Lehrstuhl für Informatik 1
Friedrich-Alexander-Universität
Erlangen-Nürnberg

PROJECT THESIS

Development of a technical cyber security concept for comfort electronics in the automotive environment in compliance with UNECE R155

Christian Körber

Erlangen, October 8, 2023

Examiner: Prof. Dr.-Ing. Felix Freiling
Advisor: Kevin Gomez

Contents

1 INTRODUCTION

This chapter provides a comprehensive overview of the topic by presenting relevant background information and the motivation for the topic. The three main research questions are defined and the outline of the thesis is presented.

1.1. Motivation

To address the increasing number of cyber security attacks in the automotive environment, the UNECE published the UNECE World Forum for Harmonization of Vehicle Regulations (WP.29) R155 regulation in January 2021, which became mandatory for Original Equipment Manufacturers (OEMs) in July 2022 [2]. Vehicles are not allowed to be sold in Europe, if they do not meet those requirements. The main aspect of R155 requires the establishment of a Cyber Security Management System (CSMS) to ensure the detection and response to possible cyber security attacks, coupled with a risk assessment and the application of mitigation measures [3]. Since vulnerabilities in the supply chain can affect the entire system, these requirements are passed down the supply chain to suppliers, who must also comply with them [2]. In addition, other standards such as ISO 21434 for cyber security must be considered [15].

1.2. Task

In this thesis, the new cyber security requirements are explored from the point of view of an automotive supplier. More specifically, it is a supplier of comfort electronics, which should answer the following questions:

- What does the supplier need to do to comply with R155?
- How does ISO 21434 relate to R155?
- Is the TARA proposed by ISO 21434 an adequate way to prove cyber security for R155?

1.3. Related Work

Since the R155 regulation is relatively new, few publications are available on this topic. On the one hand, current publications focus on general approaches to ensure cyber security in the automotive industry [5, 15].On the other hand, some focus on the comparison between R155 and ISO 21434, such as [3] and [4]. They provide a good starting point for understanding the relationship and correlation between R155 and existing standards. For example, Han et al. analyzed the test process and related requirements for alignment with R155 [10]. However, neither of the publications prioritized the point of view of a supplier and the impact of R155 on them.

1.4. Results

This work identifies the two main frameworks to be followed for cyber security in the automotive industry. TARA is the most crucial step in complying with them and is performed in this thesis on an example scenario. This results in some mitigation techniques that should be applied to a generic motor control Electronic Control Unit (ECU) and the corresponding hardware and software requirements. These include integrity and authenticity checking of received messages and secure boot, update, and access procedures. Finally, some weaknesses of the whole process are discussed. There are subjective influences in the whole process and some factors that are at least relevant in real project are neglected.

1.5. Outline

The thesis starts with an overview of the fundamentals in Chapter 2. First, the relevant standards and norms are identified and compared. Then, the performed TARA is explained in the implementation. In Chapter 3, the TARA is performed, and each step is explained in detail. The relevant results of the TARA are discussed in Chapter 4, and finally, general findings are discussed. The conclusion is drawn in Chapter 5, and possible future work is outlined.

1.6. Acknowledgments

I am highly grateful for the help of Kevin Gomez, who supervised my project and always helped me with all my concerns and questions. I could not have done this journey without Poornima Jha. She guided me through the entire project, always giving me feedback and discussing all my questions and decisions with me. Many thanks to Jan Noczensky and Florian Stützer for allowing me to work on this thesis and supporting me when I needed help. Finally, a big thank you to my girlfriend, Amira Watfa, for keeping me sane and helping me stay focused and motivated.

2 FUNDAMENTALS

2.1. Regulation and Norms

Official bodies like the European Union (EU) and independent organizations, such as the ISO, release laws, regulations, and norms to guarantee the safety, security, quality, and environmental performance of vehicles on the road [19]. The different categories do not have identical compliance requirements and can be differentiated as the following [6]:

- **Laws**: Governments are responsible for crafting laws that individuals as well as companies such as OEMs must follow to remain legal [6].
- **Regulations**: Regulations offer comprehensive instructions on implementing and enforcing laws. EU regulations must be executed in all EU countries, including the imported goods, as stated in [17, 18]. They affect only specific domains or subjects.
- **Standards**: Non-governmental bodies predominantly set standards. Product interoperability is ensured by providing reference requirements and guidelines, leading to improved safety and cost-effectiveness [16]. Standards usually provide a good baseline to start product development. Thus, the EU advocates the use of standards to advance the competitiveness of European industries [19].

2.1.1. UNECE R155

The UNECE has various working parties covering diverse subjects. For instance, WP.29 is responsible for issuing EU regulations concerning the automotive industry, thereby creating a regulatory framework. Enacting those regulations aims to enhance worldwide vehicle safety while enabling the integration of innovative vehicle technologies. As this is a broad field, WP.29 is divided into six working parties, each composed of experts in the distinct fields [8]:

- *GRBP*: Noise and Tyres
- *GRPE*: Pollution and Energy

- *GRVA*: Automated and Connected Vehicles
- *GRSG*: General Safety Provisions
- *GRSP*: Passive Safety
- *GRE*: Lighting and Light-Signaling

The GRVA prioritizes safety by regulating different vehicle aspects, including braking and steering mechanisms and technologies such as Advanced Driver Assistance Systems and Automated Driving Systems [7]. In January 2021, they issued R155 and R156 regulations regarding the safety of CSMSs and Software Update Management Systems (SUMSs) respectively [2]. CSMS will require cyber security measures throughout the vehicle life cycle, while SUMS addresses cyber security during the software update process. These regulations must be implemented for all new vehicle types from July 2022 and for all vehicles produced from July 2024 onward [4]. The regulation will only have a legal impact on OEMs, but the requirements will also be transmitted to the tier suppliers within the supply chain.

