, so that not every operator needs a direct contractual and communication relationship with every other operator. Roaming hubs take on this task by forwarding charging requests to all participating partners so that the appropriate mobility operator can authorize the charging process. At the end of the charging process, a Charge Detail Record (CDR) is created with information about the charging station used, the charging time, the costs incurred, and the contract number is transmitted via the hub.

In Europe, there are only a few hub providers. If you join a hub as a fake mobility operator, you could track all charging requests in real time with the location of the respective charging station and the UID of the customer card that are sent via the hub and create approximate movement profiles of electric vehicles. The hub operator also receives the following communication between CPO and MO, and the contract number of the respective user, so that payment transactions from different charging stations from the same provider and the assigned contract number can be traced. This makes e-mobility hubs particularly attractive targets for foreign state players.

Deep dive: Charging/Charging infrastructure

Cybersecurity Report 2022 by VicOne (2022)

VicOne names in its report three central points of attack in the area of **charging infrastructure** (2022, p. 13):

"1. CAN bus-based communication protocol between an EV and a charging station
CAN bus-based protocols are often used on EV and charging station communications, and always transfer data by plain text. This gives hackers opportunities to hijack the sessions to deploy MitM attacks. They could also transfer malicious code to the EV or charging station.

2. App/Cloud services for EV charging stations
EV charging stations are usually connected to the cloud for transactions and billing procedures. Some EVs even have apps to give users a more convenient experience. In the context of cybersecurity, this is a traditional attack surface. An attacker could gain privileges to gather user information from mobile devices or penetrate the cloud server.

3. Radio communications
Radio communications, RFID, Bluetooth, and customized radio signals are frequently used on EV charging systems. These could become remote attack surfaces that attackers use to access the EV components. For example, hackers could remotely open the charging port or transfer malicious code to the EV or charging station to gain control."

Source: VicOne 2022, p. 13 (https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf)

Disruption of fast charging processes at CCS (2022)

As electromobility ramps up, vulnerabilities are also increasingly being identified. As part of a research project (9), a vulnerability was discovered in the Combined Charging System (CCS), a widely used charging standard for battery electric vehicles. The attack aims to interrupt the charging process of one or more electric vehicles. This is an attack on the communication technology power line communication (PLC) used in the CCS. The CCS standard is applied in charging systems for a variety of transportation systems (trucks, buses, ferries, airplanes, etc.) and, in the future, will also be used in network applications. The vulnerability is only relevant with regard to fast charging (DC charging). As the information exchanged relates to safety and control, the charging process is aborted in the event of a communication failure. This procedure is prescribed by the relevant standards. This is exploited in the attack, and the control communication between the electric vehicle and charger is disrupted by radio signals to the extent that the connection between charging station and the charging electric vehicle is lost. For a complete packet loss of PLC communication, according to authors a transmission power of 10 mW, at a distance of 10 meters (in a laboratory environment) in a laboratory environment to overcome, at higher transmission powers, up to 47 meters can be achieved. The effects of an attack fortunately remain manageable, as neither the vehicle nor charger are permanently damaged. The scenario described could, however, restrict local charging availability at publicly accessible fast charging stations.
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.pdf

S. Köhler, R. Baker, M. Strohmeier, I. Martinovic: "Brokenwire: Wireless Disruption of CCS Electric Vehicle Charging", arXiv preprint, February 2022, https://arxiv.org/abs/2202.02104

Deep dive: CS on charging/charging infrastructure

Summary

- While local attacks on charging processes only cause a small amount of damage whereby you can charge at someone else's expense or disrupt someone else's charging process to be first in line, attackers who penetrate into the interior of a charging station can easily gain access to payment data of many different users and can also use the charging station as a springboard for attacks on the network operator's backend network. These networks are often insufficiently hardened, meaning that the attackers can take control of backend servers and other charging stations undetected, or in the worst case, impact the load regulation of the regional power grid.
- If the hub infrastructure that mediates between charging network operators and mobility providers is attacked, vehicle movement profiles can be created based on the brokered charging processes, and link with the personal data of the respective contract holder.
- In order to prevent charging stations, backend services and the hub infrastructure from being compromised, all operators must implement the technical and organizational measures familiar in IT operations and required for KRITIS providers in order to harden the systems, and to be able to detect, intercept and analyze ongoing attacks.

Table 2: Overview of the Attack Scenarios

Goal	Attack	Damage Potential	Countermeasures
Charging process	**UID cloning**	Charging at third-party expense	Regular checking of statements
Charging process	**ISO15118-Attacks**	Aborting a charging process, charging at third-party expense, possible vehicle sabotage	Subsequent backup of the logs not realistic; Protection of vehicles by way of fuses
Charging station	**Physical access to data**	Charging at the expense of diverse users	Intrusion detection, protection and encryption of the internal data interfaces, pen testing of the charging stations, hardening by integrators
Charging station	**Firmware manipulation**	Charging station sabotage, attacks on the backend, “free” charging processes	
Backend	**Privilege escalation**	Taking over the remote maintenance of all charging stations in the network, installing self-destruction firmware	Securing and encrypting communication with charging stations, pretesting of interfaces and servers
Hub	**Fake MO**	Access to partial motion profiles	Cannot be avoided in the medium term, long-term: New development of data protection-compliant protocols for hub communication
Hub	**Data tapping**	Access to extensive movement profiles	End-to-end encryption of communication, hardening and pretesting of the servers, long-term development of data protection-compliant protocols for hub communication

