Cybersecurity Regulations and Standards in the Automotive Domain

Thomas Schober(✉) and Gerhard Griessnig

AVL List GmbH, Hans List Platz 1, 8020 Graz, Austria
{thomas.schober2,gerhard.griessnig}@avl.com

Abstract. The automotive industry is facing rapid changes with regards to the vehicle architecture, features and connectivity. These changes are transforming today's vehicles to more and more smart, autonomous and interconnected cars, but also open a wide variety of new threats and potential attacks. Therefore, it is crucial to include topics like cybersecurity and software updates into all stages of the lifecycle of modern cars to provide an appropriate protection level. New regulations and standards have recently been published or are currently in development to address these issues. This paper provides an overview about the UN Regulations No. 155 (cybersecurity) and 156 (software update) and the international standards ISO/SAE 21434, ISO PAS 5112, ISO 24089. It shows the connections and dependencies and the actual status of the publications.

Keywords: ISO/SAE 21434:2021 · ISO/IEC 24089 · ISO PAS 5112 · UN Regulation No. 155 · UN Regulation No. 156 · Cybersecurity · Software update · CSMS · SUMS · OTA

1 Introduction

During the last years, the automotive industry was facing a lot of new technological developments. These changes include the electronic and electrical vehicle architecture (E/E architecture), the introduction of advanced driver assistance systems (ADAS) and autonomous driving (AD) and connections to systems outside of the vehicle (vehicle to everything - V2X). These changes do not only have major implications on the vehicle engineering itself, but also mean that the topics cybersecurity and software update are getting more and more important.

The E/E architecture of modern vehicles is currently in a transition phase. It is evolving from distributed E/E architectures with many different xCUs for specific functions to a more integrated architecture with differed centralized domain xCUs. In future architectures the integration will increase even further with the introduction of central high-performance computers and zone xCUs. This architecture also enables a vertical split of different functions into servers and zones. [1] This evolution will also enable concepts like the integration of many different functions that could be enabled by the vehicle-owner after Start of Production (SOP) in a pay-per-use model.

The ongoing implementation of ADAS and AD systems also leads to an emerging usage of advanced machine learning and artificial intelligence technique. Along with

M. Yilmaz et al. (Eds.): EuroSPI 2022, CCIS 1646, pp. 530–539, 2022.
https://doi.org/10.1007/978-3-031-15559-8_38

intelligent transport systems and autonomous cars also the connectivity requirements of vehicles are increasing rapidly. This includes topics like Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [2]. Another upcoming and very important topic, also from cybersecurity point of view, is the integration and even offloading of vehicle functions into the cloud. Cloud computing offers various advantages, especially for functions that require a lot of computing performance and resources. This integration leads to really interconnected vehicles.

Cybersecurity and the ability of applying software updates are crucial aspects for modern vehicles. With the changes in the E/E architecture and the introduction of new technologies new threats and risks arise. Especially the increased connectivity and the introductions of cameras, radars, furthers sensors and interfaces lead to an increased attack surface. This is especially relevant for potential remote attacks that could threaten the privacy, security and especially also the safety of all road users.

This increasing demand for the topics cybersecurity and software updates was also acknowledged by the regulation authorities and standardization organizations. Therefore, new regulations and standards were released recently, or are currently under development. The following sections provide an overview about the actual status and gives an outlook about already planned follow-up activities.

2 Overview

The documents that are referenced in this paper can be classified in two different types. The first one are regulations, the second one international standards.

The regulations defined in this document are defined by the United Nations Economic Commission for Europe (UNECE), World Forum for Harmonization of Vehicle Regulations (WP.29). These regulations are legally binding for all member states that decide to apply it, for example the European Union (EU). [3].

International standards published by the ISO (the International Organization for Standardization) are a collection of the know-how and best practices of international experts. They are not legally binding, but it is possible to achieve a certification for showing compliance by an independent certification authority.

The following table provides an overview about the regulations and standards that are handled in this document (Table 1):

Table 1. Cybersecurity Regulations & Standards Overview

Name (Type)	Main focus	Impact
UN Regulation No. 155 (Regulation)	Cybersecurity Management System (CSMS)	The regulation defines the requirements for a CSMS, in order to achieve an approval for new vehicle types. It has a direct impact on all processes around the vehicle lifecycle, from concept and development to production and operation
ISO/SAE 21434 (Standard)	Cybersecurity Engineering	The international standard defines the requirements around cybersecurity engineering and covers the whole vehicle lifecycle It has impact on all engineering processes of cybersecurity relevant items and can be used as a more detailed implementation specification of a CSMS
ISO PAS 5112 (Standard)	Auditing Cybersecurity Engineering	The standard provides an approach and guideline on how cybersecurity engineering should be audited, in order to show compliance with ISO/SAE 21434 This standard directly impacts the CSMS audit procedure
UN Regulation No. 156 (Regulation)	Software Update Management System (SUMS)	The regulation defines the requirements for a SUMS, in order to achieve an approval for new vehicle types It has impact on all processes around software update management

