A Comparative Analysis of UNECE WP.29 R155 and ISO/SAE 21434

Gianpiero Costantino*, Marco De Vincenzi † and Ilaria Matteucci‡
IIT, Consiglio Nazionale delle Ricerche
Pisa, Italy
gianpiero.costantino@iit.cnr.it, †marco.devincenzi@iit.cnr.it, ‡ilaria.matteucci@iit.cnr.it

2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) | 978-1-6654-9560-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/EUROSPW55150.2022.00041

***Abstract*—In the last years, the increasing number of cyber-attacks on vehicles has shown the importance to implement security solutions within the automotive domain. To reduce the risk that a vehicle or its components get attacked and compromised, two cybersecurity references have been released: UNECE WP.29 R155 and ISO/SAE 21434. In March 2021, the United Nations Economic Commission for Europe (UNECE) published the WP.29 R155 regulation, mandatory in some countries from July 2022 to homologate vehicles' cybersecurity. Officially released in August 2021, ISO/SAE 21434 is a cybersecurity standard which aims to be widely accepted and applied in the engineering of electrical and electronic (E/E) systems for road vehicles. In this work, we describe and analyze the two norms, comparing them to show their points of contact and differences. From our analysis, the two documents, spanned both along the entire life-cycle of a vehicle, can be considered overlapped in some processes, but also complementary to increase the cybersecurity of the vehicle. Finally, we provide a use case of application of the regulation and the standard on an E/E system, reporting the possible limits and implementations.**

***Index Terms*—UNECE WP.29 R155, ISO/SAE 21434, automotive, cybersecurity, standard, regulation.**

1. Introduction

Modern vehicles resemble four-wheel smart devices connected to the Internet. Today, medium-high level cars have built-in several Advanced Driver-Assistance Systems (ADAS), and vehicles may quickly reach level 2 of autonomous driving, i.e., "hands off". Besides, in a few times, the evolution of ADAS could move vehicles to level 5 "steering wheel optional". However, this sophisticated condition of vehicles in which millions of lines of code [1] are needed to support ADAS, makes vehicles vulnerable to cyber-attacks at the same level as computers and mobile devices. Recent automotive security history has shown several examples of attacks on vehicles. The most relevant and popular is the attack on the Jeep Cherokee [2], where, in 2015, two researchers remotely controlled the car by injecting Controller Area Network (CAN) frames [3] into the in-vehicle network. In 2018, the Keen Security Lab published a set of vulnerabilities of cars that make them prone to remote access [4]. In particular, they were able to exploit such vulnerabilities to inject Unified Diagnostic Services (UDS) frames into the CAN network bypassing the central gateway. More recently, in 2021, Weinmann and Schmotzle [5] controlled mechanical parts of a Tesla car through a drone.

As seen in the current automotive scenario and due to the evolution of vehicles in the next years, the need to implement cybersecurity solutions into vehicles becomes a more and more urgent element. So far, automotive carmakers (OEMs) have used internal cybersecurity policies when developing vehicles components. To support the carmakers' development phase, the AUTOSAR consortium collects most of the strategies that regulate the automotive world and cover some security aspects of onboard communications [6]. In March 2021, the United Nations Economic Commission for Europe (UNECE) WP.29 members delivered a new regulation, the R155 [7], for cybersecurity in road vehicles. More recently, in August 2021, a new standard on automotive cybersecurity, the ISO/SAE 21434 [8], was published to assure that carmakers and component suppliers (Tiers) apply processes and solutions to assure cybersecurity during all life-cycle of an E/E system.

Aiming at improving the knowledge and the adoption of these emergent norms, in this paper, we present a review of the regulation UNECE WP.29 R155 and the standard ISO/SAE 21434 (Section 3). We discuss their similarities and differences, showing their limitations (Section 4). Besides, we provide also a possible scenario in which we apply both norms (Section 5).

2. Related Work and Contribution

Although the recent official releases, some papers about UNECE R155 and ISO/SAE 21434 have been already published. Brandt et al. [9] describe the UNECE R155 and they propose a step-by-step pragmatic and adaptive approach to achieve compliance at a sustainable cost. On the other side, Macher et al. [10] review the draft of ISO/SAE DIS 21434 dated September 2020, describing the structure of the standard and reviewing the achieved results and the open questions. Powley [11] analyzed of ISO/SAE 21434, focusing on Section 8.7. In particular, the author showed the need for an increase in robustness of the attack feasibility assessments proposed in the standard. Concerning the previous works, our study is not focused on the application methods like [9], but it is a comparison between the standard and the regulation, while [10] and [11] are focused only on the standard.

