A Survey on the Applicability of Safety, Security and Privacy Standards in Developing Dependable Systems

Lijun Shan[1], Behrooz Sangchoolie[2], Peter Folkesson[2], Jonny Vinter[2], Erwin Schoitsch[3], Claire Loiseaux[1]

[1] Internet of Trust, Paris, France
{lijun.shan, Claire.loiseuax}@internetoftrust.com
[2] RISE Research Institutes of Sweden, Borås, Sweden
{behrooz.sangchoolie, peter.folkesson, jonny.vinter}@ri.se
[3] Austrian Institute of Technology, Vienna, Austria
Erwin.schoitsch@ait.ac.at

Abstract. Safety-critical systems are required to comply with safety standards. These systems are increasingly digitized and networked to an extent where they need to also comply with security and privacy standards. This paper aims to provide insights into how practitioners apply the standards on safety, security or privacy (Sa/Se/Pr), as well as how they employ Sa/Se/Pr analysis methodologies and software tools to meet such criteria. To this end, we conducted a questionnaire-based survey within the participants of an EU project SECREDAS and obtained 21 responses. The results of our survey indicate that safety standards are widely applied by product and service providers, driven by the requirements from clients or regulators/authorities. When it comes to security standards, practitioners face a wider range of standards while few target specific industrial sectors. Some standards linking safety and security engineering are not widely used at the moment, or practitioners are not aware of this feature. For privacy engineering, the availability and usage of standards, analysis methodologies and software tools are relatively weaker than safety and security, reflecting the fact that privacy engineering is an emerging concern for practitioners.

Keywords: Safety, Security, Privacy, Standards, Dependable Systems

1 Introduction

In safety-critical industrial sectors such as automotive, rail and health, automated systems need to conform to safety criteria which are usually specified in the form of safety standards. For example, IEC 61508, titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems [1], is the basic functional safety standard applicable to many kinds of industry. As products in such domains are increasingly computerized, networked and personalized, they need to meet criteria on information security and user privacy which are specified by security and privacy standards.

Compared to safety standards, the practice of security and privacy standards in the industrial sectors is more recent. The practitioners, i.e. organizations who apply the

standards in developing products or services, face a wide scope of security/privacy standards originally targeted at IT systems. Meanwhile, new security/privacy standards for specific industrial sectors are emerging. Given various standards with different origins published by diverse standardization organizations, for the practitioners it is not obvious which standards are available or under development, which ones they should comply with, and what are the benefits of conforming to the standards. For the developers of the standards, it is also not evident how well the standards are accepted by the practitioners and other stakeholders.

The main objective of this paper is to provide new insights into practitioners' usage and perspectives regarding the standards on safety or security or privacy (Sa/Se/Pr). For this purpose, an empirical study has been conducted in the form of a questionnaire-based survey during the course of an EU ECSEL Joint Undertaking project called SECREDAS [2]. The project deals with product security and safety for dependable automated systems in the domains of automotive, railway and health. The consortium consists of 69 academic or industrial partners from 15 countries. Our questionnaire solicited their feedback on how they apply relevant standards, and how they employ analysis methodologies or tools in their daily work to meet Sa/Se/Pr criteria. With 21 valid responses, we conducted an analysis to answer a set of intended research questions.

The results of the survey, both qualitatively and quantitatively, can help practitioners, researchers, standardization bodies and other stakeholders to view the overall status of Sa/Se/Pr engineering of dependable automated systems. The qualitative result of our study is a wide spectrum of applicable standards, assessment methodologies and software tools. This result may help practitioners to perceive the state-of-the-art of both the Sa/Se/Pr criteria and the available engineering methods/tools to meet the criteria. The quantitative analysis reveals the practices of various standards, methodologies and software tools, which helps potential users of the standards/methods/tools to focus on the most influential ones. For the developers of the standards/methodologies/tools, the results indicate the effects of their work and the interests of the practitioners.

2 Research Method

This section presents the research questions, survey design, data collection and analysis, as well as the threats to validity of our survey.

