A Preliminary View on Automotive Cyber Security Management Systems

Christoph Schmittner
AIT Austrian Institute of Technology GmbH

Jrgen Dobaj, Georg Macher, Eugen Brenner
Graz University of Technology

***Abstract*—Cyber security is increasingly recognized as an essential topic for automotive systems, especially in the area of connected and automated driving. Upcoming regulation defines requirements for cyber security on multiple levels in the automotive domain in order to achieve type approval. On the organizational level, a cyber security management system (CSMS) which covers the whole vehicle lifecycle and ecosystem is required. In addition, an argumentation for the cyber security of each vehicle type for which type approval is requested has to be given. Due to the novel nature of these requirements compared to existing type approval requirements, a test phase is ongoing. The components and scope of a CSMS are an open issue. We give an overview of the requirements for a CSMS, identify approaches and gaps, and give an outlook towards a potential framework which can address the requirements.**

***Index Terms*—Cyber Security Management System, CSMS, Automotive, Certification, Security**

I. Introduction

Vehicles are moving from isolated and mostly electromechanical systems towards connected computers with wheels [1]. This is currently driven by regulation and the wish of the automotive industry to offer additional services. Further steps towards partially and fully automated vehicle will only accelerate this trend. Goals like a further reduction of traffic accidents or energy reduction of traffic are only reachable with cooperative and automated vehicles [2]. In order to achieve safe, automated, and interacting vehicles, cyber security needs to be improved [3]. Recent evaluations and disclosures presented multiple vulnerabilities in almost all connected elements in current vehicles [4]–[6].

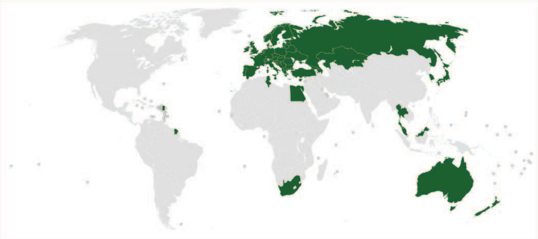

Fig. 1. Countries participating in the World Forum for Harmonization of Vehicle Regulations [7]

In order to ensure an increasing level of security the United Nations Economic Commission for Europe (UNECE) WP29 Working Party on Automated/Autonomous and Connected Vehicles (GRVA) started a Task Force on Cyber Security and software updates (CS/OTA) [8]. Figure 1 gives an overview of the 62 countries which are contracting states to the UNECE WP29 (Status 2016). Contracting state means that the Vehicle Type Approval [9], which is required to sell a vehicle, in these countries is based on the ECE regulations. We will focus here on Whole Vehicle Type Approval (WVTA). Figure 2 gives an overview about the vehicle type approval process.

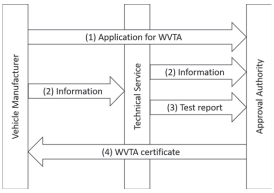

Fig. 2. Whole Vehicle Type Approval (WVTA) Process

The task force developed and delivered a recommendation for the integration of regulation on cyber security and software update for the type approval of vehicles [10], [11]. The recommendation on cyber security contains the following chapters

1) Introduction
2) Definitions (and abbreviations)
3) Cyber security principles
4) Threats to vehicle systems and ecosystem
5) Mitigations
6) Requirements for cyber security processes and how to evidence their application
7) Conclusion and recommendation for further proceedings
8) Annex A Draft proposal to introduce a Regulation on Cyber Security
9) Annex B List of threats and corresponding
10) Annex C List of Security Controls related to mitigations incl. examples
11) Annex D List of reference documents

Based on the delivered recommendation, there is currently a test phase ongoing. During this test phase, the requirements are evaluated and if necessary refined. In parallel guidance documents are developed.

In Section II we focus on *Requirements for cyber security processes and how to evidence their application* and *Annex A Draft proposal to introduce a Regulation on Cyber Security* to identify and analyze requirements on cyber security processes

978-3-9819263-4-7/DATE20/©2020 EDAA

in the automotive domain. Afterward, we give an overview of existing building blocks and open points for automotive cyber security in section III. In section IV, we present a starting point to define a CSMS compliant process, covering the complete lifecycle.