The R155 requirements can be categorized into three steps: (a) The initial aspect entails an OEM creating a CSMS, which is defined as "a systematic risk-based approach defining organizational processes, responsibilities, and governance to treat risk associated with cyber threats to vehicles and protect them from cyberattacks" [9]. The goal is to achieve cyber security throughout all stages of a vehicle's development, production, and post-production. (b) If OEMs can demonstrate their knowledge and comprehension of the risk assessment process and the implementation of cyber security measures, they are eligible to apply for the Certificate of Compliance (CoC). The CoC is awarded after an audit by an official approving authority and remains valid for up to three years but can be extended upon submission of evidence of continued compliance [3]. The CoC can then be used to assure customers and countries compliance with the R155 and may even be required for OEMs to sell their vehicles in specific markets. (c) To maintain the CoC, the OEM must submit an annual report to the approval authority that their mitigation methods are still effective and have now been expanded to cover newly emerging cyber-attacks. The supply chain is also included in this requirement as OEMs will forward the requirements to their suppliers[9]. Thus, the suppliers must prove that their components are also cyber-secure.

2.1.2. ISO 21434

The ISO also addresses cyber security in the automotive environment. In January 2016, the Society of Automotive Engineers (SAE) published the first "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", the SAE J3061 [11]. Subsequently, the ISO and the SAE started a collaboration to develop the cyber security standard ISOSAE 21434 - "Road vehicles — Cybersecurity engineering" [13, 14]. ISO 21434 provides a guideline for cyber security in electrical and electronic (E/E) systems [14]. The latter defines terminology, objectives, and requirements to promote a standard view among suppliers and OEMs [14].

The document is divided into fifteen clauses and eight annexes. While the first three clauses act as an introduction by defining the scope, normative references, and vocabulary, the latter twelve clauses define the requirements (RQ), recommendations (RC), and work products (WP) [3, 4]. Again, the entire product life cycle is covered. The main focus of this thesis will be on clause 15, which focuses on possible threats to the road user and the vehicle. The TARA carried out to identify these will be explained in detail in Section 2.2.

2.1.3. Comparison UNECE R155 and ISO 21434

As both frameworks address aspects of cyber security in the automotive environment, it is natural to analyze critical similarities and differences.

Key differences

The most apparent and significant difference is the type. ISO 21434 is an international standard and, therefore, optional, whereas the R155 is a mandatory regulation for manufacturers. Another aspect is that ISO 21434 covers the entire life cycle of a vehicle, whereas R155 additionally focuses on homologation. Furthermore, ISO 21434 has a more extensive glossary, which helps to push the recommendations more straightforward. Moreover, R155 does not define specific terms used in the document, such as "confidential" [3]. It can lead to different understandings of the required countermeasures and leaves room for interpretation by the caretakers [3]. Finally, R155 provides an explicit list of specific attacks and corresponding countermeasures, whereas ISO 21434 leaves this to the caretaker.

Key similarities

ISO 21434 and R155 have a few things in common, as they tackle the same field. Although they have different focuses, both cover the entire life cycle and try to improve the cyber security of vehicles. Rather than providing step-by-step instructions on detecting attacks and implementing countermeasures, they propose high-level solutions and focus more on what to do rather than how to do it [4]. This approach gives developers more freedom to use their solutions and algorithms but allows for more mistakes, as everyone will do as much as they think is sufficient. As a result, there are various solutions, all meeting the requirements since neither document has threshold values. A valuable condition of both is a structured level of organization to manage the cyber security steps. Compliance with ISO 21434 will force documentation of the actions taken. The documentation can then be used in the application process for the CoC of the R155. Both are strictly focused on cyber security, neglecting other relevant benchmarks in the industry, such as computation time and cost, which are usually a trade-off for a more secure environment [3].

2.2. TARA

TARA is designed to help vehicle manufacturers and their suppliers identify and mitigate cyber risks [1]. The specific objectives are defined by ISO 21434 as the following [14] :

1. Identification of assets, cyber security characteristics, and damage scenarios.
2. Identification of threat scenarios.
3. Determination of damage scenario impact ratings.
4. Identification of the attack vectors that implement the threat scenarios.
5. Determination of the ease with which the attack vectors can be exploited.
6. Determination of threat scenario risk values.
7. Selection of appropriate risk treatment options for threat scenarios.

Those goals are achieved by following a structured guideline.

3 IMPLEMENTATION

As part of this project thesis, we defined a *theoretical scenario* and conducted a TARA to analyze the effort required and identify potential issues and challenges. The resulting documentation can then be used as evidence for compliance with ISO 21434 [14] and R155 [9]. The analyzed scenario includes a generic motor control ECU. The ECU does not control the vehicle's main motor but manages small electronic motors that improve passenger comfort. Among many other examples, it controls motors that adjust the steering wheel or extract and deploy the door handle. Similar principles can thus be applied in various contexts. The following paragraphs will define the detailed tasks of the ECU.

3.1. Item Definition

ISO 21434 proposed in Section 9.3 to first perform the item definition, which involves defining the item boundary, functions, and the preliminary architecture.

Figure 3.1 displays the item boundaries and the preliminary architecture. The motor part within our control is the trust boundary motor, which includes the motor control ECU, the motor sensors, and the motor actuator itself. The motor control system is connected to the vehicle's internal bus system and, therefore, to other ECUs as well, in particular the authentication ECU, as well as to the power supply and a set of manual buttons which are within the trust boundary of the vehicle. Furthermore, the system consists of external interfaces directly linked to the motor control ECU and utilized for the tester and software update. The third one is designated for external vehicle input, such as the car key, but is connected to a separate ECU.

Afterward, a high-level description was defined for the specific tasks the ECU carried out. The Motor Control ECU implements two control systems: a door handle control system and an electronic steering wheel control system, which have the following requirements:

- The door handle control system extends the door handle when instructed by the internal bus system, specifically when the unlock button is pressed or when the key is in close proximity to the car and when sensors detect the presence of a person near the door.