2.1 Research Questions

The survey covers three inter-related themes on Sa/Se/Pr engineering: technical standards, analysis methodologies, and COTS (Commercial Off-The-Shelf) software tools. There are some overlaps between standards and methodologies, as certain standards refer to existing methodologies as guidance for performing specific activities. For example, SAE J3061 [3], titled Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, specifies a security engineering process for automotive systems. For security risk analysis, which is an iterative activity during the security engineering process, SAE J3061 recommends a number of applicable methodologies e.g. EVITA [4], TVRA [5], OCTAVE [6] and HEAVENS [7]. Nevertheless, such methodologies can be applied independent of the standard, and vice versa.

Within the scope of this paper, we formulated the following research questions (RQs).

- ***RQ1***. What standards are applicable for Sa/Se/Pr engineering of dependable systems and what are the differences (if any) between the availability of safety, security and privacy standards?
- ***RQ2***. How are the Sa/Se/Pr standards practiced?
- ***RQ3***. How do the practitioners follow the Sa/Se/Pr analysis methodologies?
- ***RQ4***. How do the practitioners employ Sa/Se/Pr engineering tools?

2.2 Survey Design

Our questionnaire consists of an introduction to the purpose of the study and 5 sections with 17 questions in total[1]. The standards under study are grouped into 8 categories according to the targeted industrial sectors and their subjects in terms of Sa/Se/Pr, as shown in Fig. 1, where "cross-domain" refers to the standards applicable to various industrial sectors. We excluded security boxes from the Rail and Health domains as security is only partially addressed in these domains.

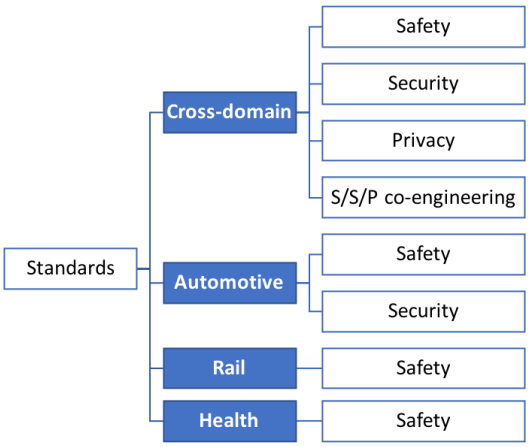

Fig. 1. Categories of the standards under study

2.3 Data Collection

The target population of the survey are SECREDAS participants, who conduct activities related to Sa/Se/Pr of automated systems in either or both of the following aspects:

a. Developing automated systems. For example, automotive OEM/Tier 1/Tier 2 companies and IT companies produce technologies, products or services for vehicles which need to meet Sa/Se/Pr requirements.

[1] The questionnaire could be found at:
http://www.internetoftrust.com/wp-content/uploads/2019/06/Secredas_Questionnaire_Standards_public.pdf

b. Providing supporting technologies, products or services. For example, research institutes conduct research on Sa/Se/Pr engineering methods or testing tools.

Fig. 2 shows the composition of the SECREDAS consortium and that of the respondents to our questionnaire. As shown in the figure, the major participants of SECREDAS are from academia, IT industry and automotive industry, so as the respondents to our questionnaire.

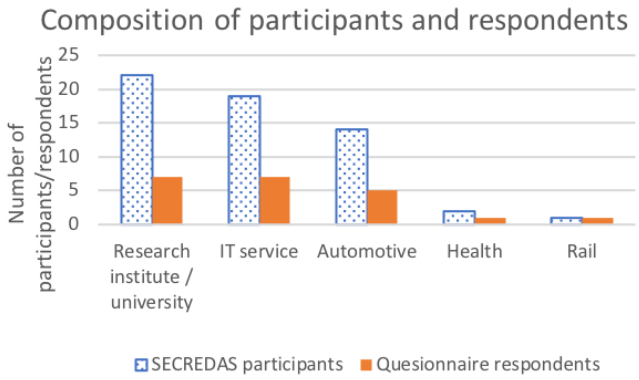

Fig. 2. SECREDAS consortium and respondents

The questionnaire was published and advertised in several plenary or group meetings of the SECREDAS project. To improve the readability of the questions, we conducted a pilot survey within five SECREDAS participants and revised the presentation of the questions following their feedback, before disseminating the questionnaire to the SECREDAS consortium. The survey data was collected from 05 Nov 2018 until 10 Feb 2019.