II. Requirements for cyber security processes and proposed regulation

The proposed requirements are divided into three sections. The first section describes the requirements of a Cyber Security Management System (CSMS) in the automotive domain. The next section describes requirements on the post-production phase, and the last section relates to the approval of a vehicle type. For the proposed regulation, there is a section describing the CSMS Certificate of Compliance, a section describing Requirements for the Cyber Security Management System, followed from a section on Requirements for vehicle types. We give in the following sections a summary of the requirements.

A. Cyber Security Management System

The cyber security management system is the overarching construct which collects all processes relevant for cyber security. A vehicle manufacturer has to ensure that suppliers and service providers implement a CSMS. The CSMS of the manufacture and his suppliers and service providers are assessed by an Approval Authority or Technical Service. While an Approval Authority or Technical Service can request a re-assessment at any point in time, the basic validity is three years. If there are changes which could impact the assessment, the vehicle manufacturer has to inform the Approval Authority or Technical Service. The processes defined in a CSMS have to include development, production, and post-production and consider the monitoring of risks and threats to the vehicle and incident response processes.

For the processes we need to differ between different definitions of lifecycle (see figure 3) in the automotive domain. For the UNECE regulation the lifecycle refers to the lifecycle of a vehicle type, e.g. from development to start of production to stop of production. If we look at ISO 26262 [12] and also SAE J3061 [13] the lifecycle is focused on the engineering of an system (element, component) which can be used in multiple vehicles. For a vehicle itself, we have the production, usage, and decommission lifecycles. In order to get type approval, e.g., to start production, an OEM needs to show that the organization and all involved supplier have a certified CSMS.

The processes need to ensure that security is sufficiently considered and include the following focus points:

- Management of cyber security in the organization
- Management (identification, assessment, categorization, and treatment) of risks to the vehicle type
- Verification of sufficient management of identified risks
- Security testing trough development and production
- Detection and response to cyberattacks on vehicle types
- Identification and management of new cyber threats and vulnerabilities of vehicle types
- Updates of the risk assessment

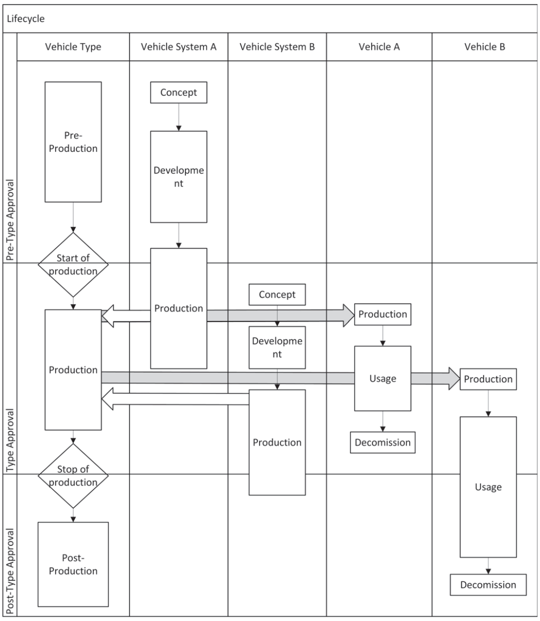

Fig. 3. Different lifecycles in the automotive domain

In addition, the vehicle manufacturer has to ensure that all processes work in the distributed development environment.

B. Post Production Phase

Requirements for the post-production phase are mainly a refinement of the requirements on CSMS to ensure that cyber security is integrated into the vehicle lifecycle. The vehicle manufacturer has to demonstrate how compliance with the regulation and protection is maintained through the vehicle lifecycle. This includes the monitoring of changes in the threat landscape and vulnerabilities. Implemented security measures need to be monitored for effectiveness. A focus is on ensuring that changing circumstances do not lead to an impact on safety and availability. In order to ensure this, incident response processes need to be in place.

C. Vehicle Types

A whole vehicle type approval can only be conducted if a certified CSMS is in place for OEM and all suppliers. The evidence for the whole vehicle type approval needs to include

- How known vulnerabilities and threats are considered in the risk assessment. The risk assessment needs to consider the whole vehicle, all vehicle systems, and their interactions.
- That elements, identified in the risk assessment as critical, are designed in a way and protected by suitable security measures so that the risk is reduced to an acceptable level. Elements include

  - Vehicle architecture and systems
  - Components and systems which are relevant to cyber security
  - Interactions between components and systems relevant to cyber security and other in-vehicle and external systems
- The tracing from identified risk to implemented mitigation to test result in order to demonstrate that all risks are sufficiently covered.

