ISO/SAE DIS 21434 Automotive Cybersecurity Standard - In a Nutshell

Georg Macher[1], Christoph Schmittner[2], and Omar Veledar[3] and Eugen Brenner[1]

[1] Institute of Technical Informatics
Graz University of Technology
{georg.macher,brenner}@tugraz.at
[2] Austrian Institute of Technology
christoph.schmittner@ait.ac.at
[3] AVL List GmbH
omar.veledar@avl.com

Abstract. A range of connected and automated vehicles is already available, which is intensifying the usage of connectivity features and information sharing for vehicle maintenance and traffic safety features. The resulting highly connected networking amplifies the attractiveness level for attacks on vehicles and connected infrastructure by hackers with different motivations. Hence, the newly introduced cybersecurity risks are attracting a range of mitigating strategies across the automotive field. The industry's target is to design and deliver safe and secure connected and automated vehicles. Therefore, efforts are poured into developing an industry standard capable of tackling automotive cybersecurity issues and protecting assets. The joint working group of the standardization organizations ISO and SAE have recently established and published a draft international specification of the "ISO/SAE DIS 21434 Road Vehicles - Cybersecurity Engineering" standard.
This document delivers a review of the available draft. This work provides a position statement for discussion of available analysis methods and recommendations given in the standard. The aim is to provide a basis for industry experts and researchers for an initial review of the standard and consequently trigger discussions and suggestions of best practices and methods for application in the context of the standard.

Keywords: ISO 21434, ISO 26262, automotive, security analysis.

1 Introduction

Prior to the introduction of connectivity features and automated driving functionalities, safety engineering was at the forefront of the automotive domain's priorities. Therefore, functional safety engineering methods and processes become industry standard and critical part of the development. Today, many connected and automated vehicles are available and connectivity features and information sharing is increasingly used for additional vehicle, maintenance and traffic safety features. This also increased the attractiveness of an attack on vehicles

by hackers with different motivations and thus introduces new risks for vehicle cybersecurity.

Consequently, new challenges regarding automotive cybersecurity have emerged; these in turn require additional efforts, engineering approaches and a very specific skill-set to deal with threats, risk management, secure design, awareness, and cybersecurity measures over the whole lifecycle of the vehicle. Well aware of this fact, the automotive industry has therefore taken high efforts in designing and producing safe and secure connected and automated vehicles. As the domain geared up for the cybersecurity challenges, they can leverage experiences from many other domains, but nevertheless, must face several unique challenges.

Automotive industry has recognized these requirements and therefore invested in the development of an industry standard to tackle automotive cybersecurity issues and protect their assets. The joint working group of the standardization organizations ISO and SAE has recently established a committee draft of the "ISO/SAE DIS 21434 Road Vehicles - Cybersecurity Engineering" standard [11]. From the point of view of the automotive industry, this standard achieves a common understanding of security by design in product development and along the entire supply chain.

This document is a review of the available draft. The aim of this work is to provide a position statement of the available draft, the presented analysis methods and recommendations given in the standard.

We further provide an overview of recommendations of the ISO/SAE DIS 21434 Road Vehicles - Cybersecurity Engineering standard regarding the mapping of cybersecurity processes in context of established processes. The aim of this work is to provide a basis for industry experts and especially researchers for an initial review of the standard. Based on this work we intend to trigger discussions on mapping and suggestions of best practices and methods for application in the context of the standard.

2 Established Safety and Security Frameworks

Safety and security engineering are tightly interlinked disciplines. They both focus on system-wide features and could greatly benefit from one another if adequate interactions between their processes are defined.

2.1 Safety engineering standards

Safety engineering is already an integral part of automotive engineering and safety standards, such as the road vehicles – functional safety norm ISO 26262 [10] and its basic norm IEC 61508 [7], are well established in the automotive industry. Safety assessment techniques, such as failure mode and effects analysis (FMEA) [8] and fault tree analysis(FTA) [9], are also specified, standardized, and integrated in the automotive development process landscape.