More articles and presentations come from private institutes and companies. For example, the British Standards Institution (BSI) in an insights paper [12] analyses the general framework where ISO/SAE 21434 will be adopted and suggests methods to be compliant with the standard. The company Trend Micro published in September 2021 a

DOI 10.1109/EuroSPW55150.2022.00041

research paper [13] on UNECE WP.29 R155, where they identify cybersecurity areas and study in deep the attack vectors defined in the regulation.

In Section 5, we report an application example of the regulation and the standard on a Tire Pressure Monitoring System (TPMS). Several works have described the possible vulnerabilities of a TPMS. In particular, in [14] the authors show that eavesdropping is easily possible at a distance of roughly 40m from a passing vehicle. In [15], the authors describe the possible information leakage with the corresponding privacy breach of a TPMS information. In [16], the authors evaluate the cybersecurity of TPMS wireless communications and they propose some implementing solutions. The authors of [17] implement a lightweight protocol for TPMS within a testing scenario. From all the above works dedicated to TPMS, for our application example, we inherit only the possible vulnerabilities of the system and, in addition, we provide a risk analysis.

To conclude, to the best of our knowledge, our work is one of the first which combines descriptions and comparisons of the two new main references to increase automotive cybersecurity: UNECE WP.29 R155 and ISO/SAE 21434. Besides, we compare them in detail by highlighting similarities and differences and we underline possible limits when applying the standard and the regulation in a use case scenario.

3. Emergent Cybersecurity Norms

In this section, we present the regulation UNECE WP.29 R155 and the standard ISO/SAE 21434 as the two major references for cybersecurity vehicle compliance in automotive.

3.1. UNECE WP.29 R155 Purpose and Structure

The United Nations Economic Commission for Europe (ECE or UNECE) represents one of the five regional commissions under the jurisdiction of the United Nations Economic and Social Council. It is composed of more than 60 countries that, as part of UNECE WP.29 members, presented in March 2021 the regulations for cybersecurity in road vehicles. Within the UNECE WP.29 regulations, two documents cover key future topics in the automotive domain: i) Cybersecurity (R155) [7] and ii) Software (SW) Update (R156) [18]. Entities such as OEM and Tiers of the UNECE countries will need to be compliant with the UNECE regulations to be authorized to present new vehicles on markets. This authorization will be mandatory for all new vehicle types from July 2022 and it will become mandatory for all vehicles produced from July 2024.

UNECE R155 covers two main aspects:

- The establishment of a Cyber Security Management Systems (CSMS) related to organizations policies and processes to manage cyber-risks spanning the entire life-cycle of vehicles, equipment, and services.
- The required documentation, the process, and the emission of the UNECE Certificate of Compliance for CSMS to homologate new vehicle types.

The most significant innovation is the requirement of a CSMS, which is *a systematic risk-based approach defining organizational processes, responsibilities, and governance to treat risk associated with cyber threats to vehicles and protect them from cyber-attacks* [7]. The OEM has to implement the CSMS to apply for a Certificate of Compliance for Cyber Security Management System. After an assessment process, the Approval Authority shall issue the Certificate, which remains valid for a maximum of three years from the date of issue unless it is withdrawn. After the CSMS implementation and the receipt of the certificate, the car manufacturer could start the Vehicle Type Approval (VTA) process for its new vehicle types. During this phase, two actors are involved: the technical service to test the vehicle and the Approval Authority, which is in charge to homologate the vehicle type after the validation and testing process. To be compliant with UNECE R155, OEMs have to consider the detection and response to possible cybersecurity attacks, the risks assessment done during the development phase, and the applied mitigations. In particular, UNECE R155 proposes in Annex 5 threats and mitigation actions. This annex is composed of three main parts, i.e., Parts A, B, and C:

3.1.1. Part A. It describes the threats, vulnerabilities, and attack methods. The table lists the vulnerabilities or attack methods related to possible threats. In particular, it describes 32 threats, divided according to the attack surface like the back-end servers or the communication channels. For each threat, it is reported an example of a vulnerability or attack method. The list is a high-level description and it does not claim to be exhaustive, but it is one of the most complete threats lists for automotive, so it could be a starting point for a vulnerability assessment. The listed threats can compromise different properties like the CIA (Confidentiality, Integrity, and Availability). For instance, confidentiality can be compromised as stated at point 7 of the Table where *"information can be readily disclosed. For example, through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders"*. Integrity is discussed at point 5 where communication channels could be used to *"conduct unauthorized manipulation, deletion, or other amendments to vehicle held code/data"* with, for example, code injection or overwriting. The third property, availability, must be assured to preserve also the safety of the users, but, as shown at points 8 and 13, could be compromised with Denial of Service (DoS) attacks.

3.1.2. Part B. It describes mitigation actions to the threats related directly to the vehicle. For instance, Table B1 deals with the vulnerabilities related to the communication channels. To assure confidentiality of the messages, the mitigation M12 states that *"confidential data transmitted to or from the vehicle shall be protected"*, but without giving any further detail or possible implementations. The other tables in Part B answer to the other threats defined in Part A, but the mitigation are always high-level solutions, leaving the carmakers the possibility to apply the best ad-hoc solution for each context.