Source: CAM/rt-solutions

2. State-of-practice – Cyber security in the automotive industry

1. Standards and regulation for the connected vehicle ecosystem
2. Empirical surveys on CS incidents and attacks in the automotive industry
3. Case study/Deep dive: Cyber security during charging and the charging infrastructure
4. **Summarized theses and conclusions**

State-of-practice of cyber security: Summarized theses and conclusions (1)

- The following **relevant challenges** arise with cyber security in the automotive industry:
  - High **competitive and time-to-market pressure** due to customer demands for connected vehicles /connected services, where **cyber security aspects** may be pushed **into the background.** CS incidents may then lead to major reputational damage.
  - Automotive cyber security principally covers the entire **product life cycle of the vehicle** from development, and production to vehicle use. The long product life cycle and the large **number of variants** make it significantly more difficult to ensure cyber security. The different phases of the product life cycle harbor **different points of attack and risks**.
  - In the past, cyber security activities have been primarily limited to protecting vulnerabilities at the time of vehicle production. In the future, manufacturers and their suppliers will have to establish structures that are geared towards continuous protection of the entire product life cycle from the start of product development. The **distributed responsibility in the complex value chain** in the large supplier and partner network increases the vulnerability to cyber attacks.
- The regulatory requirements for cyber security in motor vehicles (according to the UNECE Regulation UN R155 (15) / Regulation (EU) 2018/858)) have been mandatory since July 2022 for manufacturers to implement for all new vehicle types. From **July 2024,** all **new or existing vehicle types** will also be subject to UN R155 cybersecurity type approval. The implementation of the various standards poses a major challenge for the industry.
- **A meta-analysis** of the cyberattacks on vehicles and companies in the automotive industry reveals the **urgency and growing importance** of the topic. At the same time, the evaluations also reveal the **previous points of attack** on cybersecurity in the automotive industry internationally. The results can be summarized as follows:
  - The **quantity and quality of attacks have increased** significantly in in recent years: The automotive industry in general and supplier companies in particular are increasingly becoming more frequently affected by cyber incidents.
  - "**Ransomware attacks"** are currently considered the greatest operational threat to cybersecurity, particularly for the IT systems of automobile manufacturers and their suppliers. **Failures in prevention** as well as in the **employee behavior** play a key role in this.

State-of-practice of cyber security: Summary and Conclusions (2)

- The **supply chain and the complex supplier landscape** are considered major weak points and represent central points of attack with a high probability of occurrence and a high level of damage. Cyber security is still at a low level for many suppliers and service providers. With increasing networking and automation, the attack surface is also increasing, as these systems can also be connected to the corporate network and service provider networks.
- According to various studies, the **charging infrastructure for electric vehicles** is one of the most vulnerable cyber security areas. Parallel to the spread of electric vehicles, there is enormous pressure to implement the charging infrastructure. The charging infrastructure is not a homogeneous system, but consists of parts that are operated by different players and their service providers, and which must interoperate in order to enable charging processes and to be able to bill them correctly. The charging ecosystem with various market participants is therefore very complex and offers many points of attack. Attack scenarios arise for the **charging process**, the **charging stations**, the **charging network backend systems** and for **hub providers for roaming.**
- Transparent reporting by automotive companies on cyber attacks is still significantly underdeveloped. In principle, transparent reporting on cyber attacks and their management would increase **awareness in the industry** about the dangers and risks and could motivate other companies to implement programs and measures for most comprehensive cyber security protection possible protection. In the context of the study, transparent communication about cyber attacks is also an **indicator of a professional cyber security culture** in companies. The report recognizes that cyberattacks are part of everyday business life and they must be controlled by a high quality cyber security management system.

3. Evaluation of the quality of cyber security in automotive companies

3.1 Heuristic model for evaluating cyber security performance

Heuristic model for evaluating “cyber security performance” in the automotive industry

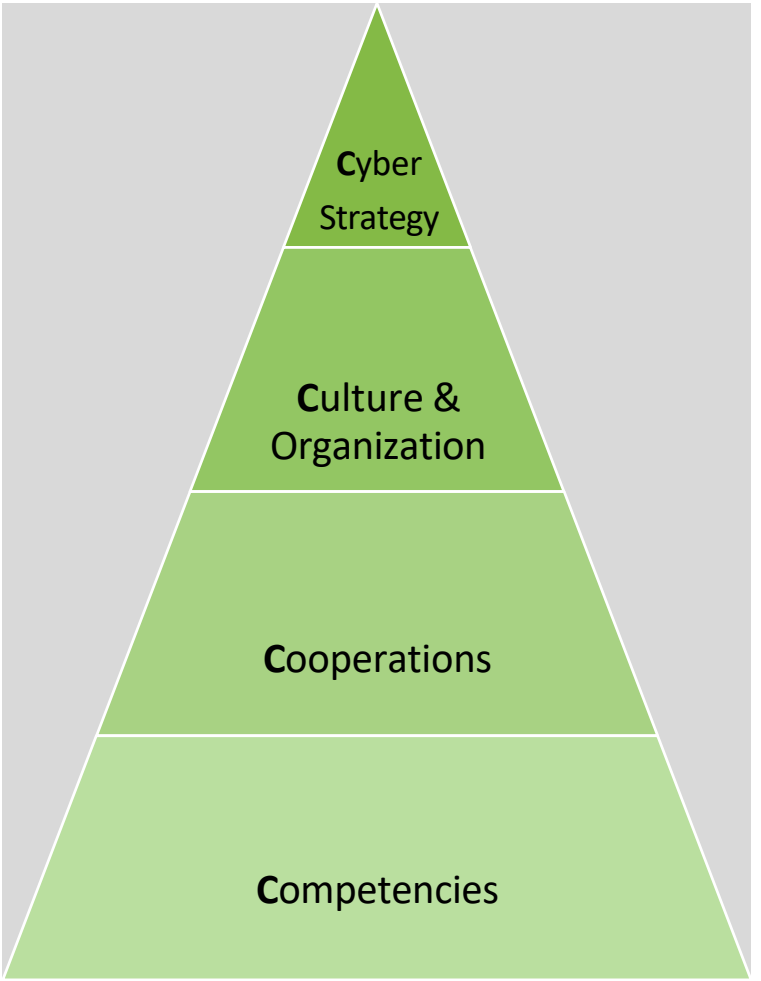
The cyber security of companies in the automotive industry is becoming increasingly important as a result of the networking of the core product vehicle and the digitalization of companies and the entire value chain. However, the companies differ significantly in terms of the quality of the conception and implementation of cyber security. A high level of cyber security performance in the company not only increases the resilience to the increasing number of cyberattacks and enables rapid detection and appropriate response to such incidents. It also enables companies to make better use of the opportunities of digitalization and networking in their own products and in the value creation stages of development and production.