If the vehicle supports storage or execution of aftermarket software, services, applications, or data, a dedicated and protected environment needs to exist. The information required need to be collected through the full supply chain and verified.

III. State of the Art for Automotive cyber security frameworks

What the UNECE requires in a CSMS is a complete cyber security process framework, covering all activities relevant to the achievement of cyber security during the complete vehicle lifecycle. It has to cover all stakeholder potentially capable of influencing the cyber security. This framework should generate evidence of why cyber security for the vehicle is achieved.

While such a holistic framework is not yet existing, there are developed starting points. We will give in the next sections an overview about a) existing cyber security processes for the automotive domain and b) existing assurance approaches. In the process, we have to differ between

- processes for managing cyber security in development, production, and post-production
- processes addressing the distributed nature of the automotive domain

The first set of processes can be summarized as risk management processes, and the second part can be summarized as automotive supply chain management.

A. Automotive cyber security risk management

The generic risk management processes is presented in ISO 31000 [14]. Risk management is defined as the iterative process, which has to be executed through the complete lifecycle. A more detailed description for risk management on an organizational and system level is defined by NIST [15]. Both approaches cover, on a high level, the requirements for a CSMS risk management.

1) Risk identification: A well-known method for automotive risk identification is threat modeling [16]. It was shown that threat modeling could be used through the complete vehicle lifecycle [17] for risk identifications due to design weaknesses and potential threats and can even be used to monitor deployed systems for vulnerabilities. Recent approaches demonstrated how threat modeling could support the security testing process [18] and can also be used as a part of a combined methodology for safety and security [19], [20]. Threat modeling relies on up-to-date knowledge about the threat and cyber security landscape which includes monitoring of the overall threat landscape and also forensic capabilities for the vehicle.

2) Risk Assessment: For risk assessment, different methods exist, which are partially included in risk identification methods. A well-established approach is defined by the common criteria [21] which assess the attack probability. Attack probability can be tailored, depending on the available information and lifecycle phase. This was used as starting point for the the EVITA project [22] and in [20], [23]. In the HEAVENS project, a collection of risk identification and assessment methods was collected [24] and published. In the CySiVuS project a unified quantitative risk assessment for safety and security based on FAIR was developed [25].

3) Risk Categorization: Risk categorization is currently still an open topic. Existing approaches are [19] which classifies threats in safety-relevant or not safety-relevant. In [22] a classification in Safety, Financial, Operational and Privacy (SFOP) is proposed. Other approaches use automated approaches to classify risks [26].

4) Risk Treatment: Risk treatment includes all measures suitable to mitigate and reduce risks and the necessary steps to verify the effectiveness of applied measures. Defense-in-depth strategies [27] are a suitable starting point for the automotive domain. Based on this technical measures for risk treatment are mainly divided into four layers [28].

1) *Interfaces:* Modern vehicles possess a wide range of interfaces which can be used as potential attack surfaces [6]. The goal is to minimize the number of interfaces and to ensure that all interfaces are protected.
2) *Gateways:* Gateways are used to interconnect different bus systems [29] and therefore well suited to place additional security measures to isolate network parts and control access.
3) *Network:* Automotive vehicles use multiple internal communication systems, tailor-made for the respective performance and safety requirements [30]. Performance restricts the applicability cryptography solutions. Due to the predefined nature of machine to machine communication, intrusion detection systems are a good approach [31].
4) *Control Units:* Most approaches on securing control units are using hardware-based security, to ensure device integrity, isolation of critical functions, and enable protected storage [32]. Such approaches can also be used for tamper protection and to ensure secure boot.

Processes for risk management need to be integrated into the lifecycle to ensure that risk identification, assessment, and categorization is considered in the correct stages of the lifecycle and to ensure that risk treatment measures are implemented in a secure way.

5) Processes: For secure development, one of the first approaches was SAE J3061 [13], which was based on the process model defined by ISO 26262 [12]. ISO/SAE 21434 [33], [34] is a further development, a standard for cyber security engineering for automotive systems which is scheduled for publication in 2020.