2.4 Threats to Validity

Construct validity. Construct validity refers to the question: does the test measure what it was meant to measure? Validity threats to our survey involve (i) the range of standards/methodologies/tools under study, and (ii) the provision of options in some questions. Concerning the range of the study, we enumerated typical standards/methodologies/tools which may be interesting to practitioners. The threat of providing incomplete lists was mitigated by allowing respondents to complement them with whatever they consider as relevant. Note that a respondent could not see the input from any other individual respondent. Typical options of answers were suggested to certain questions for helping respondents to understand the questions. The threat of providing an incomplete list of options was mitigated by allowing respondents to give any answer instead of restricting them to the given options.

External validity. External validity refers to the generalizability of the outcomes. The study is not meant to generalize its conclusion beyond its context. Seeing that the

SECREDAS participants are not equally distributed in the 4 industrial sectors, we do not seek to compare the practices of the standards between different domains.

3 Qualitative Analysis

To answer *RQ1*, this section presents the qualitative results, including a collection of applicable standards and a comparison between the availability of standards on safety, security and privacy.

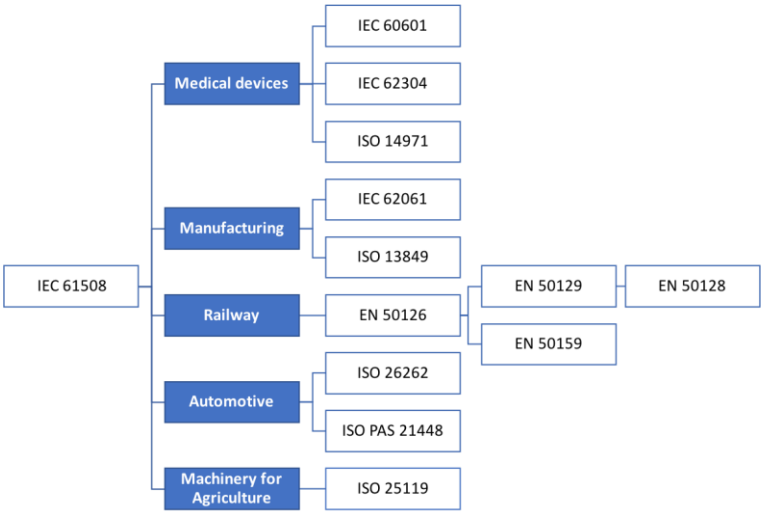

Fig. 3. Functional safety standards: given and complemented

Table 1. Security/privacy standards: given and complemented

	Given	***Complemented***
Cross-domain (Security)	• IEC 62443 [11] • ISO 2700X [12] • ISO 15408 [13] • NIST 800 [14]	• GlobalPlatform specifications [15] • ETSI TS 101 733 [16]903 [17] • ETSI TS 102 204 [18] • eIDAS Security Regulation [19] • RFC cryptographic [20] • TISAX VDA ISA [21] • ETSI TS 103 532 [22] • BSI Grundschutz [23]
Cross-domain (Privacy)	• ISO 29100 [24] • ISO 27550 [25]	• GlobalPlatform Privacy framework [26] • ISO/IEC 19286 [27] • GDPR [28] • Standard Data Protection Model [29]
Automotive (security)	• SAE J3061 [3] • ISO/SAE CD 21434 [9]	-

A set of functional safety standards have been published as variants of IEC 61508 [1] for specific industrial sectors. Fig. 3 shows those listed in the questionnaire plus ISO 25119 [8] which was supplemented by respondents.

Table 1 summarizes the security and privacy standards given in the questionnaire and those complemented by respondents. The table shows that compared to safety standards, security standards are less inter-related to one another and are published by more diverse standardization associations. A few security standards target specific industrial sectors, notably SAE J3061 [3] and ISO/SAE CD 21434 [9] for automotive. We observed that compared to the given standards which are on a higher level, some of the complemented standards are on a detailed specialized level. The table also shows that compared to safety and security standards, privacy standards are less numerous.

In the category of Sa/Se/Pr co-engineering, the questionnaire lists only one standard IEC TR 63069 [10] while no standard was supplemented by the respondents.

RQ1-Answer: Safety standards for specific industrial sectors are available, as specializations of one basic standard i.e. IEC 61508 [1]. A wider range of security standards from different origins are applicable, while few target specific industrial sectors. Privacy standards are less numerous than safety or security standards, and there is no privacy standard targeting specific sectors.