Based on expert interviews (cf. Annex) and an analysis of secondary sources a heuristic **model** was developed **to empirically assess the cyber security performance** of automotive companies. It is assumed that a high quality of cyber security in the company requires broad **skills** that are not limited to individual departments (e.g IT department) and must go beyond legal requirements (compliance). Here, cyber security knowledge needs to be anchored in the entire **organization** as well as with associated **cooperation partners** in the value chain. Accordingly, cyber security must also be reflected in the **culture** of the company in order to have a lasting positive influence on the behavior of employees with regard to cyber security. The cultural set of values is reflected in a corresponding **cyber strategy**, i.e. in the goals of corporate policy and in leadership.

Against this background, the “4C” model combines relevant performance criteria of Cyber Security in four dimensions: **C**ompetencies, **C**ooperations, **C**ulture & Organization as well as the **C**yber Strategy.

The individual dimensions and performance criteria are presented below and made empirically fruitful.

Fig. 18: Heuristic Model for Empirical Evaluation of Cyber Security Performance in the Automotive Industry



Source: CAM

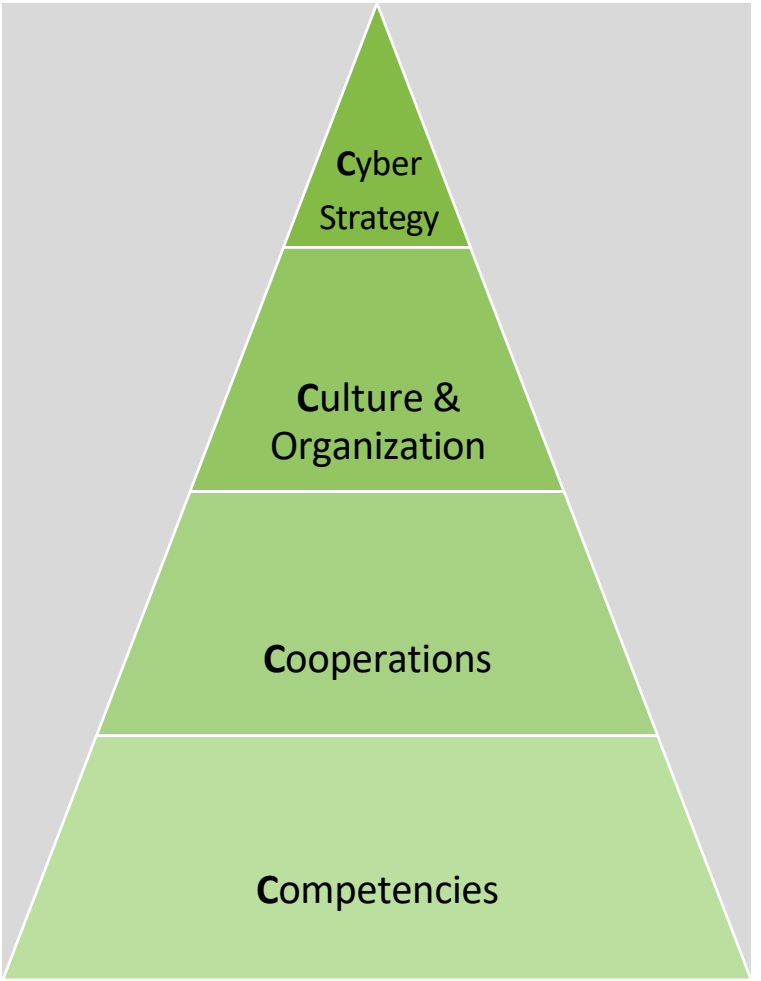
"4C"model: *Competencies, Cooperations, Culture & Organization, Cyber Strategy*

The four dimensions **C**ompetencies, **C**ooperations, **C**ulture & Organization and **C**yber Strategy of the "4C" model for measuring the cyber security performance are defined as follows :