In addition to these standards which focus mainly on the overall engineering process, IEC 62443 [35] is applicable for the production environment and NIST publications like [36] for key management. Also, secure coding guidance and guidance on how to use hardware-based security can be integrated.

B. Automotive cyber security supply chain management

Based on the UNECE requirements, the supply chain includes here not only the tiered structure of the automotive industry [37] but also the aftermarket.

For the interaction in the automotive domain approaches to ensure cyber security capabilities of suppliers can be based on existing capability and assessment schemes. As an example, an OEM can require his supplier to demonstrate information security for their systems based on a TISAX assessment [38] to ensure that critical information is protected [39]. A protected production environment can be demonstrated by assessing the environment based on IEC 62443 [35]. Automotive SPICE assessments, extend with security [40] can also be used to assess processes.

For the distribution of responsibilities and tasks, existing approaches from safety [12] can be used. The development interface agreement (DIA) was developed for distributed development of safety-critical systems. Similar interface agreements can be used to define responsibilities in the different phases of the vehicle lifecycle. As an example, the responsibility to monitor the evolving threat and vulnerability landscape could be addressed by an organization outside of the vehicle manufacturer. We see first approaches towards this with an organization like AUTO-ISAC [41]. Here also approaches on how to share information about incidents are important [42]. Figure 4 gives examples how different types of interface agreements could cover different phases of the lifecycle.

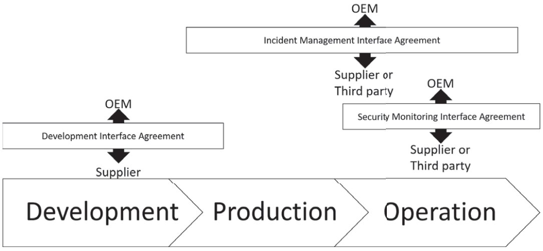
OEM
Incident Management Interface Agreement
Supplier or
Third party
OEM
Security Monitoring Interface Agreement
Supplier or
Third party
OEM
Development Interface Agreement
Supplier
Development
Production
Operation

Fig. 4. Examples for different interface agreements during the lifecycle

The management of an organization without a contractual relationship with a vehicle manufacturer is more challenging. Reverse engineering has shown that many currently available Android Auto infotainment apps include potential vulnerabilities [43]. Here the question is if a vehicle manufacturer can address this with a secure execution environment for third-party apps or if in addition, the system needs to be restricted to allow apps being tested by the vehicle manufacturer only.

A similar analysis [44] has shown that the diagnostic interface is a potential risk factor when a vehicle is visiting a repair shop. A proposal to address this is the extended vehicle concept [45]. The extended vehicle concept includes that access to vehicle data is controlled by an external organization which acts, depending on the implementation as a data clearinghouse or authentication authority. One challenge is here the potential conflict between security and controlled access with regulations on competition law [46].

C. Automotive cyber security assurance

Assurance, as defined by ISO/IEC/IEEE 15025-1, is ”grounds for justified confidence that a claim has been or will be achieved” [47]. This is done via an assurance case, consisting of a systematic argumentation and its supporting evidence and assumptions to demonstrate that a top-level claim is achieved. While ISO/IEC/IEEE 15025 gives a mathematical definition for the structure of an assurance case, there is also a benefit in graphical notations like GSN [48]. Both approaches have the challenge that there is a need to consider the evolving nature of cyber security, e.g., threat actor capabilities are increasing.

Evidence needs to show completeness and sufficiency of cyber security. Completeness shows that, based on the current state-of-the-art, all risks are considered. Sufficiency shows that the way risks are treated, is sufficient. Completeness can be shown by giving evidence that a systematic process was applied throughout the lifecycle. Evidence for sufficiency needs to show that risks are sufficiently treated. Assurance requirements for this can be taken form common criteria [21] and testing guidance from NIST [49]. Proposed techniques start by document reviews and include techniques for ongoing testing and assessment of systems already in use. For cyber security assurance, one challenge is to determine when the generated evidence is sufficient.