4 Quantitative Analysis

To answer *RQ2 - RQ4*, this section presents the results of our quantitative analysis on the received responses. The analysis focuses on the standards, analysis methodologies and tools enumerated in the questionnaire. We chose to leave the respondent-supplemented ones out of the quantitative analysis, because the information we obtained is too little to draw representative conclusions.

4.1 Practices of Standards

In the questionnaire, over each standard we posed the following three questions as the refinement of *RQ2*:

- ***RQ2.1*** Is the standard applied in the daily work? If YES:
- ***RQ2.2*** What is the motivation of applying the standard? Suggested options include:

  a. Required by regulation;
  b. Required by customer;
  c. As guidelines of product/service development.

- ***RQ2.3*** How is the conformance of the standard evaluated? Suggested options include:

  a. 3rd-party evaluation, e.g. qualification or certification;
  b. Self-evaluation.

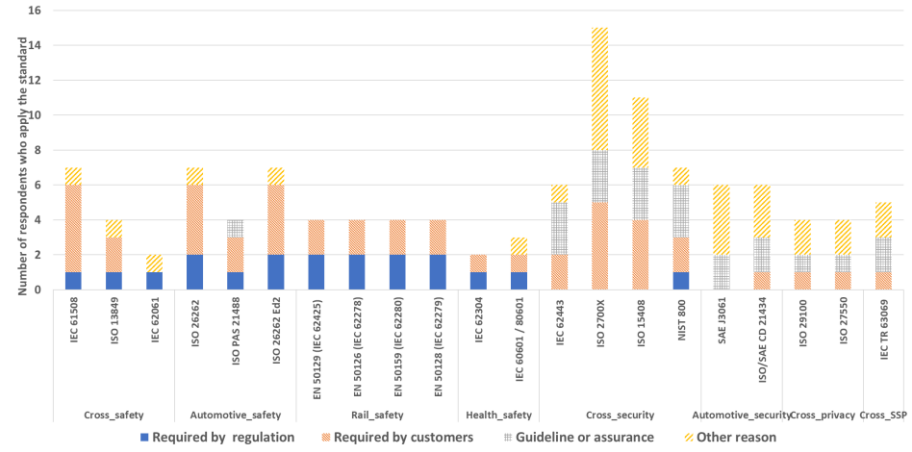

Fig. 4. Application of standards and the motivations

1) Application of standards and motivations. Fig. 4 presents our analysis result concerning questions *RQ2.1* and *RQ2.2*. The figure shows that cross-domain security standards ISO 2700X [12] and ISO 15408 [13] are the most applied ones.

In order to answer *RQ2.2*, we harmonized the answers so that each of them falls into one and only one of four disjoint groups, i.e. the three given options plus "other reason". As the questionnaire allows a respondent to give any answer to a question, within the responses who claim applying a certain standard, some select more than one motivation, while some select none of the suggested options. Note that the three suggested options reflect three levels of obligation, where "Required by regulation" is the most obligatory one and "As guidelines" is the least. We harmonized the answers to focus on the most obliging motivation for applying each standard, so as to reveal the role of each standard in Sa/Se/Pr engineering perceived by the practitioners. For example, Fig. 4 shows that 7 respondents apply IEC 61508 [1], where one is required at least by regulations, and five are by customers but not by regulations. It is worth noting that the basic safety standard IEC 61508 [1] and the automotive safety standard ISO 26262 [30] are not mandatory in a legal sense, but relevant in case of court rulings considering "Best Practices" and "State of the Art" as basis. Therefor they are de facto mandatory and required by customers on all tier x levels.

Fig. 4 reveals a difference between the motivation of conforming to the safety standards and that of the security/privacy standards. The two leading reasons for applying safety standards are firstly "Required by customers" and secondly "Required by regulation". Each of the safety standards is utilized by at least one respondent for complying with regulations. For security/privacy standards, in contrast, "Required by regulation" is rarely a reason, with only one exception of NIST 800 [14].