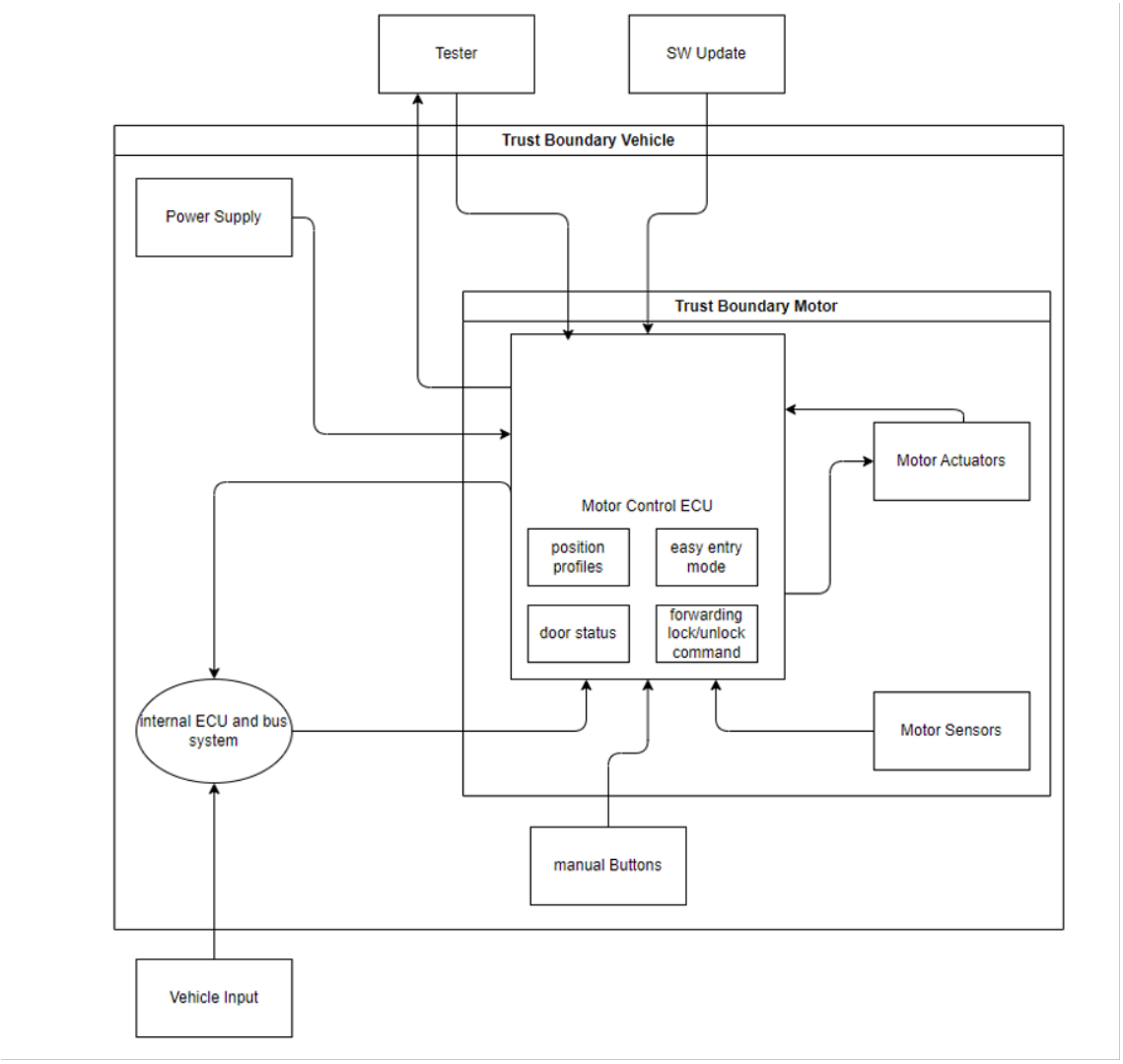

Figure 3.1.: Item boundary and preliminary architecture of generic motor control ECU

- The door handle control system automatically retracts the door handle after the door is opened and then closed again. It considers the automatic closing function when sensors detect no person near the door. It also retracts the door handle after a certain period or when the car is locked.
- The door handle control system transmits the lock/unlock command to the internal system upon button activation without processing the request or verifying whether the necessary privileges were obtained.
- The electronic steering wheel control system facilitates manual adjustments, including tilt, telescopic extension, and other parameters.
- The electronic steering control system stores various positions in its memory and automatically recalls the corresponding saved steering wheel position through a dedicated key or a menu option the driver selects.
- Additionally, the system offers an easy entry function that allows comfortable entry by moving the steering wheel as far back as possible when entering the vehicle.

From the above requirements, a table is derived that defines the items in more detail. The complete table can be found in Annex A. The motor actuator is shown here as an illustration in Table 3.1. Each function of

the motor actuator is described in detail. Moreover, every conceivable action is mapped to its corresponding requirement, including its initiation and duration. For instance, the door handle extends when receiving a door unlock command and stops after being fully extended. This process is repeated for each item and its associated functions.

Item Feature	Function	Requirement (when)	Requirement (how long)
Motor Actuators	Extend door handle	Door unlock command received	Until door handle is fully extended
Motor Actuators	Retract door handle	Door lock command received	Until door handle is fully retracted
Motor Actuators	Adjust steering wheel position	Adjustment command received	As long as the adjustment is actively being made
Motor Actuators	Move steering wheel back (easy entry)	Easy entry signal received	Until the steering wheel reaches the desired easy entry position
Motor Actuators	Send adjustment finished	When the requested adjustment is completed	Instantaneous
Motor Actuators	Send extension finished	When the extension adjustment is completed	Instantaneous
Motor Actuators	Send retraction finished	When the retraction adjustment is completed	Instantaneous

Table 3.1.: Item definition of the motor actuator

3.2. TARA

After a detailed definition of the entire functionality, the TARA process is performed in the following steps:

1. Asset Identification
2. Cyber security assurance level (CAL) Determination
3. Attack Potential based Risk Analysis
4. Risk Treatment
5. Cyber Security Goals and Requirements

The forthcoming chapters will provide a detailed explanation of the steps with the aid of an example. The complete TARA performed can be found in Annex B.

3.2.1. Asset Identification

During the asset identification phase, all assets are listed and consecutively numbered. These assets can include components, interfaces, signals, or messages. For the present example, the asset in question is the Motor Control ECU as a part of the steering wheel system environment.

ASSET ID	Assets
AS002	Motor Control ECU (steering wheel)

Table 3.2.: Asset identification motor control ECU (steering wheel)

Subsequently, the compromised function is specified, as well as a damage scenario that is a malfunction of the former caused by an external source. In addition, the cyber security properties that are violated are specified. The latter are divided into the following categories: confidentiality, integrity, availability, and authentication/authorization. In our example, the integrity of the ECU is compromised. Thus, the normal

function would be for the electronic steering wheel system to send a request for steering wheel adjustment to the motor actuator only when it receives a legitimate request from the bus system. In the case of the attack, the steering wheel starts to adjust without a proper request.