IV. CSMS Framework

As outlined in the previous Sections, there is a need for an overarching framework, covering the complete lifecycle and integrating development and operation. We propose a DevOps-approach that is suitable for structuring the process of development, production, and operation into one consistent framework. The proposed framework is based on previous work by Dobaj et al. [50], [51], and is structured into two main parts, as shown in Figure 5:

1) A *vehicle E/E architecture of the* 5^{th} *generation* [52], which first, enables the connection of vehicle systems to cloud systems for continues monitoring and second, provides the technical foundation to build a modular system architecture that can be easily updated and reconfigured [51].
2) On top of the modular E/E architecture, a *DevOps-lifecyle* can be set up to implement a continues improvement cycle. The *monitor and analyze processes* depict

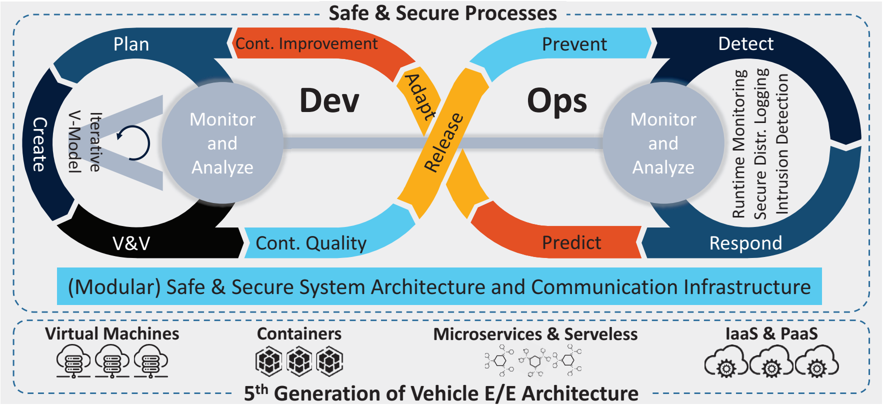

Fig. 5. Proposed DevOps framework covering the full vehicle lifecycle ranging from development, to production, to operation.

a core feature in this lifecycle, since these processes provide the foundation to detect failures and security incidents during both, development and operation.

As indicated by the V-Model in Figure 5, the proposed DevOps framework is compatible with traditional system development processes based on the V-Model. Both, a system development cycle as well as a system improvement cycle, are comprised of the same three major phases: planning, creation/implementation, and verification & validation (V&V). While development cycles are triggered by business needs, improvement cycles are automatically triggered by the *monitor and analyze processes*, whenever a failure or security incident is detected either in the V&V phase or during vehicle operation.

After a successful V&V phase, integration tests, fault-injection tests, and penetration tests are performed during the continues quality phase to guaranty system safety, security, and quality. In the subsequent release phase, code-signing and information security management are applied to provide a measure for ensuring system integrity within the distributed software deployment process. In the subsequent prevent phase, security is ensured by each vehicle individually. Anomalies are analyzed locally and transmitted to an external system for further investigation.

Whenever an incident or failure is detected during vehicle operation, the response phase forwards a report. This response is then processed and analyzed in the predict phase either manually by a human, or by automatic reasoning mechanisms such as proposed in [50]. The obtained result is forwarded to a failure or incident repository, which is part of the CSMS. This repository is frequently scanned in the adapt phase, and based on prioritization criteria, a reported failure or incident is selected to be investigated, which triggers the next continues improvement cycle.

V. Conclusion

We presented the challenge of upcoming cyber security regulation in the automotive domain and identified existing building blocks. For the overall structure of a CSMS, a DevOps-approach was introduced.

Open challenges are the mapping of building blocks to the DevOps process, e.g., a refinement of the process to include methods and activities. In addition, a distributed DevOps process is needed to consider the tiered structure of the automotive domain, and the upcoming regulation, not only on cyber security but also on software updates needs quality gates for certification. Certification depends on assurance, which needs to consider the distributed nature of automotive engineering and the evolving nature of cyber security.

Acknowledgment

The Afarcloud project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 783221. The JU receives support from the European Unions Horizon 2020 research and innovation programme. It is co-funded by the consortium members, grants from Austria, Germany, Belgium, Italy, Spain and Romania.

References

[1] C. Ebert and C. Jones, “Embedded software: Facts, figures, and future.,” *IEEE Computer*, vol. 42, no. 4, 2009.