- **C**ompetencies: Cyber security competencies are defined as the know-how within the company or the knowledge, skills and abilities of the company and its employees in relation to cyber security.
- **C**ooperations: Cooperations include the cyber security quality of the cooperation partners/supplier network or the entire value chain.
- **C**ulture & Organization: The cyber culture encompasses a company's **set of values** regarding cyber security. Corresponding characteristics influence the recognition of cyber security problems by employees as well as the openness of communication and the introduction of improvements. It is closely linked to the role model function for cyber security of the company's management. The cyberculture also manifests itself in the corresponding **quality of the cyber security organization and processes,** in which responsibilities and duties are known and all business units are involved in cyber-initiatives. It is also about the quantity/quality of resources and equipment of the workforce in all business areas in order to ward off cyber attacks and implement security measures.
- **C**yber Strategy: The strategic dimension revolves around the existence and quality of high-level cyber security action programs and guidelines in the company. This also includes the degree to which cyber security is integrated into risk management, the processes for detecting and responding to attacks, the quality of reporting to the management board and independent cyber security risk assessments (e.g. review of cyber security by "friendly hackers").

Criteria for measuring the various dimensions of the "4C" model are mapped out below to operationalize the cyber security measurement concept.

Fig. 18: Heuristic Model for Empirical Evaluation of Cyber Security Performance in the Automotive Industry



Source: CAM

3. Assessment of the quality of cyber security in automotive companies

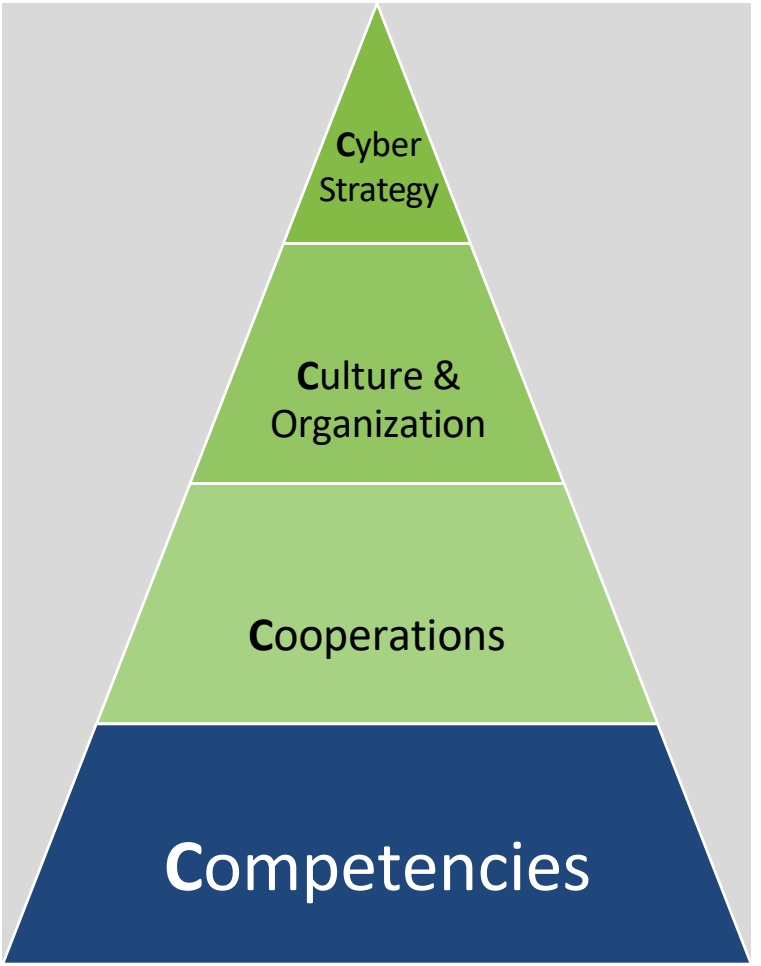
1. Heuristic model of evaluation of cyber security performance
2. **Criteria and indicators for measurement**

“4C” model: Criteria for “measuring” the quality of CS competencies

To empirically determine the **performance quality** of cyber security in automobile companies, operationalizable **criteria and indicators** on the basis of the “4C” model for the individual evaluation of modules are presented in the form of a systematized questionnaire.

Evaluation criteria	*Example questions/indicators*
Competence and weak point analysis	Is there a specific report on the status of the CS competencies in the team, including deficits as well as a plan to address the deficits? Are the key threats known at board level and the programs to deal with attacks? How do employees generally perform in awareness training?
Cyber awareness	Is the workforce fully sensitized to the topic of cyber security? Is there good employee retention in key positions in the cyber security sector? How high is the level of participation in phishing e-mails? To what extent are incidents reported by employees?
Training/Education	How often are training courses and workshops on current and future norms and safety standards offered on a mandatory basis? Are these also offered across departments?