Cyber Security Properties	Function	Damage Scenario
Integrity	Electronic steering wheel system sends steering wheel adjustment request only if receiving a legitimate request from the bus system	Steering wheel starts adjusting without a request

Table 3.3.: Asset functionality and damage scenario

The damage scenario can be used to derive the impact rating for different aspects. ISO 21434 Annex F has been used as a reference [14]. The impact can be either safety, operational, personal, or financial. The severity is assessed and categorized as severe, major, moderate, or negligible. There could also be multiple impacts on different aspects of a damage scenario. In this phase, the high-attack-level threat scenario is also formulated. If the steering wheel starts to adjust automatically, several things can happen. For instance, it could lead to an accident, thus damaging the vehicle or the road user. The resulting crash can cause severe financial damage and severe safety damage. In general, if the steering wheel does not function properly, the operability of the car is majorly impaired. The threat scenario leading to this malfunction could be a replay attack on the internal bus system.

Impact Description	Category	Impact Rating	Threat Scenario
Road users' assets can get damaged	Financial	Severe	Replay attack on internal bus system
Road users can get injured	Safety	Severe	Replay attack on internal bus system
Steering wheel not properly usable	Operations	Major	Replay attack on internal bus system

Table 3.4.: Impact description and threat scenario

3.2.2. CAL Determination

CAL defines different security levels to determine a component's protection level against attacks. The CAL level ranges from one to four, with increasing severity. The CAL rating is determined by the impact rating performed in Subsection 3.2.1 and the attack vector rating. This rating depends on the attack vector. *Attack vectors* are the concrete path to execute the corresponding attack. Correlating with the required proximity of the access methods (network, adjacent, local, physical), ease of access decreases, leading to a lower attack vector rating. To execute the replay attack, the attacker must compromise another ECU on the bus system, which copies adjustment request messages and releases them at unintended times. The initial attack requires the attacker to be adjacent to the vehicle, giving it a medium attack vector rating. As the attack vector rating is medium and the impact rating is severe, CAL 4, the highest CAL rating is awarded.

Attack Vector description	Access Modality	Attack Vector Rating	CAL
Attacker compromises another ECU on the bus system and copies adjustment request messages	Adjacent	Medium	CAL4

Table 3.5.: Attack vector description and corresponding CAL determination

3.2.3. Attack Potential based Risk Analysis

In the attack potential based risk analysis, the effort required to carry out an attack is assessed based on various criteria. This information is detailed in Annex G of ISO 21434, and the caretaker must select from various options based on their knowledge and experience. Every option has a corresponding value that increases with effort and difficulty, as shown in the table below.

- Elapsed time: $\leq$ 1 day (0), $\leq$ 1 week (1), $\leq$ 1 month (4), $\leq$ 6 months (17), $>$ 6 months (19)
- Specialist expertise: layman (0), proficient (3), expert (6), multiple expert (8)
- Knowledge of Item or Component (KOIC): public (0), restricted (3), confidential (7), strictly confidential (11)
- Window of Opportunity (WoO): unlimited (0), easy (1), moderate (4), difficult (10)
- Equipment: standard (0), specialized (4), bespoke (7), multiple bespoke (9)

Select one option for each factor, add the respective values, and obtain the final score, determining the attack feasibility rating (very low, low, medium, high). Finally, combine the attack feasibility and impact ratings to determine the final risk value. The higher the feasibility and impact, the greater the risk.

When evaluating compromising another ECU to perform a replay attack, the task was non-trivial and took weeks to complete. Nevertheless, it is feasible to complete within a month. However, a basic understanding of the system is not enough, and one must have expertise in the structure and algorithms of vehicles, which is usually limited to experts. Similarly, knowledge about the targeted item is essential for successful execution. The attacker must have access to confidential information about the component to execute the attack. Since the attacker only needs to be adjacent to the vehicle, the window of opportunity is easy. Ordinary tools are insufficient in terms of equipment, but specialized equipment can still be acquired relatively easily. The cumulative values add up to 22, indicating a low attack feasibility. Due to the potential severity of this malfunction, the final risk assessment for the attack rates at three out of five.

Elapsed Time	Specialist Expertise	KOIC	WoO	Equipment	Summary	Attack Feasibility	Risk Value
4	6	7	1	4	22	low	3

Table 3.6.: Attack potential based risk analysis

3.2.4. Risk Treatment

After collecting the risk values of all possible attacks, a decision must be made on how to treat and mitigate them. The first step is determining the risk treatment based on the CAL rating and the Risk Value. Either the risk can be retained, shared, or reduced. (a) Retain means the risk is so minimal that no mitigation techniques are applied. (b) Sharing the risk has several options, including buying insurance or sharing the risk with another company. (c) Reducing the risk means applying an actual mitigation technique to close or reduce the vulnerability. Opting for risk reduction entails outlining the planned treatment method and identifying the hardware or software responsibility to implement it. Implementing countermeasures is necessary since the risk level has been evaluated as 3. The software-based implementation involves measures for the detection of malicious internal messages and activities. Upon detection, the driver should be warned, and a freeze frame should be saved to aid in subsequent investigations.

3.2.5. Cyber Security Goals and Requirements

The final phase of TARA involves establishing a cyber security goal and deriving specific cyber security system, software, and hardware requirements and recommendations. The cyber security goal of our example is to avoid the adjustment of the steering wheel at unintended times due to a replay attack on the internal

Risk Treatment Decision	Planned Treatment Method	Responsibility
Reduce risk	Implement measures to detect malicious internal messages and activities. Warn the driver about it and save a freeze frame	Software

Table 3.7.: Risk treatment decision and planned treatment method

bus system. To achieve this, the ECU must be able to detect malicious messages on the internal bus system by checking their integrity and authenticity. After detecting incorrect messages multiple times, notify the driver. The ECU must also be able to capture a freeze frame if it detects an attack. To prevent replay attacks, the master and the ECU could include a shared counter of correctly sent messages, for example.

Cyber Security Goal	Cyber Security Requirements	Recommendations
Avoid steering wheel adjustments without request due to replay attacks on the internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the integrity and authenticity. The ECU can capture a freeze frame if it detects an attack.	The master and the ECU could include a common counter to detect replay attacks

Table 3.8.: Cyber security goals, requirements and recommendations

4 EVALUATION

This chapter discusses the results of TARA, followed by an overview of encountered hurdles and findings. From the example scenario ten relevant cyber security goals and their software and hardware requirements got derived. They cover different parts and interfaces of the ECU.