[2] European Commission, “A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility,” 2016.

[3] Intel, “Safety First for Automated Driving,” 2019.

[4] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing, “Connected cars Threats, vulnerabilities and their impact,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, (St. Petersburg), pp. 375–380, IEEE, 2018.

[5] M. Ring, J. Durrwang, F. Sommer, and R. Kriesten, “Survey on vehicular attacks - building a vulnerability database,” in *2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, (Yokohama), pp. 208–212, IEEE, 2015.

[6] Charlie Miller and Chris Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” tech. rep., Black Hat 2015, 2015.

[7] Wikipedia, "World forum for harmonization of vehicle regulations." https://w.wiki/8tP, (accessed 2019-09-07).

[8] UNECE, "Task force on Cyber Security and (OTA) software updates (CS/OTA)." https://wiki.unece.org/pages/viewpage.action?pageId=40829521, (accessed 2019-09-07).

[9] W. Kerber and D. Moeller, "Access to data in connected cars and the recent reform of the motor vehicle type approval regulation," 2019.

[10] UNECE WP.29 GRVA, "Draft recommendation on cyber security of the task force on cyber security and over-the-air issues of unece wp.29 grva." https://wiki.unece.org/pages/viewpage.action?pageId=60362218, 2018-09-21 (accessed 2019-09-07).

[11] UNECE WP.29 GRVA, "DGRVA-01-xx (UN-CS_OTA) Final Draft Recommendation on Software Updates incl. Annex A-B." https://wiki.unece.org/pages/viewpage.action?pageId=60362218, 2018-09-21 (accessed 2019-09-07).

[12] ISO/TC 22/SC 32, "ISO 26262 Road vehicles - Functional safety," *ISO - International Standardization Organization*, 2018.

[13] SAE Vehicle Electrical System Security Committee and others, "Sae j3061-cybersecurity guidebook for cyber-physical automotive systems," *SAE-Society of Automotive Engineers*, 2016.

[14] ISO, "Risk management–principles and guidelines," *International Organization for Standardization, Geneva, Switzerland*, 2009.

[15] J. T. Force, "Risk management framework for information systems and organizations," *NIST Special Publication*, vol. 800, p. 37, 2018.

[16] A. Karahasanovic, P. Kleberger, and M. Almgren, "Adapting threat modeling methods for the automotive industry," in *Proceedings of the 15th ESCAR Conference*, pp. 1–10, 2017.

[17] Z. Ma and C. Schmittner, "Threat modeling for automotive security analysis," *Advanced Science and Technology Letters*, vol. 139, pp. 333–339, 2016.

[18] M. Wolf, "Combining safety and security threat modeling to improve automotive penetration testing," 2019.

[19] G. Macher, H. Sporer, R. Berlach, E. Armengaud, and C. Kreiner, "Sahara: a security-aware hazard and risk analysis method," in *Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition*, pp. 621–624, EDA Consortium, 2015.

[20] C. Schmittner, Z. Ma, and P. Smith, "Fmvea for safety and security analysis of intelligent and cooperative vehicles," in *International Conference on Computer Safety, Reliability, and Security*, pp. 282–288, Springer, 2014.

[21] "Common Methodology for Information Technology Security Evaluation - Evaluation methodology," Sept. 2012.

[22] A. Ruddle, D. Ward, B. Weyl, S. Idrees, Y. Roudier, M. Friedewald, T. Leimbach, A. Fuchs, S. Gürgens, O. Henniger, *et al.*, "Deliverable d2.3: Security requirements for automotive on-board networks based on dark-side scenarios," 2009.

[23] D. Dominic, S. Chhawri, R. M. Eustice, D. Ma, and A. Weimerskirch, "Risk assessment for cooperative automated driving," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, pp. 47–58, ACM, 2016.

[24] M. Islam, C. Sandberg, A. Bokesand, T. Olovsson, H. Broberg, P. Kleberger, A. Lautenbach, A. Hansson, A. Söderberg-Rivkin, and S. Kadhirvelan, "Deliverable d2-security models," *HEAVENS Project, Deliverable D*, vol. 2, 2014.

[25] T. Vogt, "Tool-chain enriched security development in automotive industry." Presentation at the 12th Graz Symposium Virtual Vehicle (GSVF), 05 2019.

