Status of the Development of ISO/SAE 21434

Christoph Schmittner[1(✉)], Gerhard Griessnig[2], and Zhendong Ma[2]

[1] AIT Austria Institute of Technology, Vienna, Austria
christoph.schmittner@ait.ac.at
[2] AVL List GmbH, Graz, Austria
{gerhard.griessnig, Zhendong.ma}@avl.com

Abstract. With the ongoing trend to incorporate new functionalities and functions based on the connectivity of vehicles, cybersecurity is becoming an important issue in the vehicle development lifecycle. While the first approaches to address this topic were based on research projects or adaptions of existing concepts of other domains, there is now a new ongoing activity to develop ISO/SAE 21434 a cybersecurity engineering standard for road vehicles. This standard addresses the complete lifecycle from development and production via operation and maintenance up to the decommissioning of the vehicles. We give an overview about the ongoing development, discuss potential contents and objectives and summarize time plan and open points.

Keywords: ISO/SAE 21434 · Cybersecurity · Standard · Automotive Road vehicles · Safety · ISO 26262 · SAE J3061

1 Introduction

The introduction of wireless connections, automated and assistive driving functionalities changed vehicles from physically isolated machines with electro-mechanical control systems into "smart phones on wheels". In the recent past with the electrification of vehicles the challenges were mainly timing, reliability and functional safety, addressed by internal guidelines and standards like ISO 26262:2011 [1]. The change towards cyber-physical automotive systems over the last years promises to improve the safety of drivers and support new applications such as monitoring system behavior or dynamically change and update configuration and software from remote. However, this also requires the consideration of cybersecurity.

Starting with activities in research projects like EVITA (E-Safety Vehicle Intrusion Protected Applications) [2], OVERSEE (Open Vehicular Secure Platform) [3] or EMC^2 (Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments) [4], and followed by the publication of the SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [5] the topic of automotive cybersecurity engineering was examined. While SAE J3061 was an important step forward it was also recognized that the guidebook could not fulfill a similar role like ISO 26262:2011 for the cybersecurity engineering of road-vehicles [6, 7]. The specific characteristic of the engineering processes for automotive systems like the distributed development made the direct application of existing cybersecurity

X. Larrucea et al. (Eds.): EuroSPI 2018, CCIS 896, pp. 504–513, 2018.
https://doi.org/10.1007/978-3-319-97925-0_43

standards like IEC 62443 [8] difficult. Differences in the risk assessments and particularities in safety engineering complicated also the direct application of existing IT-Security standards [9]. Therefore, the automotive industry decided to develop a domain-specific standard, ISO/SAE 21434 “road vehicles – cybersecurity engineering”.

To give an overview about the current status and discuss the ongoing developments, this paper follows the following structure:

- Section 2 explain the motivations and gives an overview about the interaction between ISO 26262:2018 and ISO/SAE 21434
- Section 3 presents the timeline
- Section 4 and its subsections give an overview about the current content
- Section 5 gives an outlook about the ongoing development

2 Motivations for the Development of ISO/SAE 21434

There were some discussions during the development of ISO 26262:2018 [10] how to address the topic of automotive cybersecurity. Considering the history and underlying principles of these two disciplines and based on the facts that (a) not every safety-critical system is equally security-critical and (b) there are security-critical systems without immediate safety impact it was decided to restrict the cybersecurity consideration in ISO 26262:2018.

The decision was to describe only the interface from functional safety to cybersecurity in ISO 26262:2018. It was also decided to leave the interface on the cybersecurity side unspecified to not anticipate a cybersecurity standard development. In the end ISO 26262:2018 requires communication channel between safety and cybersecurity engineering. The aim is the necessity to coordinate the development of these disciplines and to exchange requirements on system, software and hardware level. An annex in Part 2 of ISO 26262:2018 gives some additional background for the interaction.

It was recognized that there is a necessity to develop an automotive cybersecurity standard. Such a domain-specific cybersecurity engineering standard is not only to collect the state of the art it should also support and ease the cooperation between partners in the automotive and its supply chain by clarifying terminology and risk management approaches and by defining clear interfaces between companies.