2) Evaluation of conformance to standards. Once an organization applies a standard, it may perform some activity to determine whether it complies with the requirements of the standard. Such activity can be either self-evaluation or 3rd-party evaluation, where the latter includes, but is not limited to, qualification and certification. Fig. 5

shows the result of *RQ2.3* on how the practitioners evaluate the conformance to the standards, where "No evaluation" represents the case where a respondent claimed applying a standard but did not choose any conformance evaluation. Here, similar to the analysis on *RQ2.2*, we harmonized the answers to *RQ2.3* by taking the strictest conformance evaluation within each answer. Hence each response who claims to apply a specific standard is placed into one and only one of the three groups in descending order of rigorousness: 3rd-party evaluation, Self-evaluation and No evaluation. Fig. 5 shows little difference on the employed conformance evaluation between the individual standards. However, "No evaluation" takes a significant proportion on security/privacy standards, which is not the case for safety standards.

3) Safety standards VS. security/privacy standards. The above analysis reveals that the practices of security/privacy standards are less mature than that of safety standards in terms of conformance evaluation. Also, the customers and authorities require less application of security/privacy standards than safety standards, possibly because they just started to perceive the importance of industrial products' conformance to security/privacy standards. These two observations reflect the fact that security/privacy are relatively new concerns to safety-critical industries.

Regarding Sa/Se/Pr co-engineering, IEC TR 63069 [10], the only standard positioned in this category in the questionnaire, is rarely practiced, probably because it is under publication first half of 2019 and hence less known to the practitioners. The result of this survey indicates that the multi-concern co-engineering challenge needs more consideration. Besides, standards are evolving with more concerns over Sa/Se/Pr co-engineering. The latest edition of safety standard IEC 61508 and that of ISO 26262 include requirements to think of cybersecurity if it impacts safety. These two standards are complemented by latest security standards IEC 62443 [11] and ISO/SAE CD 21434 [9], respectively. ISO/SAE CD 21434 [9] is already referenced in the draft regulation of UNECE for vehicle cybersecurity [31].

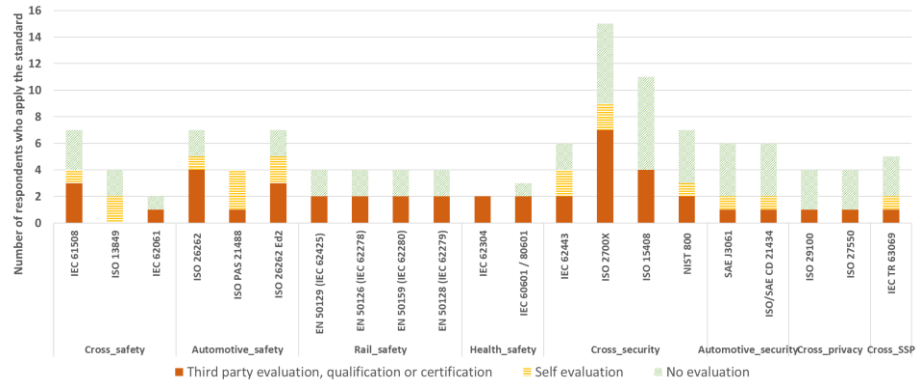

Fig. 5. Conformance evaluation with respect to the standards.

RQ2-Answer: On the application of standards, no significant difference is observed between individual Sa/Se/Pr standards. The conformance to safety standards is significantly more often imposed by customers and regulators than that of security/privacy standards. The conformance of safety standards is slightly more rigorously evaluated than that of security/privacy standards.

4.2 Practices of Analysis Methodologies

To evaluate the Sa/Se/Pr posture of a product/service or an organization, systematic assessment needs to be performed as an integrated and iterative activity throughout Sa/Se/Pr engineering. Our questionnaire investigates the practices of the methodologies which support such Sa/Se/Pr analysis. Fig. 6 shows the number of responses which claim using each methodology. For example, 8 respondents apply FMEA [32]. The figure shows that on safety, all the three methodologies listed in the questionnaire are almost equally used. The usage of different security analysis methods varies significantly. The usage of privacy analysis methodologies is minor, so as the combined Sa/Se/Pr analysis methodologies.