3.1.3. Part C. It describes mitigation actions to the threats related to entities outside vehicles, e.g. carmakers' servers.

For example, to minimize unauthorized access to back-end systems, Table C1 suggests some mitigations like the application of security checks and following the Open Web Application Security Project (OWASP) to find examples of controls.

3.2. ISO/SAE 21434 Purpose and Structure

ISO/SAE 21434, released in its first final version in August 2021, aims to be the cybersecurity standard in the engineering of electrical and electronic (E/E) systems for road vehicles. The document provides OEMs and their suppliers (e.g. Tier 1, Tier 2) guidelines to manage cybersecurity risks during the design, production, and post-production phases.

The developing process of the standard lasted about five years and it brings to supersedes the previous cybersecurity standard SAE J3061:2016 [19]. Confirmed by the direct citations in the document, ISO/SAE 21434 is inserted in a specific network of standards and regulations like ISO:26262-3:2018 [20], which is the most common standard to assure safety for road vehicles. ISO/SAE 21434 is composed of three introduction sections, fifteen clauses, which can be considered as sections, and eight annexes. In particular, the first three sections have declared the scope, the normative references, and a glossary for automotive cybersecurity. In the next fifteen clauses are defined the requirements (RQ), recommendations (RC), and work products (WP). In particular, ISO/SAE 21434 covers all the product life cycle from design to decommissioning. Following, we summarise some of the most significant clauses with their innovations.

3.2.1. Clause 5. It designs the mandatory internal cybersecurity organization for OEMs and Tiers. The main concept is that a company can assure the cybersecurity of a product only if it has a well-defined internal organization to manage cybersecurity with defined roles and responsibilities [RQ-05-01/02]. In addition, an important novelty is a definition and the request for a strong cybersecurity culture [RQ-05-06], where cybersecurity and safety have the highest priority. This clause defines also the procedures of information sharing within and outside the organization with the encouragement of disclosure internally and externally of the new potential vulnerabilities [RQ-05-09].

3.2.2. Clause 7. It defines the distribution of responsibilities with the Tiers. The process of referring to a supplier for some phases of the item life-cycle increases the risk of threats. So it is required to study the supplier cybersecurity capability [RQ-07-01] and to have a clear distribution of responsibilities [RQ-07-04].

3.2.3. Clause 8. It defines the continuous monitoring and improvement activities during the entire life-cycle of an item. In paragraph 8.5, it is required a vulnerability analysis to identify possible threats. The analysis can include a design of the architecture and an attack path analysis [RQ-08-05] that can be based on a top-down approach (e.g. attack tree) or a bottom-up approach starting from the revealed vulnerabilities [paragraph 15.6.2]. Besides, the analysis can include an attack feasibility rating. Paragraph 8.6 defines the vulnerability management process to treat any found risk with the possible decisions to avoid, reduce, share or retain the risk.

3.2.4. Clause 11. Following Clause 10, which defines the cybersecurity verification process, Clause 11 describes the validation activities for an item with the configurations intended for series production. The validation is necessary to confirm the achievement of the cybersecurity goals. In particular, it is cited Annex E, where are defined the cybersecurity assurance levels (CALs) that specify the amount of rigour required in the product development and that can be used to scale, for example, the depth and rigour of the penetration test.

3.2.5. Clause 15. It describes methods to determine the possible threats to which a user and a vehicle are exposed. The methods and the works are known as threat analysis and risk assessment (TARA). This clause aims to identify and mitigate the risk with appropriate countermeasures. In this clause, several documents are proposed: asset identification, threat scenario, impact rating, attack path analysis, attack feasibility rating, risk value determination, and risk treatment decision.

1) Asset identification to identify a damage scenario with an impact rating or threat scenario analysis, or existing catalogs of threats [RQ-15-01/02].
2) Threat scenario identification with the use of approaches based on frameworks such as EVITA, TVRA, PASTA, or STRIDE [RQ-15-03].
3) An impact rating should be defined starting from four different impact categories: safety, financial, operational, and privacy (S,F,O,P) respectively [RQ-15-04]. For each category, there are four main impact values: severe, major, moderate, or negligible [RQ-15-05]. Moreover, additional impact categories can be considered and safety-related impact ratings can be retrieved from ISO:26262-3:2018 [20].
4) Attack path analysis as defined in Clause 8.
5) Attack feasibility rating with four different possible values (high, medium, low, very low), starting from the lowest necessary effort to perform an attack to the highest effort [RQ-15-10]. Clause 15 provides also several core factors like elapsed time for an attack, specialist expertise, window of opportunity, attack complexity, that should be considered according to the chosen approach [RQ-15-12/13/14].
6) Risk value determination that can be performed with a risk matrix or risk formulas [RQ-15-16].
7) Risk treatment decision to define the risk treatment options: avoiding risk, reducing, sharing, or retaining the risk for each threat [RQ-15-17].