Fig. 19: Heuristic “4C” Evaluation Model

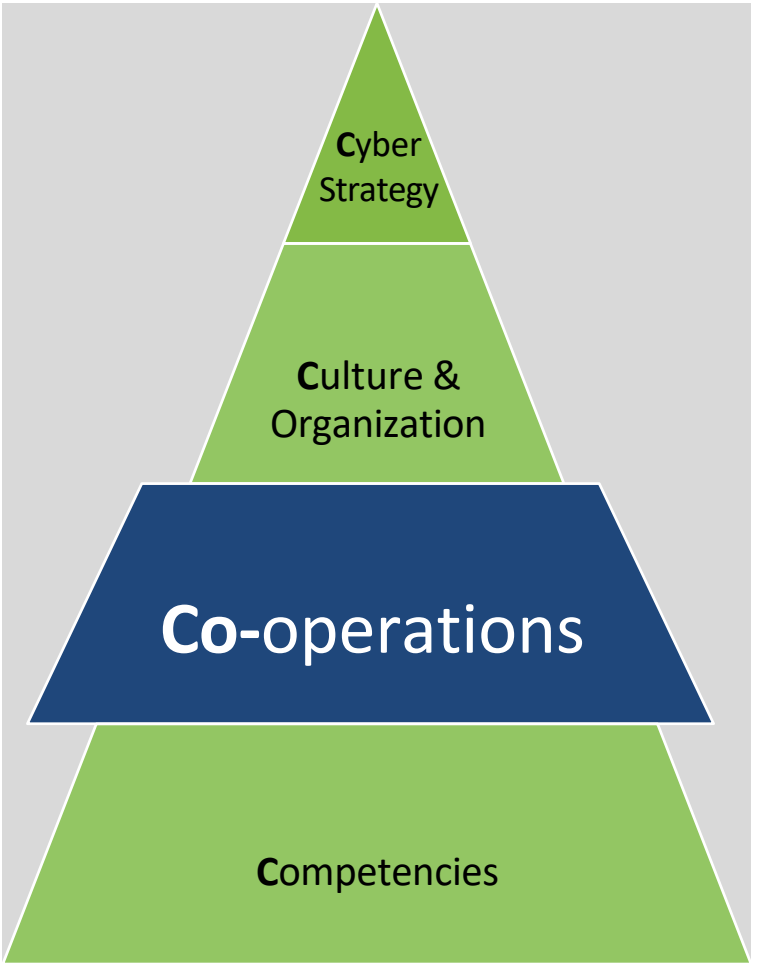


Source: CAM

“4C” model: Criteria for “measuring” the quality of CS cooperations

Evaluation criteria	*Example questions/indicators*
Supplier performance	Is supplier performance regularly measured against defined metrics (e.g. percentage of suppliers/subcontractors evaluated when they were last evaluated)? Is this accessible to members of the board ?
Involvement of the suppliers	Is the supplier/value network integrated into the company's threat assessment? Are there regular exercises on how to deal with CS incidents in the supplier/value creation network ?
Tracking CS threats in the supply chain	Are CS incidents that may not impact your own company regularly monitored and analyzed? Does the board receive continuous reporting of the greatest CS threats in the supplier/value network?

Fig. 19: Heuristic “4C” Evaluation Model

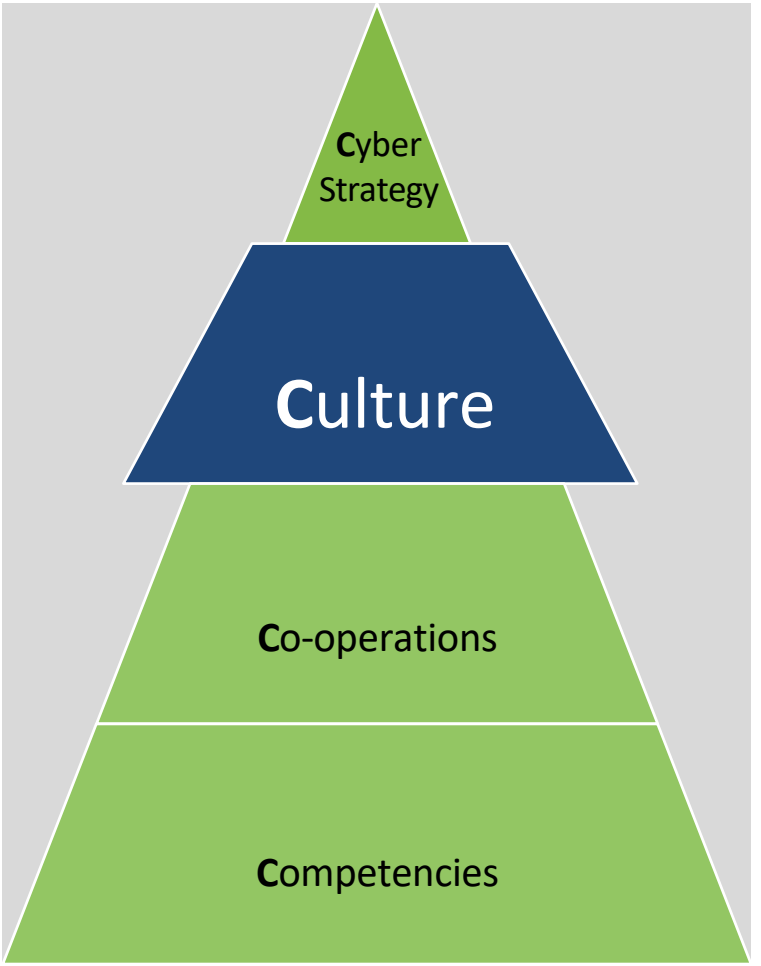


Source: CAM

"4C" model: Criteria for "measuring" the quality of the CS culture

Evaluation criteria	*Example questions/indicators*
Leadership	Would management know what to do if a (possible) attack were to occur? Does the board speak openly and positively to employees about the reasons why cyber security is important to the company?
Communication (internal)	Is there a collaborative approach to structuring security policies and processes? Is there a high level of transparency in communication about cyber attacks?
Reporting and learning	Are incident reports used to report causes, response patterns (incl. speed) and improvements to the CS organization? How can CS metrics be formulated with regard to successes (instead of: How many people clicked on a phishing e-mail, rather: How many have reported the phishing e-mail)
Transparency of communication (external)	After a registered attack, is there immediate external reporting? How detailed is the information about the CS attack (e.g attack points, extent of damage, etc.)? Are there documented "lessons learned" for future risk reduction (e.g what weaknesses facilitated the attack?)?