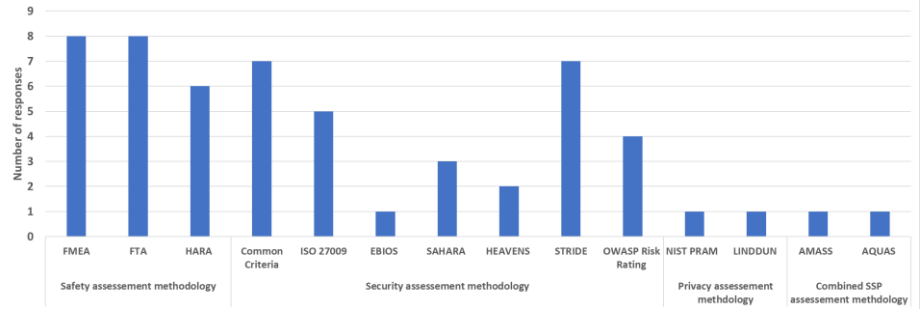

Fig. 6. Usage of safety, security or privacy analysis methods.

RQ3-Answer: Concerning safety analysis methodologies, FMEA [32], FTA [33] and HARA (Hazard Analysis and Risk Assessment) [30] are commonly used. Concerning security analysis methodologies, the STRIDE model [34] and the Common Criteria [35] are the most commonly used. The usage of security analysis methodologies is less convergent than of safety ones.

4.3 Usage of Commercial Off-The-Shelf (COTS) Tools

The survey investigates the practitioners' employment of COTS (Commercial Off-The-Shelf) tools for meeting Sa/Se/Pr requirements, and which properties each tool serves. Note that the questionnaire posed questions on two categories of tools: COTS tools and in-house tools, while only COTS tools are discussed in this paper for the sake of anonymizing the respondents.

Table 2 summarizes the software tools listed in the questionnaire and those complemented by respondents. The result of statistical analysis shows that about 38% of the respondents employ some tools to support safety engineering, and 24% for security engineering. Moreover, MathWorks Simulink and IBM Rational DOORS kit seem to be the tools that are used the most for both safety and security engineering. For privacy engineering, PTC integrity is the only tool used by only one respondent.

RQ4-Answer: MathWorks Simulink and IBM Rational DOORS kit are more used for safety and security engineering than the other tools. On privacy engineering, very few tools are available and applied in practices.

Table 2. Tools: given and complemented

Given	• Ansys SCADE code generators • Cadence Automotive Functional Safety IBM Rational DOORS kit • Mentor Graphics • Veloce • IBM Rational DOORS kit • Parasoft C/C++ test • LDRA tool suite • MathWorks Simulink
Comple-mented	• Enterprise Architect • Axivion Suite • Code Composer MISRA 2004 Coverity (static code analysis) • BugSeng ECLAIR • Git versioning system • HP Fortify Static code analyzer • ITEM Toolkit • Jenkins (unit testing) • Jira • Lauterbach Trace32 Debugger and Tracer • Medini • Microsoft Threat Modeling • Nexus IQ • PTC Integrity • Rational Clearquest (Defect tracking) • Tenable Nessus • Webinspect

5 Conclusion

To the best of our knowledge, there is little empirical study on the industrial sectors' practices of Sa/Se/Pr standards. The survey in this paper fills this gap by gathering feedback from the practitioners in real-world settings. Given that the sampling is not sufficient enough to be generalized, the observations we made from the responses are suggestive rather than definitive.

The analysis reveals that security/privacy standards are gaining popularity in safety-critical industrial sectors, though both their development and their practices are less mature than that of safety standards. Practitioners have more diverse options on the selection of security analysis methodologies, compared to that of safety analysis. Some COTS tools are applicable on Sa/Se/Pr engineering, where the availability and employment of tools for privacy engineering are still weak. Some standards linking safety and security engineering are not widely used, indicating that a multi-concern point of view for Sa/Se/Pr co-engineering is not yet widely adopted.

Note that this paper presents our observations over the responses without investigating their underlying reasons, because the limited number of responses does not facilitate a well-grounded further analysis. Some questions, for example, whether the age of a standard or the adoption by regulatory bodies can explain why some standards are more popular than others, remain interesting analysis angles for future work.

The survey described in this paper is part of a larger research effort aimed at devising an integrated Sa/Se/Pr evaluation framework for safety-critical systems. Another line of future research is to motivate practitioners to become more involved in standardization.

Acknowledgements. This work was partly supported by the SECREDAS project with the JU Grant Agreement number 783119, and the partners national funding authorities.