4.1. TARA Results

A wide variety of attacks against the generic motor control ECU were examined in the TARA. No claims of completeness were made, but an attempt was made to consider various aspects and attack vectors. The cyber security goals, corresponding requirements, and recommendations are the most significant results of the TARA. The complete TARA is available in Annex B. Only the goals and requirements of the attacks where the risk must be reduced are shown below in Table 4.1.

As a summary of the table, the ECU should implement measures to detect malicious messages by checking their integrity and authenticity. In identifying any fraudulent activity, the driver must receive a warning, and a freeze frame capture must be taken to support further investigations. Additionally, hardware measures must be utilized to safeguard keys, certificates, and other relevant security parameters. In addition, to enhance cyber security, it is recommended to disable the JTAG interface and utilize secure boot, secure update, and secure access techniques.

4.2. General Findings

The TARA provides a structured approach to cyber security. Its well-defined steps are easy to follow, enabling the identification of relevant attacks and the implementation of countermeasures.

However, the TARA also has limitations. For instance, it lacks a defined method for identifying potential threats. Cyber security frameworks such as STRIDE or the CIA triad can support brainstorming. Annex

Cyber security Goal	Cyber Security Requirements and Recommendations
Avoid steering wheel adjustments without request due to replay attacks on the internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the integrity and authenticity. The ECU shall be able to capture a freeze frame if it detects an attack. The master and the ECU could include a typical counter to detect replay attacks
Avoid not extending the door handle even though instructed due to Denial of Service attacks on the internal bus system	The ECU shall be able to detect and report failed executions of commands. The ECU shall warn the driver if multiple attempts fail.
Avoid door handle retracting/ extending at unintended times due to replay attacks on the internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the integrity and authenticity. The ECU shall be able to capture a freeze frame if it detects an attack. The master and the ECU could include a common counter to detect replay attacks.
Avoid door handle motor deploying too fast by changing the speed parameter	The ECU shall save security-relevant parameters in not accessible memory
Avoid attacker gains access to keys and certificates	The ECU shall save security-relevant keys and certificates in secure hardware modules
Avoid software Update done by malicious attackers	The ECU shall use secure software update procedure
Avoid attacker gaining diagnostic message information	The ECU shall be able to detect malicious messages on the OBD interface by checking the integrity and authenticity.
Avoid access to Debug Interface by using remainder from development to gain higher privileges	The JTAG interface of the ECU shall be disabled.
Avoid unintended cloning of the copyrighted software	The ECU shall apply secure access control by implementing authentication and authorization.
Avoid execution of malicious software on ECU	The ECU shall implement a secure boot technique.

Table 4.1.: Cyber security goals and requirements of relevant damage scenarios

5 of R155 lists vulnerabilities, attack methods, and corresponding mitigation techniques and provides a systematic approach. However, there is no claim of completeness, and new attacks arise with time. Other attacks will be considered depending on who performs the TARA. Therefore, the entire TARA is highly dependent on the caretaker.

Another example is the attack potential-based risk analysis. The caretaker estimates the values, thus highly dependent on their knowledge and expertise. However, the rating can be normalized by asking multiple team members to provide an average score or utilizing their knowledge in specific cases. The score is the primary determinant of the final results, so the entire TARA can vary in different cases.

A TARA can be utilized to prove compliance with ISO 21434 and R155. Although TARA provides a strong foundation for cyber security, it does not provide conclusive proof of a component's security in real-world situations. Other methods like RISKEE, a Risk-tree-based method for assessing risk in cyber security proposed by [12], should be considered to enhance cyber security. Additionally, TARA overlooks critical aspects like component performance and costs, which are crucial considerations in realistic projects.

From the supplier's perspective, TARA can serve as evidence to the OEM that cyber security measures have been evaluated and that the ISO 21434 standard has been followed. Currently, TARA can also be used to demonstrate compliance with R155. Of course, the resulting hardware and software requirements must also be implemented, which often incurs additional costs and expenses during real-world projects. Thus, the outcomes of TARA are only a first step in finding and evaluating potential risks, but the final result has to be discussed with the customer and a software or hardware architect. In cases where implementing a mitigating strategy proves to be overly expensive or impairs the process considerably, alternative options such as risk-sharing or opting for a less intensive mitigation approach may be more suitable.

5 Conclusion and Future Work

Beginning in July 2022 for all new vehicle types and then for all vehicles produced from July 2024 forward, OEMs are required to comply with UNECE R155. The latter requires the implementation of cyber security measures throughout the entire process of a vehicle, including its development, and these requirements will be passed down the supply chain to suppliers.

This thesis aimed to identify steps for a supplier to comply with R155. The primary requirement for this is some form of proof that cyber security concerns have been assessed and mitigation techniques have been applied against potential threats. One recommended approach is to perform a TARA, a structured method proposed in the ISO 21434 standard for analyzing threats, assessing their risks, and identifying appropriate mitigation measures. A well-documented TARA can then serve as evidence of cyber security measures for R155.

To evaluate TARAs suitability for proving cyber security for R155, an exemplary TARA was performed on an imaginary example involving a generic electronic motor control ECU for comfort. The key preventative measures that must be taken involve identifying malicious messages, utilizing a secure hardware module to protect vital cyber security tokens, and implementing secure boot, update, and access techniques.

While TARA provides a structured approach to addressing various aspects of cyber security, it does have limitations. Its outcomes rely heavily on the individual responsible for its execution. There are numerous decisions that lack concrete benchmarks, instead relying on the expertise and knowledge of the caretaker. Thus the results of these decisions vary depending on the individual, making it, in my opinion, an inadequate method for establishing cyber security. However, it serves as a good starting point that can be extended and improved in the future.

In future work, methods to further eliminate subjective opinions can be explored. One potential solution is to provide a more structured approach for identifying possible attacks. Thus far, the R155 offers a partial list of attacks that cannot accommodate new and emerging threats. Additionally, addressing the subjectivity of attack feasibility evaluation is necessary. Finally, the examined case could be expanded. In the conclusion the hardware and software requirements for the example have been identified, and their feasibility could be evaluated.