4. UNECE R155 and ISO/SAE 21434 similarities and differences

The development of regulation UNECE R155 and standard ISO/SAE 21434 started when it was evident that cybersecurity should be applied to road vehicles to continue to assure the users' safety and the protection of

personal data. UNECE R155 was released in its first version in March 2021, so it is earlier than ISO/SAE 21434, released in August 2021, but, while some standards like ISO 26262 are widely cited in ISO/SAE 21434, the regulation is never directly quoted. Nevertheless, in this section, we investigate the similarities and differences between the regulation and the standard, providing also some limitations discovered during our analysis. To anticipate the conclusions of the following analysis, in our opinion, the regulation and the standard have similar requirements like the risk identification and the definition of mitigation measures. Besides, they can be considered complementary because, for example, UNECE R155 requires a CSMS, which can be used as evidence to answer the request of ISO/SAE 21434 of an organizational and project cybersecurity management [Clauses 5-6]. At the same time, documents required by the standard like the vulnerability analysis and risk value determination can be used as evidence of a cybersecurity management of the risks during the UNECE homologation.

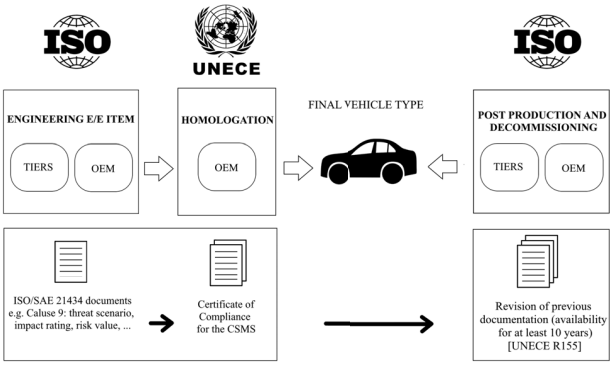

Figure 1. UNECE R155 and ISO/SAE 21434 main application and documentation during the vehicle production, homologation and post-production phase.

4.1. Similarities

Even if UNECE R155 and ISO/SAE 21434 are different types of documents, the first is a regulation, while the second is a standard, both are applied on the product lifecycle to improve the cybersecurity of road vehicles. Due to this common process application, it is possible to identify some shared activities and documentation. In this context, the word "similarity" has the meaning of "points of contact", where both documents agreed on similar requests or solutions. Firstly, both UNECE R155 and ISO/SAE 21434 propose high-level solutions, describing only the intentions, and leaving the carmakers the possibility to apply the most suitable solutions to each item. For example, UNECE R155 identifies the possible threats of malicious internal (e.g. CAN) messages (Table A at point 11 in [7]), and as mitigation suggests the consideration of measures to detect malicious internal messages or activity, without giving any further details (Table B1 in [7]). ISO/SAE 21434 in clause 15.6.2 cites a possible threat scenario like the spoofing of CAN messages and it requires an analysis of the attack path, a vulnerability analysis, attack feasibility ratings, a risk value determination, and a risk treatment decision. However, the clause leaves the carmaker free to apply its implementations and mitigations. Both UNECE R155 and ISO/SAE 21434 do not provide direct solutions to be implemented to reach cybersecurity. From one side, this situation is intended to leave the producer free to adopt the best suitable solutions for each context. On the other side, this lack of defined solutions can create a fragmented situation in a highly connected environment like automotive, without any control of reliability of the adopted solutions, which can reduce cybersecurity in the network. Besides, both documents do not provide any threshold, for example, for the vulnerability assessment or the risk decision treatment. In this way, each carmaker can define its thresholds with the consequence that different carmakers can define distinct action limits, giving a different cybersecurity level to the same item.

Both documents require a structured organization to manage cybersecurity. UNECE R155 requires the CSMS with risk identification, security tests, continuous cybersecurity monitoring, and improvements. ISO/SAE 21434 contains all these concepts and requires, like UNECE R155, constant monitoring of the cybersecurity activities with internal and/or external audits. Both documents adopt the concept of *risk mitigation*, intended as the process of developing actions and solutions to reduce and dealing threats. In particular, UNECE R155 at point 7.2.2.2d recommends verifying that the identified risks are appropriately managed, while ISO/SAE 21434 in Clause 15.9 defines the possible risk treatment decisions: avoiding, reducing, sharing, and retaining the risk.