(*continued*)

Table 1. (*continued*)

Name (Type)	Main focus	Impact
ISO/SAE 24089 Standard	Software Update Engineering	The standard defines requirements around the topic software update engineering It impacts the development and distribution processes of software updates and can be used as a more detailed implementation specification for a SUMS

In 2021 the UN Regulation No. 155 [4] and an Interpretation document regarding the regulation have been published. The Regulation No. 155 defines requirements for approval of vehicles with regards to cybersecurity and for a so-called cyber security management system (CSMS).

Also in 2021, the international standard ISO/SAE 21434 [5] was released. This international standard defined requirements for the cybersecurity engineering and defines a framework for the CSMS implementation.

This international standard is accompanied by the publicly available specification ISO PAS 5112 [6] that defines guidelines for the auditing of cybersecurity engineering. The ISO PAS 5112 was published in March 2022 (Fig. 1).

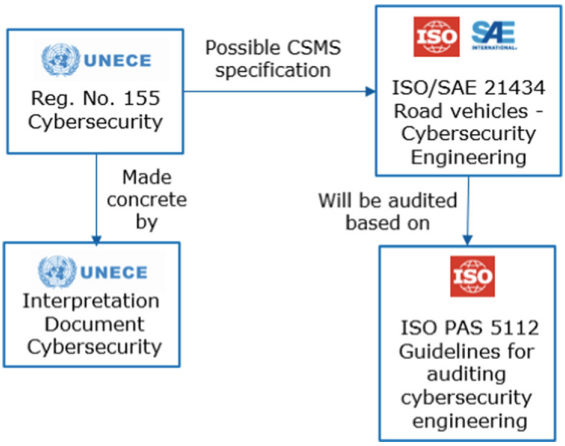

Fig. 1. Cybersecurity regulations & standards source: own illustration

Next to the cybersecurity regulations and standards the topic software updates has been addressed recently. In 2021 the UN Regulation No. 156 [7] and the corresponding Interpretation document have been released. This regulation defines uniform provisions concerning the approval of vehicles with regards to software update and software updates

management system (SUMS). A large part of the standard is reflecting the topic of over the air (OTA) software updates.

Like in the topic cybersecurity the UN Regulation is also accompanied by a corresponding international standard. The ISO 24089 [8] defines requirements for software update engineering and the framework for a SUMS implementation. The draft version (DIS) is already available for purchase. The final version should be released end of 2022 (Fig. 2).

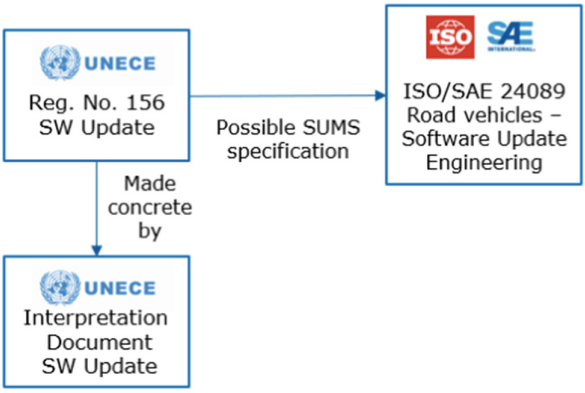

Fig. 2. Software update regulations & standards source: own illustration

The following picture shows the timeline of the different standards and regulations (Fig. 3):

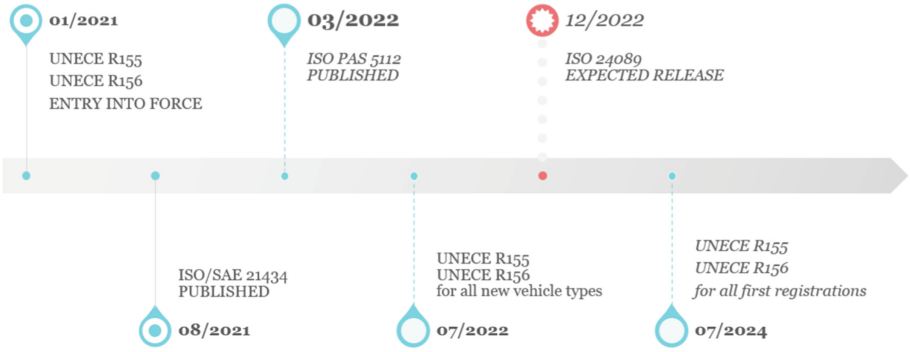

Fig. 3. Regulations & standards publication timeline source: own illustration

3 Cybersecurity Standards and Regulations

The following section provides an overview about the different cybersecurity related regulations and standards.