Fig. 19: Heuristic "4C" Evaluation Model

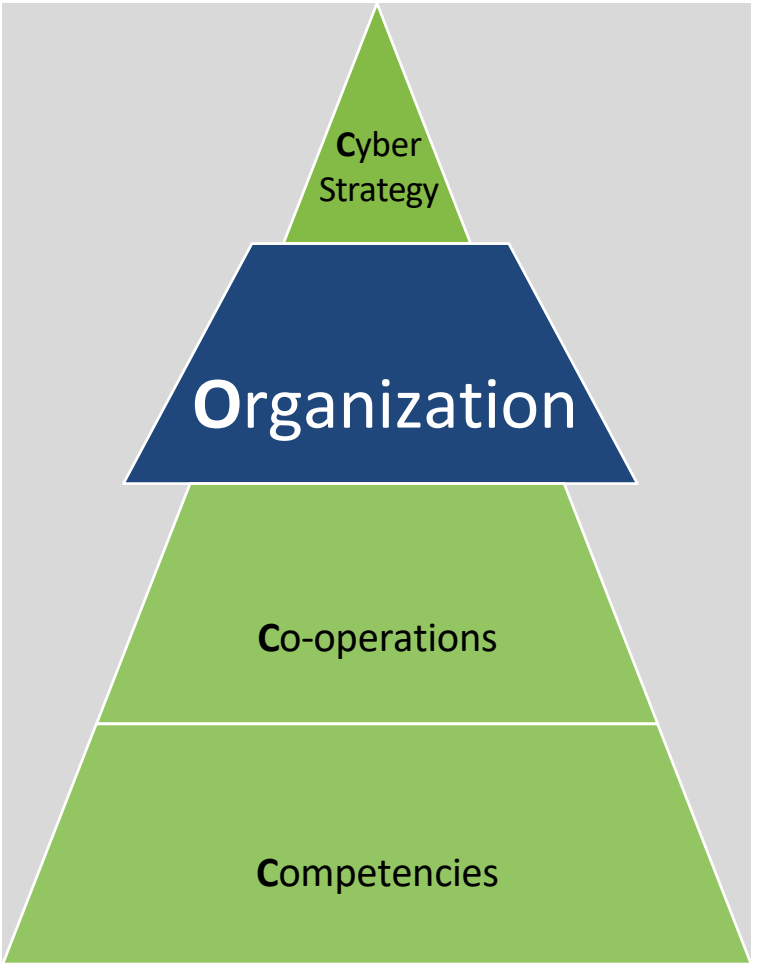


Source: CAM

“4C” model: Criteria for “measuring” the quality of the CS organization

Evaluation criteria	*Example questions/indicators*
Level of implementation and equipment	Are all applicable standards and regulations (over)fulfilled)? Is there a Cyber Security Management System (CSMS) in operation? Are the resources/equipment made available to the workforce sufficient, both in terms of quantity and quality, in order to ward off cyber attacks and implement security measures ?
Prioritization	Are all business units (HR, Legal, PR) working together on CS initiatives? Are other business areas outside of IT entrusted with the development, control and improvement of the cyber security concept?
Responsibility/ Accountability	Are there clear definitions of responsibility and accountability in cyber security reporting /communication?
Effectiveness	To what extent do Key Performance Indicator (KPI) dashboards simplify the reporting process and provide the board with clear and up-to-date information to support good decision-making?

Fig. 19: Heuristic “4C” Evaluation Model



Source: CAM

“4C” model: Criteria for “measuring” the quality of the CS strategy

Example questions/indicators
Are there comprehensive cyber security guidelines?
Are structural plans and procedures in place to detect and respond to CS incidents and recover from a CS attack ?
What is the quality of reporting of CS to the management board? (level of detail, frequency)
Is an independent cyber security risk assessment carried out regularly?
Are all board members involved in CS discussions?
Does the board have sufficient expertise to provide direction on cyber security strategy and to make accountability decisions?
What is the degree of integration of CS in the company and as part of risk management?
How is the quality of staff training measured with regard to raising awareness about CS?