3 Timeline ISO/SAE 21434

The New Work Item Proposal (NWIP) was submitted in 04.2016 and the development started in 10.2016 with the definition of the overall scope and establishment of four topic groups. Of particular note is that the working group itself consists of ISO and SAE experts, one of the first active Joint Working Groups between ISO and SAE [11].

On ISO side the topic is assigned to ISO/TC 22/SC 32 [12] which is also responsible for the development of ISO 26262. At ISO the WG8 is responsible for the functional safety standard development and WG11 is responsible for the cybersecurity standard development.

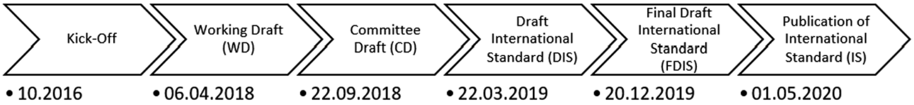
Kick-Off
Working Draft (WD)
Committee Draft (CD)
Draft International Standard (DIS)
Final Draft International Standard (FDIS)
Publication of International Standard (IS)
• 10.2016
• 06.04.2018
• 22.09.2018
• 22.03.2019
• 20.12.2019
• 01.05.2020

Fig. 1. ISO 21434 timeline

As seen in Fig. 1 there are different maturity stages for standard development with different expectations on the content and opportunities to contribute. We are currently at the Working Draft stage. At this stage the included contents are more or less known, but the specification of requirements and approaches is still ongoing. This means that the mentioned topics will probably be included in the final version, but detailed approaches might change.

While the WD is only shared and commented on a joint working group (JWG) level the committee draft (CD), the draft international standard (DIS) and finally the final draft international standard (FDIS) are open to additional experts from SAE and ISO national bodies. Procedures for ISO and SAE are different, but the collaborative way requires the process to satisfy both sides. In general, after each stage there will be a ballot phase with commenting. CD and DIS will receive technical and editorial comments, FDIS is restricted to editorial comments. After the balloting phase comments are discussed and resolved on JWG level. The first version of ISO/SAE 21434 is planned to be published beginning of May 2020.

4 Overview of the Contents

Due to various reasons we cannot discuss the complete draft with all ongoing developments. The goal is to give an overview of the concepts and structure and highlight and discuss a few interesting topics.

It need to be remarked that this presentation is based on our own interpretation of the current documents and discussions and we can neither claim to predict the final version nor to present all topics which are in discussion. We present a snapshot from our viewpoint of the current status at the time of the working draft which can and will change.

4.1 Generic Overview

The scope of the overall project was defined during the kick-off meeting and refined in consecutive meeting. The current wording in ISO/SAE 21434 is:

> "This document specifies requirements for cybersecurity risk management for road vehicles, their components and interfaces, throughout engineering (e.g. concept, design, development), production, operation, maintenance, and decommissioning. A framework is defined that includes requirements for cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders. This document is applicable to road

vehicles that include electrical and electronic (E/E) systems, their interfaces and their communications. This document does not prescribe specific technology or solutions related to cybersecurity."

The work was split into four part groups, addressing all elements of cybersecurity engineering during the complete vehicle lifecycle. Below the part groups are specialized task forces preparing proposals how specific topics are addressed.

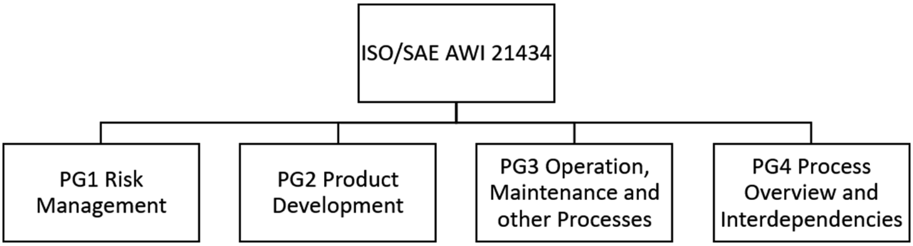
ISO/SAE AWI 21434
PG1 Risk Management
PG2 Product Development
PG3 Operation, Maintenance and other Processes
PG4 Process Overview and Interdependencies

Fig. 2. ISO 21434 JWG structure

Although each group listed in Fig. 2 started with the development of a standalone document it was combined for the WD and there is still an ongoing discussion if the standard will be one combined document or multiple documents.