IEC 61508 Ed 2.0 provides a first approach of integrating safety and security; security threats are to be considered during hazard analysis in the form of a security threat analysis. However, this threat analysis is not specified in more

details in the standard and Ed 3.0 is about to be more elaborated on security-aware safety topics.

ISO 26262 Ed 2.0, which was published at the end of 2018, includes more recommendations for the interaction between safety and security. Based on a initial discussion on how to treat safety and cybersecurity in Automotive standardization, separate standards were published, but with a description of interactions. Annex E of ISO 26262:2018 delivers additional guidance on interactions. For the management, coordination of plans and milestones is suggested and field monitoring is also mentioned. During concept phase a focus is on the interaction between HARA and TARA and the coordination between countermeasures. In the development phase a focus is on consecutive analysis and the identification of potential impacts between the disciplines. The Annex is concluded with guidance on the interaction in the production phase.

2.2 Security engineering standards

The SAE J3061 [22] guideline is a predecessor of ISO/SAE 21434 and establishes a set of high-level guiding principles for cybersecurity by:

- defining a complete lifecycle process framework
- providing information on some common existing tools and methods
- supporting basic guiding principles on cybersecurity
- summarizing further standard development activities

SAE J3061 states that cybersecurity engineering requires an appropriate lifecycle process, which is defined analogous to the process framework described in ISO 26262. Further, no restrictions are given on whether to maintain separate processes for safety and security engineering with appropriate levels of interaction or to attempt direct integration of the two processes.

The guidebook also recommends an initial assessment of potential threats and an estimation of risks for systems that may be considered cybersecurity relevant or are safety-related systems, to determine whether there are cybersecurity threats that can potentially lead to safety violations. A report on the application of SAE J3061 was published [20].

While other standards, such as the IEC 62443 [1] or the ISO 27000 series [2] are not directly aimed at automotive systems, they are nevertheless relevant for the production and backend systems on automotive systems.

In [13] we reviewed available threat analysis methods and the recommendations of the SAE J3061 guidebook regarding threat analysis and risk assessment method (TARA) in context of ISO 26262 (2011) and SAE J3061. We provided an evaluation of available analysis methods together with a review of recommended threat analysis methods. Furthermore, we investigate systematic approaches to support the identification of trust boundaries and attack vectors for the safety- and cybersecurity-related aspects of complex automotive systems also in context of ISO 26262 (2011) and SAE J3061 in [14]. In the work of [15] we proposed a structured method for integrating security and safety engineering in the existing Automotive SPICE context.

Aside from this, in [18] we presented a first overview about the ongoing development and status of ISO/SAE 21434. Our working group presented ThreatGet, a new tool for security analysis, based on threat modelling [5] and a method for evaluating risk in cybersecurity, called RISKEE [12]. This method is based on attack graphs and the Diamond model [3] in combination with the FAIR method for assessing and calculating risk. In comparison to these works we update the overview to consider the ongoing development, review the current status regarding methodological guidance and give a first evaluation on integrating cybersecurity into established automotive processes.

In recent years, SafeComp workshops have started a discussion on automotive efforts taken in the context of designing and producing safe and secure connected and automated vehicles. With the focus on industry standards to tackle automotive cybersecurity issues and additional standards by European Telecommunications Standards Institute (ETSI) and International Telecommunication Union (ITU) working on security topics of connected vehicles [21]. Further activities of last years SafeComp also focus on presenting the method gaps and a proposal towards a solution to achieve coordinated risk management by applying a quantitative security risk assessment methodology [4].

3 ISO/SAE DIS 21434

In January 2016, the first guidebook for cyber-physical vehicle systems cybersecurity, SAE J3061 [22], was issued and marked the beginning of the cooperation between ISO and SAE to collaborate on the development of a cybersecurity standard for road vehicles in September 2016. The purpose of the fist standard to be created (ISO/SAE 21434 [11]) was to (a) define a structured process to ensure cybersecure design, (b) thus reducing the potential for a successful attack and reducing the likelihood of losses, and (c) provide clear means to react to cybersecurity threats consistently across global industry.