[26] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transportation Research Part A: Policy and Practice*, vol. 124, pp. 523–536, 2019.

[27] Information Assurance Solutions Group, "Defense in depth.pdf," 2010.

[28] Andy Birnie and Timo van Roermund, "A multi-layer vehicle security framework," 2016.

[29] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty, "Security challenges in automotive hardware/software architecture design," in *Proceedings of the Conference on Design, Automation and Test in Europe*, pp. 458–463, EDA Consortium, 2013.

[30] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars*, Bochum, 2004.

[31] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, "Intrusion detection system for automotive controller area network (can) bus system: a review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 184, 2019.

[32] L. Chen, J. Franklin, and A. Regenscheid, "Guidelines on hardware-rooted security in mobile devices," tech. rep., National Institute of Standards and Technology, 2012.

[33] A. Barber, "Status of work in process on iso/sae 21434 automotive cybersecurity standard," *presentation, ISO SAE International*, vol. 10, 2018.

[34] C. Schmittner, G. Griessnig, and Z. Ma, "Status of the development of iso/sae 21434," in *European Conference on Software Process Improvement*, pp. 504–513, Springer, 2018.

[35] IEC, "Iec 62443 - security for industrial automation and control systems," *International Electrotechnical Commission*, 2018.

[36] E. Barker and W. Barker, "Recommendation for key management, part 2: Best practices for key management organizations (2nd draft)," tech. rep., National Institute of Standards and Technology, 2018.

[37] M. Broy, I. H. Kruger, A. Pretschner, and C. Salzmann, "Engineering automotive software," *Proceedings of the IEEE*, vol. 95, no. 2, pp. 356–373, 2007.

[38] O.-S. Goia *et al.*, "Tisax assessment for information security in the automotive industry," 2019.

[39] ISO, "Information technology security techniques information security management systems requirements," *International Organization for Standardization, Geneva, Switzerland*, 2013.

[40] G. Macher, A. Much, A. Riel, R. Messnarz, and C. Kreiner, "Automotive spice, safety and cybersecurity integration," 09 2017.

[41] A. ISAC, "Automotive information sharing and analysis center." https://www.automotiveisac.com/, (accessed 2019-09-23).

[42] C. Johnson, M. Badger, D. Waltermire, J. Snyder, and C. Skorupka, "Guide to cyber threat information sharing," tech. rep., National Institute of Standards and Technology, 2016.

[43] A. K. Mandal, A. Cortesi, P. Ferrara, F. Panarotto, and F. Spoto, "Vulnerability analysis of android auto infotainment apps," in *Proceedings of the 15th ACM International Conference on Computing Frontiers*, pp. 183–190, ACM, 2018.

[44] P. Kleberger, T. Olovsson, and E. Jonsson, "An in-depth analysis of the security of the connected repair shop," in *The Seventh International Conference on Systems and Networks Communications (ICSNC), Proceedings. Lisbon, 18-23 November, 2012. IARIA.*, p. 99, 2012.

[45] E. A. M. A. ACEA, "Safe and secure access to vehicle data." https://cardatafacts.eu/, (accessed 2019-09-23).

[46] M. McCarthy, M. Seidl, S. Mohan, J. Hopkin, A. Stevens, and F. Ognissanto, "Access to in-vehicle data and resources," 2017.

[47] I. ISO, IEC, "Systems and software engineering systems and software assurance part 1: Concepts and vocabulary." "https://www.iso.org/obp/ui/iso:std:73567:en", 2019.

[48] T. Kelly and R. Weaver, "The goal structuring notation–a safety argument notation," in *Proceedings of the dependable systems and networks 2004 workshop on assurance cases*, p. 6, Citeseer, 2004.

[49] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," *NIST Special Publication*, vol. 800, no. 115, pp. 2–25, 2008.

[50] J. Dobaj, J. Iber, M. Krisper, and C. Kreiner, "Towards Executable Dependability Properties," 2018.

[51] J. Dobaj, M. Krisper, and G. Macher, "Towards Cyber-Physical Infrastructure as-a-Service (CPIaaS) in the Era of Industry 4.0," 2019.

[52] W. Haas and P. Langjahr, "Cross-domain vehicle control units in modern E/E architectures," 2016.