6 List of Acronyms

CAL Cyber security assurance level

CoC Certificate of Compliance

CSMS Cyber Security Management System

ECU Electronic Control Unit

E/E electrical and electronic

EU European Union

ISO International Organization for Standardization

KOIC Knowledge of Item or Component

OEM Original Equipment Manufacturer

RC recommendations

RQ requirements

SAE Society of Automotive Engineers

SUMS Software Update Management System

TARA Threat Analysis and Risk Assessment

UNECE United Nations Economic Commission for Europe

VTA Vehicle Type Approval

WP work products

WP.29 UNECE World Forum for Harmonization of Vehicle Regulations

WoO Window of Opportunity

6 BIBLIOGRAPHY

[1] Zainab Anifowose. Aligning Mitre attack framework with threat analysis and risk assesment (TARA) to support R155 compliance, 2023.

[2] Rohit Bohara et al. Cyber security and software update management system for connected vehicles in compliance with UNECE WP.29, R155 and R156. In *Software Engineering Workshops*, pages 41–53. Gesellschaft für Informatik e.V., 2023. doi: 10.18420/se2023-ws-07.

[3] Gianpiero Costantino et al. A comparative analysis of UNECE WP.29 R155 and ISO/SAE 21434. In *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 340–347. 2022. doi: 10.1109/EuroSPW55150.2022.00041.

[4] Gianpiero Costantino et al. In-depth exploration of ISO/SAE 21434 and its correlations with existing standards. In *IEEE Communications Standards Magazine*, volume 6, pages 84–92, 2022. doi: 10.1109/MCOMSTD.0001.2100080.

[5] Masoud Ebrahimi et al. A systematic approach to automotive security. In *Formal Methods*, pages 598–609. Springer International Publishing, 2023. doi: 10.1007/978-3-031-27481-7_34.

[6] FOCUS. Standards vs. regulations, Jan 2017. URL `https://www.focusstandards.org/standards-vs-regulations-vs-laws/`. (accessed: 08.05.2023).

[7] United Nations Economic Commission for Europe. Working party on automated/autonomous and connected vehicles - introduction, . URL `https://unece.org/transport/vehicle-regulations/working-party-automatedautonomous-and-connected-vehicles-introduction`. (accessed: 08.05.2023).

[8] United Nations Economic Commission for Europe. Wp.29 - introduction, . URL `https://unece.org/wp29-introduction`. (accessed: 08.05.2023).

[9] United Nations Economic Commission for Europe. Un regulation no. 155, 2021. URL `https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security`.

[10] Yanyan Han et al. Automotive cyber security test method for UN-R 155 regulation. In *Second International Conference on Testing Technology and Automation Engineering (TTAE 2022)*, volume 12457, page 124571F. International Society for Optics and Photonics, SPIE, 2022. doi: 10.1117/12.2660280.

[11] SAE International. Cybersecurity guidebook for cyber-physical vehicle systems j3061:201601, 2016. URL https://www.sae.org/standards/content/j3061_201601/.

[12] Michael Krisper et al. RISKEE: A risk-tree based method for assessing risk in cyber security. In *Systems, Software and Services Process Improvement*, pages 45–56. Springer International Publishing, 2019. doi: 10.1007/978-3-030-28005-5_4.

[13] Georg Macher et al. ISO/SAE DIS 21434 automotive cybersecurity standard - in a nutshell. In *Computer Safety, Reliability, and Security. SAFECOMP Workshops*, pages 123–135, 09 2020. doi: 10.1007/978-3-030-55583-2_9.

[14] International Organization for Standardization SAE International. Road vehicles — cybersecurity engineeringm iso/sae 21434, 2021. URL https://www.iso.org/standard/70918.html.

[15] Christoph Schmittner et al. A preliminary view on automotive cyber security management systems. In *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1634–1639, 2020. doi: 10.23919/DATE48585.2020.9116406.

[16] European Union. European standards, . URL https://single-market-economy.ec.europa.eu/single-market/european-standards_en. (accessed: 16.05.2023).

[17] European Union. Types of eu law, . URL https://commission.europa.eu/law/law-making-process/types-eu-law_en. (accessed: 08.05.2023).

[18] European Union. Types of legislation, . URL https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en. (accessed: 08.05.2023).

[19] European Union. Standardisation policy, . URL https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-policy_en. (accessed: 08.05.2023).

A

ITEM DEFINITION

Item Feature	Function	Requirement (when)	Requirement (how long)
Tester	Retrieve debug information	When the developer connects to the debug interface and requests information	As long as the developer is connected to the interface
Software update	Perform software update	When new software versions are available and the developer connects to the device	Duration of the update process
Software update	Retrieve information about current Software (version, hash etc.)	When connected and requested	Instantaneous
Power supply	Provide continuous power	Continuous	Continuous
Motor actuators	Extend door handle	Door unlock command received	Until door handle is fully extended
Motor actuators	Retract door handle	Door lock command received	Until door handle is fully retracted
Motor actuator	Adjust steering wheel position	Adjustment command received	As long as the adjustment is actively being made
Motor actuator	Move steering wheel back (easy entry)	Easy entry signal received	Until the steering wheel reaches the desired easy entry position
Motor actuator	Send adjustment finished	When the requested adjustment is completed	Instantaneous
Motor actuator	Send extension finished	When the requested extension is completed	Instantaneous
Motor actuator	Send retraction finished	When the requested retraction is completed	Instantaneous
Motor sensors	Detect door handle position	Start of door handle movement	Continuous while door handle movement
Motor sensors	Monitor steering wheel position	Continuous monitoring	Continuous
Motor sensors	Monitor door open/closed status	Continuous monitoring	Continuous
Motor sensors	Detect persons near the door	Continuous monitoring	Continuous
Motor sensors	Detect person in the driver seat	Continuous monitoring	Continuous
Manual buttons	Send easy entry activation signal	button pressed	Instantaneous
Manual buttons	Send manual lock/unlock request	button pressed	Instantaneous
Internal ECU and bus system	Send door handle extension signal	Unlock button pressed or a car key is close to car	Instantaneous
Internal ECU and bus system	Send door handle retraction signal	Lock button pressed	Instantaneous
Internal ECU and bus system	Send adjustment request	User inputs adjustment parameters	Until adjustment is completed
Internal ECU and bus system	Transmit car key ID	Receiving car key ID from authentication ECU	Instantaneous
Internal ECU and bus system	Send chosen User	When specific user is selected in car menu	Instantaneous
Internal ECU and bus system	Sends lock signal	When receiving lock input	Instantaneous
Internal ECU and bus system	Sends unlock signal	When receiving unlock input	Instantaneous
Internal ECU and bus system	Send Key proximity status	Key presence or absence near the door detected	Continuous