As already mentioned, ISO/SAE DIS 21434 [11] is intended for application to road-vehicles and focuses on setting minimum criteria for automotive cybersecurity engineering. In the standard neither specifics to cybersecurity technologies, solutions or remediation methods are given. Nor, are there unique requirements for autonomous vehicles or road infrastructure given. A risk-oriented approach for prioritization of actions and methodical elicitation of cybersecurity measures is encouraged.

3.1 ISO/SAE DIS 21434 Structure and Sections

Key principle focused by the ISO/SAE DIS 21434 [11] are cybersecurity activities of all phases of the vehicle life-cycle; ranging from design and development, production, operation and maintenance to decommissioning. In this section, the structure of the ISO/SAE DIS 21434 draft, depicted in 3.1, is analysed and briefly described before a more detailed description is given in the following sections of this work.

Section 1 defines the Scope of the norm.

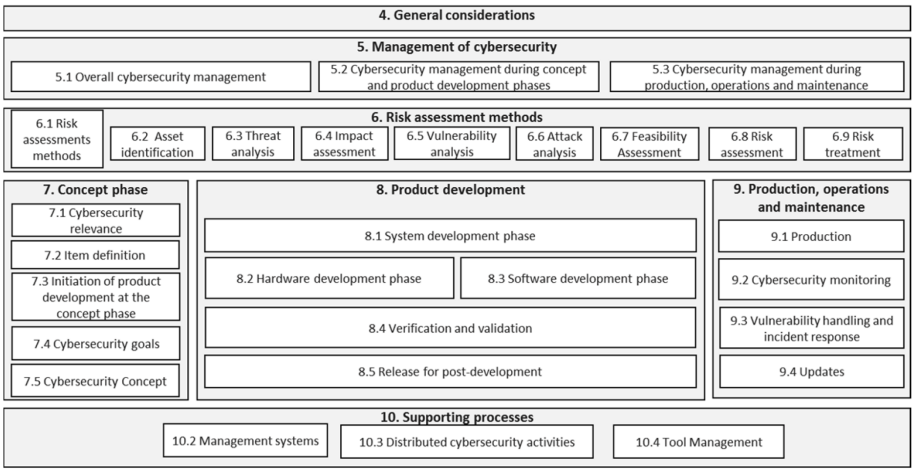

Fig. 1. Overview of the ISO/SAE DIS 21434 chapter structure [11]

Section 2 provides normative references.
Section 3 defines abbreviated terms and definitions of terms used in the document.
Section 4 is an *informative part* describing the vehicle ecosystem, organizational cybersecurity management and the related automotive lifecycle.
Section 5 includes descriptions regarding the organizational cybersecurity strategy, policy and objectives.
Section 6 defines risk management requirements, which includes a plan and method to determine the extent to which the road user is threatened by a potential circumstance or event.
Section 7 deals with the concept phase and defines cybersecurity goals, resulting from a threat analysis and risk assessment; as well as cybersecurity requirements definition to achieve the cybersecurity goals.
Section 8 specifies the implementation and verification of cybersecurity requirements specific to product development phase.
Section 9 is focusing on production, operation and maintenance phase and specifing requirements to ensure that the cybersecurity specifications are implemented in the produced item; also covering in-field cybersecurity activities.
Section 10 describes supporting processes, including organizational processes.
Annexes are also *informative parts* describing several activities, examples and methods which have not been agreed to be mandatory.

The sections 1, 2, and 3 define the Scope of the norm and abbreviated terms and definitions of terms used in the document on the first pages and are not further detailed in this work, since already introduced in the introduction section and more details do not provide additional added value.

3.2 ISO/SAE DIS 21434 Sections 4 - General considerations

This section informs of the vehicle ecosystem, organizational cybersecurity management and the related automotive lifecycle. In this context, automotive cybersecurity is defined, as concerning the protection of all assets in the vehicle against cybersecurity threats. Automotive cybersecurity thus considers (a) threats to the vehicle or its components and (b) threats to the ecosystem that compromise assets outside of the vehicle but utilize vulnerabilities within the vehicle. Additionally, a general organizational overview of cybersecurity management and the cybersecurity engineering lifecycle activities is provided.