4.2 PG1 Risk Management

Risk Management is one of the core activity in security engineering. In the end the goal of security engineering could be summarized as ensuring that risks due to cybersecurity issues are inside acceptable parameters.

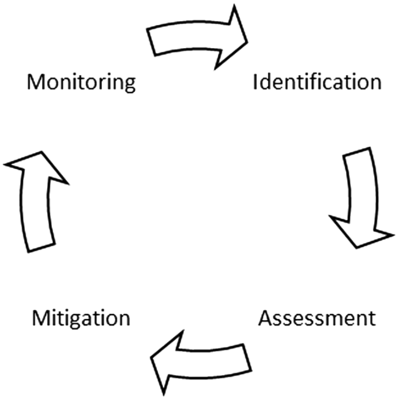

Fig. 3. PG1 risk management process

As shown in Fig. 3 there are four core activities to risk management which should follow each other. Due to the changing and evolving risk landscape in cybersecurity risk management is an ongoing process during the complete lifecycle. Therefore, the concept behind PG1 is to provide methods and approaches which can be used in other sections of the lifecycle.

One of the first methods provided is the cybersecurity relevance assessment. If one of the questions in Table 1 is answered with yes, the system is in scope of the ISO/SAE 21434. The goal of this relevance assessment was to provide a quick tool which can be used to determine if cybersecurity should be considered during the development. Due to the fact that attacks can use different attack surfaces and move through the vehicle network, the relevance assessment should ensure that no system which should be taken into account is omitted.

Table 1. Cybersecurity relevance assessment

Physical or wireless connection to any part of any internal vehicle communication network	Yes/no
Physical or wireless connection to any part of any external vehicle communication network	Yes/no
Indirect connection to any part of any vehicle communication network	Yes/no
Contains electronic or optoelectronic devices or hardware	Yes/no
Contains software	Yes/no
Contains a sensor	Yes/no

An important topic in PG1 is how to adapt existing risk management techniques for the automotive domain and distributed development. For risk management in general the ISO 2700X [13] standard series is referenced, but with adaptions to the automotive domain. An example is the concept for the division between, threat and vulnerability analysis. Threats are identified on the OEM level, with a view on the complete system. Vulnerability analysis is then the responsibility of the supplier who knows implementation details.

The risk assessment is based on parameters of ISO 15408 [14]. There was a discussion about defining a counterpart to the Automotive Safety Integrity Level (ASIL) from ISO 26262 during the risk assessment, which is then used to define rigor and applicable methods, but this is currently on hold. There was no consensus how to determine and treat such a parameter. One issue was the dynamic nature of risk parameters in cybersecurity, which could require frequent adjustments.

4.3 PG2 Product Development

The Product development sections is based on the same triple V-process as ISO 26262. System, Software and Hardware development. The strong reference to ISO 26262 was done because ISO 26262 is not only used for safety engineering but is also describing the general system engineering approach used in the automotive domain. Following roughly the same process should support the adoption (process structure and phases are easily understandable for all automotive experts) and interaction between system, safety and cybersecurity engineering. A major difference is the missing risk based tailoring. This means there is currently no tailoring based on the risk level.

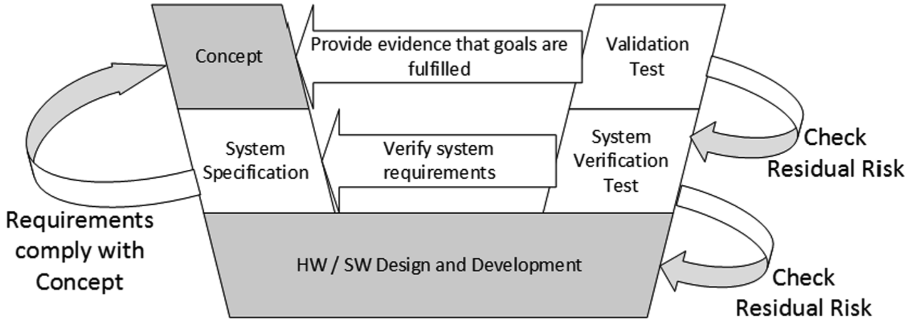
Concept
Provide evidence that goals are fulfilled
Validation Test
System Specification
Verify system requirements
System Verification Test
Check Residual Risk
Requirements comply with Concept
HW / SW Design and Development
Check Residual Risk

Fig. 4. System development phase

Figure 4 shows an overview of the system development phase. In the Concept Phase the Item is defined and, utilizing Threat Analysis and Risk Assessment (TARA) from PG1, Cybersecurity Goals are defined. During System Specification requirements are refined and assigned to Software and Hardware. After the System Concept is defined and during Software and Hardware Phase Vulnerability Analysis and Risk Assessment (VARA) are used to ensure that no additional threats are introduced and the residual risk is acceptable. Guidance on implementation is for Software mostly focused on secure software development and security functions and for Hardware on the usage of hardware security functions. After Software and Hardware Phases are completed Verification and Validation provide everything to release the system for production.

There is still an ongoing discussion about testing for security. Automated test methods have the advantage that they can be used earlier in the development process and their and their repeatability and comparability is better. Automated methods cannot replace manual pen-testing. Pen-testing is the best representation of a human attacker with his ingenuity, but it requires a more or less finalized system.

4.4 PG3 Operation, Maintenance and Other Processes

In cybersecurity vulnerabilities and weaknesses can be introduced throughout the complete lifecycle. It is therefore important to ensure cybersecurity during production and operation. PG3 focusses on these phases of the lifecycle.

Figure 5 gives an overview of the considered topics in PG3. The first section of PG3, gives requirements how to ensure that no unauthorized modification was introduced in the supply chain or during production. Focus is on how to protect hand-over of software and information from design to production and how to protect hardware during transport. Presented methods range from cybersecurity methods, like cryptographic hashes, to controlling and restricting the physical access. In addition, production requires relative unrestricted access in order to install and configure software and distribute cryptographic keys. During this stage the system is vulnerable and access to tools and systems need to be controlled. It is also necessary to ensure that production interfaces are deactivated and protected if they are no longer needed.

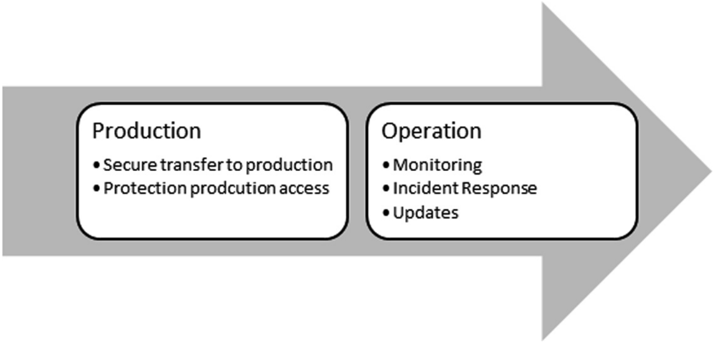
Production
• Secure transfer to production
• Protection prodcution access
Operation
• Monitoring
• Incident Response
• Updates

Fig. 5. Topics during production and operation

In order to ensure cybersecurity during operation it is necessary to monitor not only for incidents but also for vulnerabilities in used software and hardware components and prevent their exploitation. This section is still in development due to discussions if monitoring sources should be defined by requirements or given as informative examples. Policies and procedures on how to react on vulnerabilities and incident response programs conclude the section on cybersecurity during the operation process.

The last sections is about updating the system. The goal was here not to restrict or define technical approaches on updating, but define a state of the art about update processes. All cybersecurity related systems, meaning all system which implement cybersecurity requirements or could influence the cybersecurity of the system need to have update capabilities. In addition, the system need to be able to recover from a failed update. Failed refers here to all conditions like an interruption of the update process or a corruption during transmission which result in an unsuccessful update. It is necessary to balance here between availability, recovering back to the original state, and security. Updates for high-risk vulnerabilities can indicate that no recovery is allowed, e.g. if the update is not successful the system is no longer usable. Although there are no restrictions on the technical means by which an update is delivered, there are requirements on how to release an update, e.g. the approval process and on the protection of the update during transport.

Directly related to the update topic is the End-of-Support (EoS). After End-of-Support there are no requirements to monitor for vulnerabilities and provide updates. Each partner in the supply chain needs to inform the next partner about the EoS for the systems in his responsibility. If the support is not ensured by another partner higher-up in the supply chain the customer needs to be informed (Fig. 6).

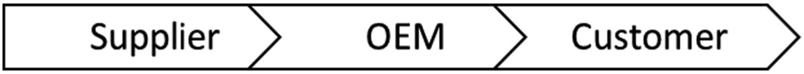

Fig. 6. End-of-Support communication

4.5 PG4 Process Overview and Interdependencies

Topics which are not directly related to a concrete cybersecurity activity, but which are nevertheless necessary for the achievement of cybersecurity are developed in PG4. An important topic addressed is the cybersecurity culture and cybersecurity management across the organization. The goal here is to define requirements and guidelines which will ensure that cybersecurity is accepted as a priority and quality attribute. It is similar in the direction and requirements to safety culture and safety management. A few examples for good and poor cybersecurity culture are given. Since cybersecurity is still a somehow new topic in the automotive domain confidence levels for cybersecurity capabilities are defined. These levels can be used to demonstrate evidence of cybersecurity in the supply chain. As an example, for incident response level 1 is reached if the responsible persons are defined. Level 2 is reached if policies are defined and accepted. Level 3 requires training and the ongoing evaluation of the policies based on training exercises.

The Development Interface Agreement (DIA) concept from ISO 26262, which is used to document responsibilities, information exchange and work share between supplier and OEM is included in an extended version. A template for the structure and the requirement to use RASIC [15] or similar models to define responsibilities tries to introduce more formalism. The concept can also be used in multiple lifecycle phase, not only during the engineering but even later during operation. For this additional Interface Agreements are introduced. Figure 7 gives an overview about described types of interface agreements. The idea was that different types can cover different stages of the lifecycle and parts, like for example the maintenance e.g. providing updates could also shifted from supplier to a third party.

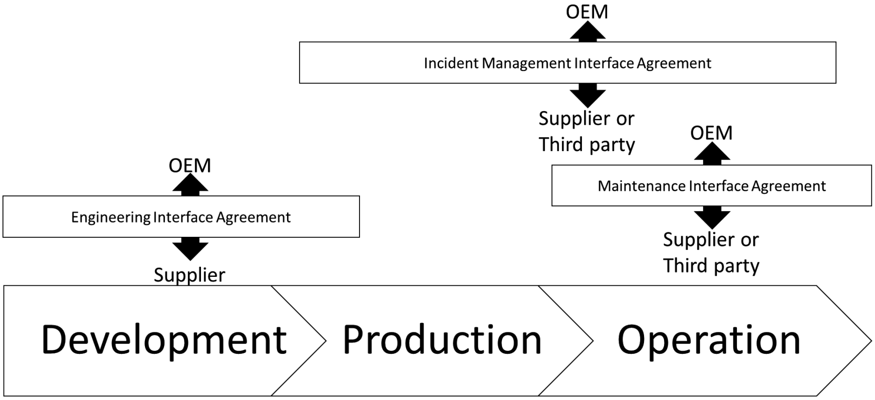
OEM
Incident Management Interface Agreement
Supplier or Third party
OEM
Maintenance Interface Agreement
Supplier or Third party
OEM
Engineering Interface Agreement
Supplier
Development
Production
Operation

Fig. 7. Different types of interface agreements

Also similar to the ISO 26262 safety element out of context (SEooC) is the definition of a cybersecurity element out of context (CEooC). The difference between a CEooC and a component of the shelf (COTS) is that a CEooC was defined with an automotive cybersecurity context in mind. In order to use a CEooC the main focus is therefore to ensure that the assumed context and the intended usage are overlapping. For a COTS it is also necessary to check which cybersecurity activities were carried out and identify missing steps which are necessary to achieve ISO/SAE 21434 compliance.

While requirements for cybersecurity auditing and assessment are already defined, there is still an ongoing discussion about the cybersecurity case. Such a case would document and collect all evidence to show that a system was developed in accordance with ISO/SAE 21434. Some existing guidance documents [16] suggest to provide such a documentation for auditing.

Annexes in PG4 describe also the high-level interaction between functional safety, IT-security and cybersecurity.

5 Summary and Outlook

Cybersecurity is increasingly becoming an important topic and there are multiple approaches to address this topic from governmental and legislative side [17, 18]. ISO/SAE 21434 has the potential to establish a common ground within the automotive industry to address cybersecurity challenges. With the current version the collection of topics is concluded. While this was a huge step, the time plan for the development of all topics is still rather short.

Some topics, like privacy and interaction between safety and security are still in discussion due to the time pressure. The goal is to have a first edition till May 2020 which includes the core topics. There are also dependencies between cybersecurity and system quality which could be detailed in the standard if there is sufficient time.

Since: (a) Cybersecurity is still a rather new topic for the automotive domain. (b) There is no common starting point like IEC 61508 [19] was for the development of functional safety for automotive. There are some topics which are accepted as relevant but without a known state of the art. Since a standard collect and codifies state of the art there are some topics which cannot be addressed. Nevertheless, based on the current status and development speed it is likely that the first version will be published in 2020.

References

1. International Organization for Standardization: ISO 26262:2011 Road vehicles - Functional safety (2011)
2. Fraunhofer Institute for Secure Information Technology: EVITA Project Summary, Deliverable D0 (2013)
3. Project Consortium, OVERSEE Final Event and Workshop on Concepts of Open In-Vehicle Platforms takes place on 19–20 December 2012 in Brussel, 12 December 2012. https://www.oversee-project.com/index.php%3Fid=17&tx_ttnews[tt_news]=37&cHash=aa04921e19dfc4094f0e2f71c6133bce.html. Accessed 22 Mar 2018

4. Weber, W., Hoess, A.: D13.7 – Final Report Part A - Publishable Summary, 15 August 2017
5. SAE: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (2016)
6. Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P.: Using SAE J3061 for automotive security requirement engineering. In: Skavhaug, A., Guiochet, J., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2016. LNCS, vol. 9923, pp. 157–170. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45480-1_13
7. Macher, G., Armengaud, E., Brenner, E., Kreiner, C.: Threat and risk assessment methodologies in the automotive domain. Procedia Comput. Sci. **83**, 1288–1294 (2016)
8. International Electrotechnical Commission: IEC 62443: Industrial communication networks – Network and system security
9. Johnson, C.: Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems (2016)
10. International Organization for Standardization: ISO 26262:2018 Road vehicles - Functional safety (FDIS) (2018)
11. Attacking the cybersecurity threat - SAE International. http://articles.sae.org/15208/. Accessed 27 Mar 2018
12. ISO/SAE AWI 21434 - Road Vehicles – Cybersecurity engineering. https://www.iso.org/standard/70918.html. Accessed 27 Mar 2018
13. International Standardization Organization: ISO 27000 series, Information technology - Security Techniques
14. International Standardization Organization: ISO 15408, Information technology - Security techniques - Evaluation criteria for IT security (Common Criteria) (2009)
15. Smith, M.L., Erwin, J., Diaferio, S.: Role & Responsibility Charting (RACI), p. 14 (2005)
16. Cybersecurity Best Practices for Modern Vehicles, National Highway Traffic Safety Administration, Washington DC, USA. Report No. DOT HS 812 333, October 2016
17. Markey, E., Blumenthal, R.: Security and Privacy in Your Car Act (2015)
18. United Nations Economic Commission for Europe (UNECE): UNECE Webseite (2018). https://www.unece.org/info/ece-homepage.html. Accessed 08 Mar 2018
19. International Electrotechnical Commission: IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems (2010)