Table A.1.: Item definition

Item Feature	Function	Requirement (when)	Requirement (how long)
Motor control ECU	Send door handle extension request	Receiving signal to extend from internal bus system and a person detected near the door	Until door handle is fully extended
Motor control ECU	Send door handle retraction request	Receiving signal to retract from internal bus system	Until door handle is fully retracted
Motor control ECU	Send door handle retraction request	No person detected near the door for 30s	Until door handle is fully extended
Motor control ECU	Send door handle retraction request	Door opened and then closed again	Until door handle is fully retracted
Motor control ECU	Forward the lock/unlock command	Receiving the manual lock/unlock request	Instantaneous
Motor control ECU	Send adjustment request	Receiving a car ID after unlock of the car and getting the right parameters from memory. If 0 mph	Until adjustment is finished
Motor control ECU	Send adjustment request	After receiving another selected user from the bus system. If 0 mph	Until adjustment is finished
Motor control ECU	Send easy entry request	After receiving easy entry activation signal. If 0 mph	Until adjustment is finished
Motor control ECU	Send stop easy entry mode request	After detecting a person sitting in the driver seat	Until adjustment is finished

Table A.2.: Item definition continued

B

FULL TARA

Row	Asset ID	Assets	Confidentiality	Integrity	Availability	Authentication
1	AS001	Motor control ECU (steering wheel)		Y		
2	AS001	Motor control ECU (steering wheel)				
3	AS001	Motor control ECU (steering wheel)		y		
4	AS001	Motor control ECU (steering wheel)				
5	AS001	Motor control ECU (steering wheel)				
6	AS002	Motor control ECU (door handle system)		y		
7	AS002	Motor control ECU (door handle system)		y	y	
8	AS002	Motor control ECU (door handle system)		y		
9	AS002	Motor control ECU (door handle system)				
10	AS002	Motor control ECU (door handle system)		y		
11	AS002	Motor control ECU (door handle system)		y		
12	AS002	Motor control ECU (door handle system)				y
13	AS003	Data communication to software update		y		y
14	AS004	Data communication with tester/OBD	Y			y
15	AS004	Data communication with tester/OBD	y		y	
16	AS005	Firmware of motor control ECU	y			y
17	AS005	Firmware of motor control ECU	y	y		

Table B.1.: Full Tara part 1

Row	Function	Damage Scenario
1	Electronical steering wheel system sends steering wheel adjustment request only if standing with 0mph	Unintended electronic adjustment of steering wheel while driving
2	Electronical steering wheel system sends steering wheel adjustment request only if standing with 0mph	Unintended electronic adjustment of steering wheel while driving
3	Electronical steering wheel system sends steering wheel adjustment request only if receiving a legitimate request from the bus system	Steering wheel starts adjusting without a request
4	Electronical steering wheel system sends steering wheel adjustment request only if receiving a legitimate request from the bus system	Steering wheel starts adjusting without a request
5	Electronical steering wheel system sends steering wheel adjustment request only if receiving a legitimate request from the bus system	Steering wheel starts adjusting without a request
6	Door handle control system extends the door handles after being instructed by the internal bus system	The door handle doesn't extend the door handle even though instructed
7	Door handle control system retracts the door handle after the door has been closed	The door handle doesn't retract after the door being closed
8	Door handle system only adjusts motor position if intended by user	The door handle retracts/ extends at unintended times
9	Door handle system only adjusts motor position if intended by user	The door handle retracts/ extends at unintended times
10	Door handle control system always stores the correct door handle position status	The door handle sends wrong door handle status position to other ECUs
11	Door handle control system retracts the door handle with the intended speed	The door handle motor deploys too fast
12	The ECU does protect its keys and certificates	Attacker gains access to keys and certificates
13	Software update should only be allowed by authorized entities	Software update done by malicious attacker
14	Sending diagnostic messages to OBD port only if an authorized entity is requesting data	Attacker gaining diagnostic message information
15	Debug interface is not usable	Access to debug interface by attacker
16	Copyrighted software on ECU should not be able to be downloaded	Unintended cloning of the copyrighted software
17	The ECU should only execute authorized code	Execution of malicious software on ECU

Table B.2.: Full TARA part 2

Row	Impact Description	Safety	Operations	Personal	Financial	Impact Rating
1	Road users may get injured	Y				Major
2	Road users assets may get damaged				Y	Major
3	Road users assets may get damaged				y	Severe
4	Road users may get injured	y				Severe
5	Steering wheel not properly usable		y			Major
6	Car user may not be able to enter the car		y			Major
7	Car may be less aerodynamic and use more gasoline				y	Neglibile
8	Car user may not be able to enter the car	y				Severe
9	Attacker may get unintended access to the vehicle				Y	Severe
10	Door handle functionally doesn't work, door has to be physically opened		y			Moderate
11	Damage to linkage or motor		y			Major
12	use as backdoor to infiltrate system	y				Severe
13	ECU compromised and not working the intended way	Y	Y	Y	Y	Severe
14	leak of diagnostic message infomration			y		Moderate
15	ECU compromised and not working the intended way	y	y	y	y	Severe
16	Extraction of copyright or proprietary software from ECU (product piracy)					Severe
17	Complete control over the ECU by the attacker	y	y	y	y	Severe

Table B.3.: Full TARA part 3

Row	Attack Vector Description	Physical	Local	Adjacent	Network	Attack Vector Rating	CAL
1	Attacker compromises data source by physically accessing the data source and sends wrong information	y				Very low	CAL1
2	Attacker is able to physically install a man in the middle on the CAN bus to exchange the message when the request is done	y				Very low	CAL1
3	Attacker compromises another ECU on the bus system and copies adjustment request messages			y		Medium	CAL4
4	Attacker compromises another ECU on the bus system and copies adjustment request messages			y		Medium	CAL4
5	Attacker compromises another ECU on the bus system and copies adjustment request messages			y		Medium	CAL4
6	Attacker compromises another ECU on the bus system and floods CAN with messages			y		Medium	CAL3