3.3 ISO/SAE DIS 21434 Sections 5 - Management of Cybersecurity

The objective of this section is to:

a describe of the organizational objectives regarding cybersecurity and the organizational strategy to achieve these objectives
b the specification of organization-specific rules and processes to implement the organizational cybersecurity strategy
c assign responsibilities for cybersecurity engineering and the corresponding authority
d provide the resources needed
e foster a cybersecurity culture
f manage the competences and awareness needed to perform the cybersecurity activities
g apply continuous improvement
h perform an organisational cybersecurity audit
i manage interactions between cybersecurity processes.

Paragraph 5.1.4.7 details the interaction between cybersecurity processes and existing processes within the organisation. This section also states that effective communication channels between cybersecurity, functional safety, privacy and other disciplines that are related to the achievement of cybersecurity shall be maintained. This also includes communication between cybersecurity and functional safety engineering to exchange relevant information (e.g. threat and hazard information, violations of either cybersecurity goals or safety goals). In this context the SAHARA method [16] was intended with the same purpose.

Furthermore, paragraph 5.1.4.6 expresses the requirement of a cybersecurity audit, which shall be performed to independently judge whether the organizational processes achieve the process related objectives of this standard. This paragraph also states that the independence scheme can be based on Automotive SPICE, IATF 16949 in conjunction with ISO 9001, or ISO 26262.

Aside from this, general statements are given with regard to cybersecurity management during the concept phase and product development (paragraph 5.2) and during production, operation and maintenance (paragraph 5.3). Which also includes tailoring of cybersecurity activities for reuse (5.2.4.2.2), system or component out of context development (5.2.4.2.3) and off-the-shelf development (5.2.4.2.4).

3.4 ISO/SAE DIS 21434 Sections 6 - Risk assessment methods

This section is introduced with an informative risk assessment methods introduction paragraph (6.1), which generally deals with risk assessment on organisational level, but does not specify any specific risk assessment methods or does not propose approaches to be used.

Here the work of SafeComp2016 [13] analysed some possible TARA analyis methods for their applicability in the automotive context. Recently the work of Dobaj et al. [4] proposed a solution to achieve coordinated risk management by applying a quantitative security risk assessment methodology. This methodology extends established safety and security risk analysis methods with an integrated model, denoting the relationship between adversary and victim, including the used capabilities and infrastructure. This model is used to estimate the resistance strength and threat capabilities, to determine attack probabilities and security risks Other related works may be EVITA method [6], HEAVENS model, or the threat matrix approach. As mentioned initially, a method for evaluating risk in cybersecurity called RISKEE [12], is based on attack graphs and the Diamond model [3] in combination with the FAIR method for assessing and calculating risk. In terms of a structured threat analysis and threat modelling, the presented ThreatGet tool for security analysis [5] shall be mentioned.

Paragraph 6.2 deals with asset identification and thus focuses on (a) assets, (b) their security properties (e.g. CIA) and (c) damage scenarios (e.g. a safety, financial, operational or financial impact) in the event of the loss of their security properties. To that aim, candidate assets and potential damage scenarios shall be identified, and an impact analysis shall be performed on the potential damage scenarios; also here no specific methods or approaches are suggested.

In the following paragraphs the threat analysis (6.3), impact assessment (6.4), and vulnerability analysis (6.5) are depicted. The objective of the threat analysis is to identify threats scenarios that could potentially compromise the security properties of the item. The impact assessment in addition assess the impact or the extent of damage of a given damage scenario. The impact is defined as something that would be experienced or eventually sustained by the stakeholders (e.g. road users or businesses). While vulnerability analysis results in (a) a list of security vulnerabilities, (b) distinguish flaws and weaknesses and (c) attack paths that connect these security vulnerabilities to an attack.

Paragraph 6.6 describes the objective of attack analysis, which is to develop and/ or update a set of attack paths which could be exploited to realize a threat scenario. The assessment of the exploitability of these attack paths is subject of an attack feasibility assessment (described in paragraph 6.7).