Fig. 19: Heuristic “4C” Evaluation Model

Source: CAM

List of Sources

Sources

CENTER OF AUTOMOTIVE MANAGEMENT

- Baker, R., Köhler, S., Strohmeier, M., & Martinovic, I. (3. March 2023). BROKENWIRE : Wireless Disruption of CCS Electric Vehicle Charging. Retrieved on 14. September 2023 from https://arxiv.org/pdf/2202.02104.pdf
- BSI (2022): Automotive industry situation. Cybersecurity in the automotive industry 2021/2022. Accessed on July 4, 2023. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.html
- BSI (2023): Automotive industry situation. Cybersecurity in the automotive industry 2022/2023. Accessed on July 4, 2023. Online: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2022-2023.html
- Boehner, M. (2019). Security for connected vehicles along the entire life cycle. ATZelektronik, 14 (1–2), 16–21.
- Conti, M., Donadel, D., Poovendran, R., & Turrin, F. (9. September 2022). EVExchange: A Relay Attack on Electric Vehicle Charging System. Retrieved from https://labs.ece.uw.edu/nsl/papers/EVExchange_2022.pdf
- Curry, Sam (2023): Webhackers vs. Auto-Industry. Accessed on July 4, 2023. Online: https://samcurry.net/web-hackers-vs-the-auto-industry/)
- Dalheimer, M. (22. December 2017). Schwarzladen III: Mit USB zum Profit (Charging Manipulation III: With USB to Profit). Retrieved on 14. September 2023 from gonium.net: https://gonium.net/post/2017-12-22-mit-usb-zum-profit/
- Dalheimer, M. (26. October 2017). Schwarzladen: Ladekarten manipulieren leicht gemacht (Charging Manipulation: Manipulating Charge Cards Made Easy). Retrieved on 14. September 2023 from gonium.net: https://gonium.net/post/2017-10-26- schwarzladen/
- Dudek, p. (7. June 2019). V2G Injector Whispering to cars and charging units through the Power-Line. Retrieved on 14. September 2023 from https://www.sstic.org/media/SSTIC2019/SSTIC-actes/v2g_injector_playing_with_electric_cars_and_chargi/SSTIC2019-Slides-v2g_injector_playing_with_electric_cars_and_charging_stations_via_powerline-dudek.pdf
- Ecomento (2023): New VW E-Golf will start in 2028at the earliest, e-up! expires 2024. Accessed on December 19, 2023. Online: https://ecomento.de/2023/04/03/neuer-vw-e-golf-fruehestens-2028-e-Up-laeuft-2024-aus/
- ENISA (2021): ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS. Accessed on July 4, 2023. Online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
- Ermert, M. (22. March 2022). Attack on satellite network KA-Sat: Experts investigate the origin. Retrieved on 14. September 2023 from heise online: https://www.heise.de/news/Attack-auf-Satellitennetzwerk-KA-Sat-Experten-suche-nach-dem-Ursprung-6544706.html
- Humphries, M. (2022): Teenage Hacker Gains Remote Control of 25 Teslas in 13 Countries. Accessed on Nov. 14, 2022, at https://www.pcmag.com/news/teenage-hacker-gains-remote- control-of-25-teslas-in-13-countries.
- Huq, N./Gibson, C./Vosseler, R. (2020). Driving Security Into Connected Cars: Threat Model and Recommendations. (Trend Micro Research, Ed.) Accessed on July 4, 2023. Online: *http://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf*
- Huq, N./Gibson, C./Vosseler, R. (2020a). Trend Micro. “The Cybersecurity Blind Spots of Connected Cars.” Accessed on Nov. 14, 2022, at https://documents.trendmicro.com/assets/white_papers/wp-driving-security-into-connected-cars.pdf.

Sources

- Inf0sec1. (2022): Twitter - “Playing around with #FlipperZero…” Accessed on July 4, 2023. Online: https://twitter.com/inf0sec1/status/1545804925522829313?t=4-n6SQ3H8OhD_WFXwiLZMg&s=19.
- itemis SECURE 2023: Overview of ISO/SAE 21434. Accessed on July 4, 2023. Online: https://www.security-analyst.org/inside-the-iso-sae-21434/
- Jadhav, A. (2021): Automotive Cybersecurity. In: M. Kathiresh, R. Neelaveni (eds.): Automotive Embedded Systems. Springer Nature Switzerland.
- Johns, E. (2020): Cyber Security Breaches Survey 2020. Accessed on July 4, 2023. Online: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf*
- *Johnson, W.(30. January 2023). Electrify America bug opens hacking vulnerability concerns [Updated]. Retrieved from Tesla News, Tips, Rumors and Reviews: https://www.teslarati.com/electrify-america-chargers-hacking-vulnerability-bug/*
- Klapwijk, P., & Driessen-Mutters, L. (November 2018). Exploring the public key infrastructure for ISO 15118 in the EV charging ecosystem. Retrieved from https://elaad.nl/wp-content/uploads/downloads/Exploring-the-PKI-for-ISO-15118-in-the-EV-charging-ecoystem-V1.0s2.pdf
- Koenen, J. (2021): Hackers paralyze auto supplier EDAG. Accessed on July 4, 2023. Online: *https://www.handelsblatt.com/unternehmen/industrie/cyberattack-hacker-legen-autozulieferer-edag-lahm/27005604.html*
- KonBriefing*(2023):* Hacker attack 2023 in Germany current today. Hacker attacks on companies and organizations. Accessed on on July 4, 2023. Online: https://konbriefing.com/de-topics/hackerattack-deutschland.html
- Charging Station Regulation Section 8 (4). (no date). Ordinance on minimum technical requirements for the safe and interoperable construction and operation of publicly accessible charging points for electrically powered vehicles 1. Retrieved on 14. September 2023 from https://www.gesetze-im-internet.de/lsv/8.html
- McKinsey 2019 (Johannes Deichmann, Benjamin Klein, Gundbert Scherf, and Rupert Stützle): The race for cybersecurity: Protecting the connected car in the era of new regulation. McKinsey Center for Future Mobility.
- McKinsey 2020 (Ondrej Burkacky, Johannes Deichmann, Benjamin Klein, Klaus Pototzky, Gundbert Scherf): Cybersecurity in automotive. Mastering the challenge. McKinsey Center for Future Mobility (ed.). Accessed on July 4, 2023. *Online*: *https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf*
- McKinsey 2022: The future of automotive computing: Cloud and edge. October (https://www.mckinsey.com/industries/semiconductors/our-insights/the-future-of-automotive-computing-cloud-and-edge)
- Miller, C./ Valasek, C. (2015): Remote Exploitation of an Unaltered Passenger Vehicle. Accessed on July 4, 2023. Online: http://illmatics.com/Remote%20Car%20Hacking.pdf
- Nio (2022): NIO Becomes the First in China to be Granted UN R155 Cybersecurity Management System Certification, Press Release January 25. Accessed on July 4, 2023. Online: https://www.nio.com/blog/nio-becomes-first-china-be-granted-un-r155-cybersecurity-management-system-certification
- Nolte, M. (2020): OBD interface: How independent workshops are making access to vehicle data more difficult. Accessed on July 4, 2023. Online: *https://herthundbuss.com/branche-mehr/obd-schnittstelle-erschwerter-zugang-fuer-freie-werkstaetten/*