Following the discussed similarities and as shown in Figure 1, the documentation created for the ISO/SAE 21434 could be used also in the Certificate of Compliance emission of the UNECE R155. The standard requires several work products and documents that can be used to be compliant with point 7.2.2.2 of UNECE R155, which requires proof that security is adequately considered during the item's life. In addition, both documents require the continuous revision of the work products after the production of the item to assure a continuous assistance service until the communication of the end of support, as required in ISO/SAE 21434.

Another limit that can have both documents is the meeting of the compliance at acceptable implementation costs for the carmakers and consequentially for the customers. The regulation and the standard define complete management systems to achieve cybersecurity, but the complexity of the automotive environment can lead to practical difficulties to implements cybersecurity solutions. For instance, the confidentiality of every message in and outside the vehicle can be achieved by applying cryptographic protocols, for example on CAN or LIN messages, but computation and time costs should be considered. Will time cost be acceptable for time-sensitive messages, without compromising safety? In our opinion, this topic has to be deeply investigated by regulators and carmakers to avoid the risk of a reduction of the cybersecurity thresholds by the carmakers, for example, during the vulnerability assessments, to reach a compromise between cybersecurity and operations.

4.2. Differences

Table 1 shows some differences between the two documents. The most relevant difference is inbuilt and fundamental: UNECE R155 is a regulation, defined as a legally binding directive for all the countries belonging to UNECE, while ISO/SAE 21434 is a standard, so it is not mandatory for automotive industries, but it is expected to be widely accepted. UNECE R155 defines the term July 2022 to be implemented in the new vehicle types and July 2024 for the first registration vehicles, while ISO/SAE 21434 started to be applicable from August 2021.

TABLE 1. MAIN DIFFERENCES BETWEEN UNECE R155 AND ISO 21434.

	UNECE R155	ISO 21434
Document Type	regulation	standard
Application	mandatory	optional
First Release Date	March 2021	August 2021
Application Phase	Homologation	Life-cycle Product
Approach	Risk-based	Security by design
Glossary	13 terms	40 terms

Even if the two norms shape the entire product life-cycle, as shown in Figure 1, they have two different main application phases. To be compliant with ISO/SAE 21434 it is necessary to create documents for annual audit during the life-cycle of a product, from the design to the de-commissioning. UNECE R155 requires the documentation during the homologation phase when the carmakers have to obtain the approval of the Certificate of Compliance for the CSMS to sell the vehicle. The required documentation for UNECE R155 has to be created or inherited from all the phases of the product life-cycle. Thus, the presence of the UNECE R155 only during the homologation phase is just referred to when the documentation is verified by the Authority but it affects the entire life-cycle of the product.

Another difference, reported in Table 1, is the presence in ISO/SAE 21434 of a glossary more than three times larger than the glossary of UNECE R155. The definitions, contained in the standard, could become the reference to avoid misunderstanding in the usage of cybersecurity terms in automotive. While a possible limit of UNECE R155 could be, for example, the usage of the adjective "*confidential*" in Part B, Table B1 point 7.1, mitigation M12, where the regulation requires to protect "*confidential data*" transmitted, but it does not specify which are the confidential data. Without a clear definition, each car-maker can have its definition of confidential data. For example, one company can consider only personal data like name, surname as confidential, while, as shown in several works like [21], [22], [23], a driver could be identified also from data generated during the driving like speed or revolutions per minute (rpm). Should be also the vehicle data considered confidential? The lack of a complete glossary like in ISO/SAE 21434 could be a risk for cybersecurity.

UNECE R155 provides some tables with several possible threats and mitigations, while ISO/SAE 21434 does not deal directly with attacks. UNECE R155 requires a list of documents to be compliant, but this list is less detailed than ISO/SAE 21434, which in its Annex A Table A.1 provides a precise list of possible work products.

A possible limit exclusive of ISO/SAE 21434 is where the standard defines the attack feasibility rating in its Annex G, but, as described in [11], the three possible approaches are not interchangeable. The wrong choice of one approach can lead to misinformed risk-based decisions. According to [11], further developments need to investigate which method is closest to real-world attack feasibility.

5. Application of ISO/SAE 21434 and UNECE R155: a use case

In this section, we describe an application scenario in which two manufacturers apply the standard ISO/SAE 21434 on a Tire Pressure Monitoring System (TPMS) product of the body domain, and, as a mandatory request, they need also to achieve the UNECE homologation for the product. In this scenario, we consider an in-vehicle communication network like in Figure 2, and we focus on the body domain, composed of the sensors for vehicle dynamic controls, referring to the four wheels and their relative position and movement. The communications in the body domain can be performed using the CAN protocol, which is the most used protocol to exchange messages among Electronic Control Units (ECUs) of vehicles.