Finally, the risk assessment (paragraph 6.8) and risk treatment (6.9) deal with classification of the identified threat scenarios (based on the impact and attack feasibility) and the selection of appropriate risk treatment options.

As already mentioned, dedicated methods or specific approaches are not mentioned in this normative part, but are mentioned in parts of the Annex.

3.5 ISO/SAE DIS 21434 Sections 7 - Concept Phase

This section of the norm determines if the system under development is cybersecurity relevant (paragraph 7.1), the item definition in cybersecurity context (7.2), and the initiation of product development at concept phase (7.3). It also includes, in alignment with the ISO 26262 approach, the definition of cybersecurity goals (7.4) and a cybersecurity concept (7.5). Here the link to the SAHARA method [16] shall be mentioned, which was one of the first methods to map the safety HARA analysis on the cybersecurity challenge.

The determination of the cybersecurity relevance of an item is not specifically mentioned, but Annex H provides a questionnaire that can be used to assess an item. The item definition and mining of cybersecurity goals is very much aligned with the safety-related approach known from ISO 26262 [10]. The cybersecurity concept consists, again as known from ISO 26262, of the cybersecurity requirements that achieve the cybersecurity goals along with their allocation at the appropriate level of architecture.

Also the cybersecurity concept contains a collection of cybersecurity requirements which achieve the cybersecurity goals in implementation-independent manner.

3.6 ISO/SAE DIS 21434 Sections 8 - Product development

This section of the standard describes the remaining product development phases. *System development* phase in paragraph 8.1, which can be linked to ISO 26262 part 4, *Hardware development* phase (paragraph 8.2), which can be linked to ISO 26262 part 5, and *Software development* phase (paragraph 8.3), which can be linked to ISO 26262 part 6. The additional paragraphs 8.4 is dealing with verification and validation and 8.5 is dealing with post-development release. In this context the work of Schmittner et al. [19] provides an FMEA application for security topics, called FMVEA.

Also different risk assessment activity types are mentioned at various stages in the system development but not detailed; at concept phase an assessment of the threats for the item and its operational environment and at system development phase an assessment of system specification vulnerabilities that cause residual risk and an assessment of system integration vulnerabilities that cause residual risk are done. Only mentioning, that system development shall be planned to identify methods and measures for system development and the cybersecurity activities.

Clause 8.1.4.2.2.3 mentions the following best practices of cybersecurity design:

1. Principle of least privilege
2. Authentication
3. Authorization
4. Audit
5. End to End Security
6. Architectural Trust Level (segregation of interfaces, defense in depth)

7. Segregation of interfaces (to allow proper cyber security analysis)
8. Protection of Maintainability during service (test interface, OBD)
9. Testability during development (test interface) and operations
10. Security by default (simplicity, non-obfuscation, no reliance on expert users)

Further, *system integration* shall be verified and tested by a combination of the proper methods, namely (a)requirement-based positive and negative testing, (b) interface testing, (c) penetration testing, (d) vulnerability scanning and (e)fuzz testing. For *hardware design*, the following mechanisms that ensure cybersecurity functionalities should be considered (clause 8.2.4.3.3):

- design cybersecurity domain (domain separation)
- self-protection of security functionalities
- protection against bypass of the security functionalities
- secure initialization of the security functionalities

Further, all physical and logical interfaces of hardware elements related to cybersecurity, shall be identified by their purpose, usage and parameters. Since interfaces are a potential entry point for cybersecurity attacks and should serve as an input to the vulnerability analysis, also mentioned in [17].

For cybersecurity related *software development*, software cybersecurity requirements have to be derived from the system cybersecurity requirements and allocated to software modules. Software unit design specifications and their implementations need to be verified statically and dynamically. Therefore, secure design rules and coding guidelines, domain separation, self-protection, non-bypass characteristics, and secure initialization definition shall be considered. Paragraph 8.3.4.6.5 states design principles for software unit design and implementation at the source code level. Including also the properties of (a) correct order of execution of subprograms and functions, (b) consistency of the interfaces, (c) correctness of data flow and control flow, (d) simplicity, readability and comprehensibility, and (e) robustness, verifiability and suitability for software modification. Regarding *verification and validation* most activities are described in Annex F.