Sources

- NBC News. (June 16, 2022). YouTube. "Thieves Turning To Cutting Edge Technology To Steal Cars. Accessed on July 4, 2023. Online: https://www.youtube.com/watch?v=rx5mjOEixMY.
- NCSC (2023): Cyber-Security-Board-Toolkit. Accessed on July 4, 2023. Online: https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf
- P3 Group 2022 (Authors: Lucas Bublitz; Alexander Boll; Patrick Eisele; Tobias Löhr; Damian Weinzierl): Automotive Cybersecurity. Cluster Electromobility South-West, January 2022.
- PwC (2023): Global Automotive Cyber Security Management System (CSMS) Survey 2022. Cybersecurity puts the automotive industry under pressure. Accessed on July 4, 2023. Online: https://www.pwc.de/de/im-fokus/cyber-security/global-automotive-cyber-security-management-system-survey.html
- Tengler, S. (2020). Top 25 Auto Cybersecurity Hacks: Too Many Glass Houses To Be Throwing Stones, Forbes. Accessed on July 4, 2023. Online: https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh__=8a10f2d7f65d
- Toulas, Bill (2022): Bleeping Computers. "General Motors credential stuffing attack exposes car owners info." Accessed on July 4, 2023. Online: https://www.bleepingcomputer.com/news/security/general-motors-credential-stuffing-attack-exposes-car-owners-info/
- Red Packet Security (2022): Red Packet Security. "Cuba Ransomware Victim: Etron." Accessed on July 4, 2023.[Online: https://www.redpacketsecurity.com/cuba-ransomware-victim-etron/.
- UNECE 2021: UN Regulation No. 155. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. Agreement: 22 January 2021.
- Upstream 2022: Global Automotive Cyber Security Report, Upstream Security Limited
- VDA (2021): Automotive Cyber Security. Recommendation for Cyber Security Interface Agreement (CSIA), with reference to ISO/SAE 21434. Berlin.
- Vector (2022): Automotive Cybersecurity with ISO 21434, CSMS & SUMS, Webinar May 2022. Accessed on July 4, 2023. Online: https://www.youtube.com/watch?v=NlRw9d_NAr4
- VicOne (2022): Automotive Cybersecurity in 2022. VicOne Report accessed on July 4, 2023. Online: https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf
- Vosseler, R., Huq, N., Gibson, C. & Kropotov, V.(2021): Cybersecurity for Connected Cars. Exploring Risks in 5G, Cloud, and Other Connected Technologies. (Trend Micro Research, ed.). Accessed on July 4, 2023. Online: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected- technologies.pdf
- Westhues, J. (October 2003). Proximity Cards. Retrieved on 14 September 2023 by cq.cx - Jonathan Westhues: https://cq.cx/prox.pl
- Wikipedia 2023: ISO/SAE 21434. Accessed on December 19, 2023. Online: https://de.wikipedia.org/wiki/ISO/SAE_21434
- Wittich, Holger 2023: Porsche Macan discontinued from spring 2024. Accessed on December 19, 2023. Online: https://www.auto-motor-und-sport.de/verkehr/eu-cybersicherheit-porsche-macan-wird-eingestellt/
- Zastrow, Kai 2022: UNECE regulatory developments on Cybersecurity and OTA NECE regulatory developments on Cybersecurity and OTA.

Attachment

List of illustrations

List of tables and abbreviations

List of tables

List of abbreviations

CS	Cyber Security
CSMS	Cyber Security Management System
EU	European Union
ISO	International Organization for Standardization
KMU	Small and medium-sized companies
OTA	Over-The-Air
SAE	Society of Automotive Engineers
UN	United Nations
UNECE	United Nations Economic Commission for Europe
V2X	Vehicle-to-Everything

Imprint and Copyright

Company:
Dr. Bratzel Center of Automotive Management GmbH & Co. KG (CAM)
Director: Prof. Dr. Stefan Bratzel
Responsible for the contents: Prof. Dr. Stefan Bratzel
Authors: Prof. Dr. Stefan Bratzel

Address Block
Center of Automotive Management
An der Gohrsmühle 25
51465 Bergisch Gladbach
Germany

Phone: +49 (0) 22 02 / 2 85 77 - 0
Fax: +49 (0) 22 02 / 2 85 77 - 28
E-mail: info@auto-institut.de

Disclaimer and Copyright