3.1 UN Regulation no. 155

The UN Regulation No. 155 defines uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system.

The Regulation applies mainly to vehicles used for the carriage of passengers and vehicles used for the carriage of goods.

In the European Union, the regulation will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

The UN Regulation No. 155 requires the vehicle manufacturer to obtain a Certificate of Compliance for the Cyber Security Management System (CSMS). This certificate will be issued by an approval authority or its technical service and is valid for three years.

The CSMS must cover the development, the production and the post-production phase. It includes all processes used to manage cybersecurity. This includes topics like risk analysis, risk treatment, cybersecurity controls and cybersecurity testing. Furthermore, it is required to implement cybersecurity monitoring and incident handling processes to recognize new attacks and to handle them in an appropriate timeframe.

In the Annex 5 of the regulation document a list of threats and corresponding mitigations is listed. It is stated that at least these threats and measures must be considered within the CSMS processes. The following threats are considered:

- Threats regarding back-end servers related to vehicles in the field
- Threats to vehicles regarding their communication channels
- Threats to vehicles regarding their update procedures
- Threats to vehicles regarding unintended human actions facilitating a cyber attack
- Threats to vehicles regarding their external connectivity and connections
- Threats to vehicle data/code
- Potential vulnerabilities that could be exploited if not sufficiently protected or hardened

For all threats potential mitigations measures are listed.

3.2 ISO/SAE 21434

The international standard ISO/SAE 21434 addresses cybersecurity in the engineering of E/E systems within road vehicles. The aim of the standard is to cover the different phases of the vehicle development and specify requirements that must be fulfilled to ensure an appropriate cybersecurity level.

The standard defines different requirements, recommendations and work products/deliverables that must be created before, during and after the product development. The whole standard is based on a risk-oriented approach (Fig. 4):

The standard is divided into different sections. It consists of the following main areas:

- Organizational cybersecurity management
- Project dependent cybersecurity management

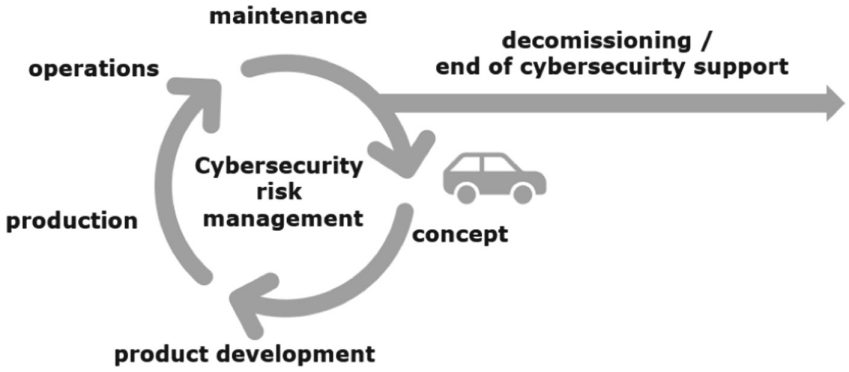

Fig. 4. Overall cybersecurity risk management Source: ISO/SAE 21434 [5]

– Distributed cybersecurity activities
– Continual cybersecurity activities
– Concept phase
– Product development phase
– Post-development phase
– Threat analysis and risk assessment methods

3.3 ISO PAS 5112

The ISO PAS 5112 Road vehicles – Guidelines for auditing cybersecurity engineering is related to ISO/SAE 21434 and extends ISO 19011 - Guidelines for auditing management systems, to the automotive domain. It is aimed for all organizations within the automotive domains that must conduct audits at the organizational level. The project and product level are not in the focus of ISO PAS 5112.

The ISO PAS 5112 covers the management of an audit programme, the planning and conducting of management system audits and the needed competences of an audit team. It includes a set of audit criteria that are based on the objectives of ISO/SAE 21434. The ISO PAS 5112 also includes an example questionnaire that can be adapted.

According to ISO PAS 5112 the audit team should have specific knowledge and skills in different areas, especially related to road vehicle cybersecurity. The required knowledge and skills are:

– automotive technologies
– road vehicle cybersecurity processes and risk management
– cyber security management systems
– ISO/SAE 21434

The informative questionnaire in Annex A of ISO PAS 5112 covers objectives of ISO/SAE 21434 and can be used by the audit team as a reference. It can also be extended, if needed. The questionnaire includes the following sections:

– Cybersecurity Management (4 questions)

– Continual Cybersecurity Activities (4 questions)
– Risk Assessment and Methods (3 questions)
– Concept and Product development Phase (3 questions)
– Post-development Phase (6 questions)

Distributed Cybersecurity Activities (1 question).
Each question includes the following topics:

– The question itself
– ISO/SAE 21434 Objectives
– Guidelines for the auditor (Topics that the auditor should verify)
– Evidence examples (e.g., ISO/SAE 21434 work products)

4 Software Update Standards and Regulations

The following section provides an overview about the different software update related regulations and standards.