References

1. IEC61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems. Standard, International Electrotechnical Commission (IEC) (2010).
2. SECREDAS project. http://secredas.eu. Accessed 2019/04/03.
3. SAE J3061-2016 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Standard, Society of Automotive Engineers (SAE) (2016).
4. Henniger, O., Ruddle, A., Seudié, H., Weyl, B., Wolf, M., Wollinger, T.: Securing vehicular on-board IT systems: The EVITA project. In VDI/VW Automotive Security Conference (p. 41) (2009).
5. ETSI TS 102 165-1 V5.2.3 (2017-10) CYBER; Methods and protocols; Part 1: Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA). Standard, European Telecommunications Standards Institute (ETSI) (2017).
6. Alberts, C. J., Dorofee, A.: Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc. (2002).
7. HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS) project. https://research.chalmers.se/en/project/5809. Accessed 2019/04/03.
8. ISO 25119:2018 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems. Standard, International Organization for Standardization (ISO) (2018)
9. ISO/SAE CD 21434 Road Vehicles – Cybersecurity engineering. Standard, International Organization for Standardization (ISO), under development.
10. GlobalPlatform Specifications. https://globalplatform.org/specs-library/. Accessed 2019/04/03.
11. ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES). Standard, European Telecommunications Standards Institute (ETSI) (2013).
12. ETSI TS 101 903 V1.4.1 (2009-06) XML Advanced Electronic Sig- natures (XAdES). Standard, European Telecommunications Standards Institute (ETSI) (2009).
13. IEC 62443:2018 Security for industrial automation and control systems. Standard, International Electrotechnical Commission (IEC) (2018).
14. ETSI TS 102 204 V1.1.4 (2003-08) XML Advanced Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface. Standard, European Telecommunications Standards Institute (ETSI) (2003).
15. ISO/IEC 27000 family - Information security management systems. Standard, International Organization for Standardization (ISO) (2018).

16. eIDAS: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Regulation, The European Parliament and the Council of the European Union (2014).
17. ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security. Standard, International Organization for Standardization (ISO) (2015).
18. RFCs Internet cryptographic standards. Standard, Federal Information Processing Standards (FIPS).
19. NIST Special Publication 800-series. Standard, National Institute of Standards and Technology (NIST) (2018).
20. Trusted Information Security Assessment Exchange (TISAX). Standard, German Association of the Automotive Industry (VDA) (2017).
21. ETS ITS 103532 V1.1.1(2018-03) CYBER; Attribute Based Encryption for Attribute Based Access Control. Standard, European Telecommunications Standards Institute (ETSI) (2018).
22. BSI IT-Grundschutz. Standard, German Federal Office for Information Security (BSI) (2015).
23. GlobalPlatform Privacy Framework v1.0. Standard, GlobalPlatform (2017).
24. ISO/IEC 29100:2011 Information technology – Security techniques – Privacy framework. Standard, International Organization for Standardization (ISO) (2011).
25. ISO/IEC 19286:2018 Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services. Standard, International Organization for Standardization (ISO) (2018).
26. ISO/IEC PDTR 27550: Information technology – Security techniques – Privacy engineering. Standard, International Organization for Standardization (ISO), under development.
27. General Data Protection Regulation (GDPR). Regulation, European Parliament and Council of the European Union (2018).
28. Standard Data Protection Model (SDP Model). Standard, German Federal and State Commissioners (2017).
29. IEC TR 63069 ED1: Industrial-process measurement, control and automation - Framework for functional safety and security. Standard, International Electrotechnical Commission (IEC), under development.
30. ISO 26262:2018 Road vehicles – Functional safety. Standard, International Organization for Standardization (ISO) (2018).
31. Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA. Standard, United Nations Economic Commission for Europe (UNECE) (2018).
32. Stamatis, D. H.: Failure mode and effect analysis: FMEA from theory to execution. ASQ Quality press (2003).
33. Ericson, C. A.: Fault tree analysis. In: System Safety Conference, Orlando, Florida. Vol. 1, pp. 1-9 (1999).
34. Shostack, A.: Threat modeling: Designing for security. John Wiley & Sons (2014).
35. Common Criteria. https://www.commoncriteriaportal.org. Accessed: 2019/04/03.