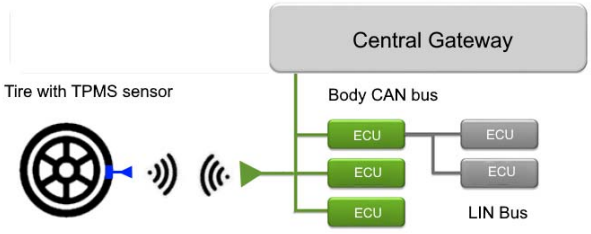

Figure 2. TPMS schema with the body domain network [24].

The CAN protocol for in-vehicle communications was originally designed for multiplex electrical wiring within vehicles. Messages are commonly named *CAN frames* and the latest version is CAN2.0, dating back to 1991. The CAN protocol was introduced without any security protection on top of it: authentication, integrity, and confidentiality are not supported. This makes the CAN protocol vulnerable to an active attacker who wants to gain some digital access to the vehicle, either locally or remotely [2] [25]. The single TPMS is composed of a sensor that monitors the pressure of the tire and sends wireless data to the vehicle's receiver, which processes and broadcasts those data to the vehicle's ECU through the CAN bus.

As shown in [14] and [15], the TPMS could be attacked, generating security and privacy risks. In particular, in [14], the authors show that data eavesdropping is easily possible at a large distance from a passing vehicle, while in [15] the attacker can replace the original message with a malicious one that could impact other ECUs. In [26], the authors show a possible privacy leakage in which an attacker can track the behaviors of the driver by messages eavesdropping.

Following the ISO/SAE 21434 guidelines, during the designing of a TPMS system, a carmaker or a Tier has to analyze all the possible threats and vulnerabilities to treat

the risks. In this example, we analyze the risks coming from the previously described attacks on TPMS. In our scenario, to be compliant with the standard, a manufacturer has to secure TPMS by implementing a solution to address at least authentication and integrity properties on CAN messages, as it is also proposed by AUTOSAR [6]. This may mitigate attacks from an attacker model as follow:

- *tampering*, the manipulation of frames to invalidate their contents so that receiving ECUs cannot perform the operations that were originally meant.
- *fuzzing*, the manipulation of frames to study the behavior of target ECUs.
- *forging*, the generation of a valid frame to generate a valid signal and activate a specific ECU functionality.
- *replaying*, the reuse of valid frames to repeat the generation of a valid signal and reactivate a specific ECU functionality.
- *masquerading*, the generation of a valid frame to abuse the identifier of another, genuine ECU.

In Table 2, we report an high-level analysis of how two different manufacturers, on the same system/component, can implement two different risks and treatment analyses to be both compliant with ISO/SAE 21434 and reach homologation. To assign the occurrence, impact, and risk values in Table 2, we apply TVRA methodology [27] as reported in [28], where the product of occurrence probability and impact value return the risk which is a measurement for the risk that the concerned system is compromised. The risk scale is composed of three categories from the lowest to the most significant for cybersecurity: *Minor*, *Major*, and *Critical*. In particular, both manufacturers can achieve compliance with the standard and reach the homologation by implementing a complete CSMS. Moreover, without having a minimum threshold level to reach for the risk analysis in the standard and the regulation, both carmakers can achieve their goal even by applying a different risk analysis on the same component type. Due to this last aspect, *Manufacturer A* may consider the system secure assuring some properties like authentication and integrity for messages coming from TPMS. On the other hand, *Manufacturer B* can consider a wider threat model in which an attacker can also perform the *sniffing attack* on the clear-text payload. Considering this threat, an attacker may reconstruct the signals database, e.g., DBC, which is a CAN data description file format, nullifying all the previously adopted solutions for TPMS. Besides, the DBC with data coming from TPMS can be considered a private product of the carmaker, containing information related to the driving style of the driver. In Table 2, we report also the risk decisions of the manufacturers. According to ISO/SAE 21434, there are four possible options to treat the risk: avoiding the risk removing the risk sources, reducing with proper actions, sharing through contracts, or transferring risk by buying insurance, and retaining. In our scenario, it is not possible to remove the risk sources and it is however highly dangerous for the security to keep the risk, so we choose, as a possible real situation, that our manufacturers can reduce the risk, by implementing some mitigations as reported in Table 2.

To conclude, we point out that, giving different risk values to the threats, the same component may result more exposed to attacks, such it is for the *Manufacturer A* case than the component of *Manufacturer B*. However, based on the current standard and regulation, both manufacturers can reach the homologation for the TPMS system. More specifically, *Manufacturer A* may formally be compliant with UNECE R155, even if it applies only authenticity and integrity on CAN messages, because, in our example, it provides risk mitigation for the possible selected threats. However, in Table 2, we report the UNECE homologation with *high probability*, and not acquired, because the lack of the analysis of some attacks could lead to a refusal of the homologation, but this occurrence seems to be highly unlikely because in the regulation it is not required a specific threshold or attack analysis for a system domain like body or chassis. *Manufacturer A* does not consider the unauthorized access to the body domain a possible threat. However, without threshold values for the risk analysis, one manufacturer can consider sufficient its risk decisions and mitigations, but, in this situation, the same component of two different manufacturers can have a different cybersecurity level, exposing the customer to risks.

6. Conclusion

Considering the urgent need for cybersecurity regulations in the automotive domain, the two documents, UNECE R155 and ISO/SAE 21434 will serve as a reference for the development of secure vehicles soon. In this paper, we have presented a discussion and comparison of the two documents by underlining their similarities and differences. Moreover, we have highlighted their possible limitations using an application scenario.

From our study, we can conclude that both documents ask for evidence of the application of the "risk-based" and "secure by design" methodology and they can be considered complementary to reach cybersecurity in automotive. In particular, ISO/SAE 21434 can provide the guide and the documentation support to be compliant with UNECE R155, while UNECE R155 refers to ISO/SAE 21434 in several points as described in Section 4.1. At the same time, in our opinion, the UNECE R155 and ISO/SAE 21434 should be extended due to the lack of thresholds that may lead to the subjective assignment of risk values different from one carmaker to another. A possible implementation may be the definition of more detailed frameworks, for example, different for each domain of the vehicle network, to define thresholds or values to assign during the risk assessment and mitigation analysis.

References

[1] Doug Newcomb. (2012) The next big os war is in your dashboard. [Online]. Available: https://www.wired.com/2012/12/automotive-os-war/

[2] Chris Valasek and Charlie Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," https://illmatics.com/Remote%20Car%20Hacking.pdf, 2015, last access: 28/01/2021.

[3] International Organization for Standardization, "Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling," https://www.iso.org/standard/63648.html, 2015, last access: 28/01/2021.

TABLE 2. COMPARATIVE ANALYSIS OF TWO MANUFACTURERS' RISK EVALUATIONS

Possible risk decisions [ISO/SAE 21434: 15.9.2]: avoiding, reducing, sharing, or retaining								
OP: Occurrence Probability (Low, Medium, High), **IL: Impact Level** (Low, Medium, High), **RR: Risk Rating** (Minor, Major, Critical)								
System	**Considered Risks**	**Compromised Properties**	**OP**	**IL**	**RR**	**Risk Decision**	**Mitigation**	**Result**
MANUFACTURER A								
TPMS CAN communication	Tampering, fuzzing, forging, replaying, masquerading	Authentication, integrity	Low	Medium	Minor	Reducing	TPMS ID randomization [26]	Compliant with ISO/SAE 21434 and, *with high probability,* homologation UNECE R155
MANUFACTURER B								
TPMS CAN communication	Tampering, fuzzing, forging, replaying, masquerading, *sniffing*	Authentication, integrity, *confidentiality*	Medium	Medium	Major	Reducing	TPMS ID randomization [26] and *Basic Software (BSW) module CINNAMON* [29]	Compliant with ISO/SAE 21434 and homologation UNECE R155

[4] Tencent Keen Security Lab, "New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars," https://keenlab.tencent.com/en/2018/05/22/New- CarHacking-Research-by-KeenLab-Experimental- Security-Assessment-of-BMW-Cars/, 2018, last access: 28/01/2021.

[5] R.-P. Weinmann and B. Schmotzle, "TBONE – A zero-click exploit for Tesla MCUs," https://kunnamon.io/tbone/tbone-v1.0-redacted.pdf, 2021.

[6] AUTOSAR. (2020) Specification of Secure Onboard Communication AUTOSAR CP R20-11. [Online]. Available: https://www.autosar.org/fileadmin/user_upload/standards/classic/20-11/AUTOSAR_SWS_SecureOnboardCommunication.pdf

[7] UNECE, "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system," United Nations Economic Commission for Europe, Geneva, CH, Regulation Addendum 154 – UN Regulation No. 155, 2021. [Online]. Available: https://unece.org/sites/default/files/2021-03/R155e.pdf

[8] ISO, "Road vehicles — cybersecurity engineering," International Organization for Standardization, Geneva, CH, Standard ISO/SAE FDIS 21434:2021 Ed.1, 2021. [Online]. Available: https://www.iso.org/standard/70918.html

[9] T. Brandt and T. Tamisier, "The future connected car – safely developed thanks to unece wp.29?" in *21. Internationales Stuttgarter Symposium*, M. Bargende, H.-C. Reuss, and A. Wagner, Eds. Wiesbaden: Springer Fachmedien Wiesbaden, 2021, pp. 461–473.

[10] G. Macher, C. Schmittner, O. Veledar, and E. Brenner, "ISO/SAE DIS 21434 automotive cybersecurity standard - in a nutshell," in *SAFECOMP 2020 Workshops, Lisbon, Portugal, September 15, 2020, Proceedings*, ser. LNCS, vol. 12235. Springer, 2020, pp. 123–135.