Table B.4.: Full TARA part 4.1

Row	Attack Vector Description	Physical	Local	Adjacent	Network	Attack Vector Rating	CAL
7	Attacker compromises another ECU on the bus system and floods it with messages			y		Medium	
8	Attacker compromises another ECU on the bus system and copies adjustment request messages			y		Medium	CAL4
9	Attacker compromises another ECU on the bus system and copies adjustment request messages			y		Medium	CAL4
10	Attacker is able to physically install a man in the middle on the CAN bus	y				Very low	CAL1
11	Attacker changes adjustment speed data by physically accessing the data source	y				Very low	CAL1
12	Physically accessing the ECU and extracting the stored data	y				Very low	CAL2
13	Attacker physically connects to the software update interface and updates the software	y				Very low	CAL2

Table B.5.: Full TARA part 4.2

Row	Attack Vector Description	Physical	Local	Adjacent	Network	Attack Vector Rating	CAL
14	Attacker physically connects to the OBD and tries to gain information by pretending to be a trustworthy source	y				Very low	CAL1
15	Physically accessing the ECU and resoldering the removed debug port	y				Very low	CAL2
16	Attacker physically accessing the ECU and connecting to the ECU	y				Very low	CAL2
17	Attacker physically accessing the ECU and injecting code	y				Very low	CAL2

Table B.6.: Full TARA part 4.3

Row	Elapsed time	Specialist Expertise	KOIC	WoO	Equipment	Summary	Attack Feasibility Rating	Risk Value
1	4	6	7	4	7	28	Very low	1
2	4	3	7	4	4	22	Low	2
3	4	6	7	1	4	22	Low	3
4	4	6	7	1	4	22	Low	3
5	4	6	7	1	4	22	Low	3
6	4	3	3	4	4	18	Medium	3
7	4	3	3	4	4	18	Medium	1
8	4	6	7	4	4	25	Very low	2
9	4	6	7	4	4	25	Very low	2
10	4	3	7	4	4	22	Low	1
11	4	6	7	4	7	28	Very low	2
12	4	6	7	4	4	25	Very low	2
13	4	6	11	4	0	25	Very low	2
14	4	6	7	4	0	21	Low	2
15	4	6	7	4	4	25	very low	2
16	4	6	7	4	7	28	Very low	2
17	4	6	7	4	7	28	Very low	2

Table B.7.: Full TARA part 5

Row	Risk Treatment Decision	Planned Treatment Method	Responsible
1	Retain risk		
2	Retain risk		
3	Reduce risk	Implement measures to detect malicious internal messages and activities	Software
4	Reduce risk	Implement measures to detect malicious internal messages and activities	Software
5	Reduce risk	Implement measures to detect malicious internal messages and activities	Software
6	Reduce risk	Employ measures to detect and recover from denial of service attacks. Warn the driver about it.	Software
7	Retain risk		
8	Reduce risk	Implement measures to detect malicious internal messages and activities. Warn the driver about it and save a freeze frame	Software
9	Reduce risk	Implement measures to detect malicious internal messages and activities. Warn the driver about it and save a freeze frame	Software
10	Retain risk		
11	Reduce risk	Implement measures to prevent changes of parameters	Hardware, software
12	Reduce risk	Use secure hardware modules to store keys and certificates	Hardware, software
13	Reduce risk	Use secure software update procedures	Software
14	Reduce risk	Verify authenticity and integrity of received messages of OBD interface	Software
15	Reduce risk	JTAG disablement	Hardware, software
16	Reduce risk	Apply access control techniques and design to protect the system code	Hardware, software
17	Reduce risk	Apply secure boot techniques	Hardware, software

Table B.8.: Full TARA part 6

Row	Cyber Security Goal	Hardware, Software Requirements
1	Avoid unintended adjustment of steering wheel while driving due to manipulation of vehicle data	
2	Avoid unintended adjustment of steering wheel while driving due to a man in the middle attack	
3	Avoid steering wheel adjustments without a request due to replay attack on internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the authenticity. Limit the number of failed commands to X times. The ECU should be able to capture a freeze frame if it detects an attack.
4	Avoid steering wheel adjustments without a request due to replay attack on internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the authenticity. Limit the number of failed commands to X times. The ECU should be able to capture a freeze frame if it detects an attack.
5	Avoid steering wheel adjustments without a request due to replay attack on internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the authenticity. Limit the number of failed commands to X times. The ECU should be able to capture a freeze frame if it detects an attack.
6	Avoid not extending the door handle even though instructed due to Denial of Service attacks on the internal bus system	The ECU shall be able to detect and report failed executions of commands. The ECU shall warn the driver if multiple attempts fail.
7	Avoid not retracting the door after the door being closed due to Denial of Service attacks on the internal bus system	
8	Avoid door handle retracting/ extending at unintended times due to replay attack on internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the integrity and authenticity. The ECU shall be able to capture a freeze frame if it detects an attack.
9	Avoid door handle retracting/ extending at unintended times due to replay attack on internal bus system	The ECU shall be able to detect malicious messages on the internal bus system by checking the integrity and authenticity. The ECU shall be able to capture a freeze frame if it detects an attack.
10	Avoid door handle sending the wrong door handle status position to other ECUs	
11	Avoid door handle motor deploying too fast by changing the speed parameter	The ECU shall save security-relevant parameters in not accessible memory
12	Avoid attacker gains access to keys and certificates	The ECU shall save security-relevant keys and certificates in secure hardware modules
13	Avoid software update done by malicious attacker	The ECU shall use secure software update procedure
14	Avoid attacker gaining diagnostic message information	The ECU shall be able to detect malicious messages on the OBD interface by checking the integrity and authenticity
15	Avoid access to Debug Interface by using remainder from development to gain higher privileges	The JTAG interface of the ECU shall be disabled
16	Avoid unintended cloning of the copyrighted software	The ECU shall apply secure access control by implementing authentication and authorization. The software shall be maintained in a secure environment during production.
17	Avoid execution of malicious software on ECU	The ECU shall implement a secure boot technique. The software should be backed up for an automatic recovery.

Table B.9.: Full TARA part 7