4.1 UN Regulation No. 156

The UN Regulation No. 156 defines uniform provisions concerning the approval of vehicles with regards to software update and software updates management system.

The Regulation applies mainly to vehicles of a wide range of categories that permit software updates.

In the European Union, the regulation will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

The UN Regulation No. 156 requires the vehicle manufacturer to obtain a Certificate of Compliance for the Software Update Management System (SUMS). This certificate will be issued by an approval authority or its technical service and is valid for three years.

The regulation consists of three main areas of requirements that must be fulfilled to be compliant [9]:

– Software Update Management System (SUMS) Requirements
– Vehicle Requirements (Safe and secure execution of updates)
– Software Identification Requirements (RxSWIN)

The SUMS requirements basically define the organizational structure and processes that must be implemented to manage updates in a secure way. Therefore, all type approval relevant hardware and software versions must be recorded. Updates must be analysed regarding their compatibility, interdependencies and impact, especially also on safety or safe driving of the vehicle. Users must be informed about updates and the cybersecurity of updates must be ensured before and during sending them to the vehicle.

For every vehicle type evidence that the SUSM applies to it must be provided. A secure software update delivery mechanism must be implemented. The authenticity and integrity of software updates must be ensured. The RxSWIN must be protected and must be easily readable from the vehicle. The regulation also includes specific requirements for over-the-air updates (OTA). It must be ensured that users are informed about updates and that they are only executed if it is safe to do so.

Along with the SUMS the so-called RX Software Identification Number (RxSWIN) must be maintained. This is a dedicated identifier defined by the vehicle manufacturer representing information about the type approval relevant software of the Electronic Control System.

4.2 ISO 24089 (DIS)

ISO 24089 specifies requirements and recommendations for software update engineering in road vehicles on the organizational and on the project level. The requirements and recommendations apply to the vehicles XCUs and to software updates after the original development. It also defined requirements for the deployment of software updates to road vehicles.

The standard defined requirements and recommendations structured in the following areas:

- Organization level software update requirements
- Project level software update requirements
- Infrastructure design and development
- Vehicle and vehicle systems design and development
- Software update package development
- Software update campaign operations

In addition to the requirements and recommendations ISO 24089 also defines different work products/deliverable that must be created.

5 Conclusion and Outlook

First, it must be mentioned that the regulation and standardization of cybersecurity and software update management is still a very new topic. All the mentioned standards and regulations have either be published during 2021 (UN Regulations No 155, 156, ISO/SAE 21434), 2022 (ISO PAS 5112), or will be published during 2022 (ISO 24089). Therefore, all these documents are the first version where it can be foreseen already that further updates and improvements will follow.

The ISO's expert working group WG 11[1] that deals with cybersecurity for electrical and electronic components of road vehicles and that created ISO/SAE 21434 has already initiated follow-up activities after the recent release of the international standard:

[1] ISO WG 11 that operates under technical committee ISO/TC 22, Road vehicles, subcommittee SC 32, Electrical and electronic components and general system aspects.

- PWI 8475 - Cybersecurity Assurance Levels (CAL) and Target Attack Feasibility (TAF)
- PWI 8477 - Cybersecurity verification and validation
- Harmonization Task Force (This Task Force will analyse potential harmonisation between ISO/SAE 21434 and other relevant ISO standards and documents that would bring benefit to the users of ISO/SAE 21434)

Next to the further work on the ISO standards there are also further groups working on the topic of automotive cyber security. One of them is "The Verband der Automobilindustrie e.V." (VDA) that published the following documents:

- Automotive SPICE for Cybersecurity, 1st edition, 2021
- Automotive Cybersecurity Management System Audit, 1st edition, December 2020

References

1. Haas, W., Langjahr, P.: Cross-domain vehicle control units in modern E/E architectures (2016)
2. European Union Agency for Cybersecurity (ENISA): Good practices for security of smart cars (2019)
3. United Nations Economic Commission for Europe: FAQ, https://unece.org/faq 04 April 2022
4. United Nations: UN Regulation No. 155 - Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system (2021)
5. International Organization for Standardization: ISO/SAE 21434 - Road vehicles - Cybersecurity engineering (2021)
6. International Organization for Standardization: ISO PAS 5112 - Road vehicles – Guidelines for auditing cybersecurity engineering (2022)
7. United Nations: UN Regulation No. 156 - Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system (2021)
8. International Organization for Standardization: ISO/DIS 24089 - Road vehicles - Software update engineering (2022). (DIS)
9. UNECE: François Guichard, GRE-85–36. https://unece.org/sites/default/files/2021-10/GRE-85-36e.pdf (2021)