3.7 ISO/SAE DIS 21434 Sections 9 - Production, operation and maintenance

This section deals with production (paragraph 9.1) to ensure that the cybersecurity specifications from development are implemented in the produced item and that the implement processes prevent the introduction of additional cybersecurity vulnerabilities. The cybersecurity monitoring (9.2), to have processes in place for gathering relevant cybersecurity information and review of cybersecurity information. Additionally, the handling and incident response (9.3) processes to present how to handle cybersecurity events and updating of basic cybersecurity requirements and capabilities are mentioned (9.4).

3.8 ISO/SAE DIS 21434 Sections 10 - Supporting processes

The processes described in this section shall support the cybersecurity activities and define interactions, dependencies and responsibilities between customers and suppliers. This includes management systems (paragraph 10.2), distributed cybersecurity activities (10.3) describing the relation between customer and suppliers and tool management (10.4). Although, there are no standard tools for development processes mentioned, a hint towards safety standards such as ISO 26262, IEC 61508, DO-178B is referred for tool qualification also of cybersecurity tools.

4 Review

A challenging task of the ISO/SAE 21434 committee was to create a brand new cybersecurity standard for the specifics of the automotive industry without building upon a wider variety of previous standards. While SAE J3061 was an important step forward, it was also recognized that this guidebook could not fulfil a similar role as was intended by ISO/SAE 21434, alike to ISO 26262, for the cybersecurity engineering of road-vehicles. The cybersecurity topic in the automotive context is a very new one and the ambition to provide a framework that includes requirements for cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders is aiming high. The fact, that this standard is not prescribing specific technology or solutions related to cybersecurity makes the descriptions of processes and approaches additionally ambiguous.

Another stated high aim is to provide clear means to react to cybersecurity threats consistently across global industry. That is rather challenging to achieve.A prominent example, is the CAL, a counterpart to the Automotive Safety Integrity Level (ASIL) from ISO 26262 during the risk assessment. The CAL should have be used to define rigorous and applicable methods, but since no consensus was found yet on how to determine and treat such a parameter, this part has also been moved to the Annex only. Thus, a risk-oriented approach for prioritization of actions and methodical elicitation of cybersecurity measures is encouraged, but no further added value in terms of best practices or agreed approaches is given.

In conclusion, the performed work is highly credited. The first common standard is an important and major step in the right direction, but in the context of a standard not all answers to questions related to methods, guidelines and best practices can (or are intended) to be provided. Thus, the aim, also of this work, is to share a bases for discussion and exchange between industry experts and researchers. Based on this, best practices and state-of-the-art methods for application in the context of the standard can be mined.

5 Conclusion

The joint working group of the standardization organizations ISO and SAE has recently established and published a draft of the "ISO/SAE 21434 Road Vehi-

cles - Cybersecurity Engineering" standard. With this standard, the goal was to provide a basis for an entire uniform cybersecurity development process in the automotive industry. The relevant aspects for product definition, design, implementation and testing with this standard have been described, but no specific implementation details or best practice approaches given.

Therefore, in this work we highlight the outcomes of this, currently draft standard and described how security standards, such as ISO/SAE 21434, are not the silver-bullet answer to applications in practice. Their state is often fragmented, or described at an abstract level for direct application in working environment and is not intended to provide answers to questions related to methods, guidelines and best practices.

Thus, one aim of this work is to provide a basis for industry experts and especially researchers for an initial review on the standard. The more important goal was to trigger discussions on mapping and suggestions of best practices and methods for application in the context of the standard and the domain. This work solely provided also some additional related work and was intended to provide a position statement for discussion, invite experts to get in contact and set/improve the state-of-the-art.