[11] S. Powley, "Comparative evaluation of cybersecurity methods for attack feasibility rating per iso/sae dis 21434," 02 2020.

[12] M. Brown, "Addressing the challenges of a sector in transformation and preparing to meet new cyber compliance burdens (iso/sae 21434)," 2020.

[13] T. Micro, "Identifying cybersecurity focus areas in connected cars based on wp.29 un r155 attack vectors and beyon," T. Micro, Ed., 2021. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/a-roadmap-to-secure-connected-cars

[14] I. Rouf, R. D. Miller, H. A. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington, DC, USA, August 11-13, 2010, Proceedings*, 2010, pp. 323–338. [Online]. Available: http://www.usenix.org/events/sec10/tech/full_papers/Rouf.pdf

[15] K. Daimi and M. Saed, "Securing tire pressure monitoring system," https://www.thinkmind.org/index.php?view=article& articleid=aict_2018_3_10_10010, pp. 32–37, 2018.

[16] D. K. Kilcoyne, S. Bendelac, J. M. Ernst, and A. J. Michaels, "Tire pressure monitoring system encryption to improve vehicular security," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 1219–1224.

[17] K. Emura, T. Hayashi, and S. Moriai, "Toward securing tire pressure monitoring systems: A case of present-based implementation," in *2016 International Symposium on Information Theory and Its Applications, ISITA 2016, Monterey, CA, USA, October 30 - November 2, 2016*. IEEE, 2016, pp. 403–407. [Online]. Available: https://ieeexplore.ieee.org/document/7840455/

[18] UNECE, "Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system," United Nations Economic Commission for Europe, Geneva, CH, Regulation Addendum 155 – UN Regulation No. 156, 2021. [Online]. Available: https://unece.org/sites/default/files/2021-03/R156e.pdf

[19] SAE, "Cybersecurity guidebook for cyber-physical vehicle systems," Society of Automotive Engineers, USA, Tech. Rep. J3061_201601, 2016. [Online]. Available: https://www.aiag.org/store/publications/details?ProductCode=PPAP-4

[20] ISO, "Road vehicles — functional safety," International Organization for Standardization, Geneva, CH, Standard ISO 26262:2018, 2021. [Online]. Available: https://www.iso.org/standard/68383.html

[21] J. Carmona, F. García, D. Martín, A. de la Escalera, and J. M. Armingol, "Data fusion for driver behaviour analysis," *Sensors*, vol. 15, no. 10, pp. 25 968–25 991, 2015. [Online]. Available: https://doi.org/10.3390/s151025968

[22] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, "Automobile driver fingerprinting," *Proc. Priv. Enhancing Technol.*, vol. 2016, no. 1, pp. 34–50, 2016. [Online]. Available: https://doi.org/10.1515/popets-2015-0029

[23] G. Costantino, F. Martinelli, I. Matteucci, and P. Santi, "A privacy-preserving infrastructure for driver's reputation aware automotive services," in *Socio-Technical Aspects in Security and Trust - 9th International Workshop, STAST 2019, Luxembourg City, Luxembourg, September 26, 2019, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 11739. Springer, 2019, pp. 159–174.

[24] Electronic Specifier. (Retrieved October 2021) The evolution of gateway processors in the auto market. [Online]. Available: https://www.electronicspecifier.com/products/artificial-intelligence/the-evolution-of-gateway-processors-in-the-auto-market

[25] G. Costantino and I. Matteucci, "CANDY CREAM - hacking infotainment android systems to command instrument cluster via can data frame," in *2019 IEEE International Conference on Computational Science and Engineering, CSE 2019, and IEEE International Conference on Embedded and Ubiquitous Computing, EUC 2019, New York, NY, USA, August 1-3, 2019*, M. Qiu, Ed. IEEE, 2019, pp. 476–481. [Online]. Available: https://doi.org/10.1109/CSE/EUC.2019.00094

[26] M. Vaszary, A. Slovacek, Y. Zhuang, and S. Chang, "Securing tire pressure monitoring system for vehicular privacy," in *18th IEEE Annual Consumer Communications & Networking Conference, CCNC 2021, Las Vegas, NV, USA, January 9-12, 2021*, 2021, pp. 1–6. [Online]. Available: https://doi.org/10.1109/CCNC49032.2021.9369576

[27] ETSI, "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," in *Tech. Rep. TR 102 893*, 2010, p. 33.

[28] HEAVENS, "Security models v2.0," 2016, p. 67.

[29] G. Bella, P. Biondi, G. Costantino, and I. Matteucci, "CINNAMON: A module for AUTOSAR secure onboard communication," *CoRR*, vol. abs/2111.12026, 2021. [Online]. Available: https://arxiv.org/abs/2111.12026