Acknowledgments

This work is supported by the *DRIVES* project. The Development and Research on Innovative Vocational Educational Skills project (*DRIVES*) is co-funded by the Erasmus+ Programme of the European Union under the agreement 591988-EPP-1-2017-1-CZ-EPPKA2-SSA-B.

References

1. IEC 62443: Industrial communication networks – network and system security.
2. ISO 27000 series, information technology - security techniques.
3. S. Caltagirone, A. Pendergast, and C. Betz. The diamond model of intrusion analysis. Technical report, Center For Cyber Intelligence Analysis and Threat Research Hanover Md, 2013.
4. J. Dobaj, C. Schmittner, M. Krisper, and G. Macher. Towards integrated quantitative security and safety risk assessment. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 102–116, Cham, 2019. Springer International Publishing.
5. M. El Sadany, C. Schmittner, and W. Kastner. Assuring compliance with protection profiles with threatget. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 62–73, Cham, 2019. Springer International Publishing.
6. O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger. Securing vehicular on-board it systems: The evita project. In *VDI/VW Automotive Security Conference*, page 41, 2009.
7. ISO - International Organization for Standardization. IEC 61508 Functional safety of electrical/ electronic / programmable electronic safety-related systems.

8. ISO - International Organization for Standardization. IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) , 2006.
9. ISO - International Organization for Standardization. IEC 61025 Fault tree analysis (FTA) , December 2006.
10. ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1-10, 2011.
11. ISO - International Organization for Standardization. ISO/SAE DIS 21434 Road Vehicles - Cybersecurity engineering, 2020.
12. M. Krisper, J. Dobaj, G. Macher, and C. Schmittner. Riskee: A risk-tree based method for assessing risk in cyber security. In *European Conference on Software Process Improvement*, pages 45–56. Springer, 2019.
13. G. Macher, E. Armengaud, E. Brenner, and C. Kreiner. A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In *Computer Safety, Reliability, and Security - 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 20-23, 2016, Proceedings*. Springer International Publishing, 2016.
14. G. Macher, R. Messnarz, A. Armengaud, Eric andRiel, E. Brenner, and C. Kreiner. Integrated Safety and Security Development in the Automotive Domain. In *SAE Technical Paper*. SAE International, 2017.
15. G. Macher, C. Schmittner, J. Dobaj, E. Armengaud, and R. Messnarz. An integrated view on automotive spice, functional safety and cyber-security. In *SAE Technical Paper*. SAE International, 04 2020.
16. G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner. SAHARA: A security-aware hazard and risk analysis method. In *Design, Automation Test in Europe Conference Exhibition (DATE), 2015*, pages 621–624, March 2015.
17. G. Macher, H. Sporer, E. Brenner, and C. Kreiner. An automotive signal-layer security and trust-boundary identification approach. *Procedia Computer Science*, 109:490 – 497, 2017. 8th International Conference on Ambient Systems, Networks and Technologies, ANT-2017 and the 7th International Conference on Sustainable Energy Information Technology, {SEIT} 2017, 16-19 May 2017, Madeira, Portugal.
18. C. Schmittner, G. Griessnig, and Z. Ma. Status of the development of ISO/SAE 21434. In X. Larrucea, I. Santamaria, R. V. O'Connor, and R. Messnarz, editors, *Systems, Software and Services Process Improvement*, volume 896, pages 504–513. Springer International Publishing.
19. C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security Application of Failure Mode and Effect Analysis (FMEA). In A. Bondavalli and F. Di Giandomenico, editors, *Computer Safety, Reliability, and Security*, volume 8666 of *Lecture Notes in Computer Science*, pages 310–325. Springer International Publishing, 2014.
20. C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, and P. Puschner. Using SAE j3061 for automotive security requirement engineering. In A. Skavhaug, J. Guiochet, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, volume 9923, pages 157–170. Springer International Publishing.
21. C. Schmittner and G. Macher. Automotive cybersecurity standards - relation and overview. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, and F. Bitsch, editors, *Computer Safety, Reliability, and Security*, pages 153–165, Cham, 2019. Springer International Publishing.
22. Vehicle Electrical System Security Committee. SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems.