A Survey on the Application of Safety, Security, and Privacy Standards for Dependable Systems

Lijun Shan
Internet of Trust
Paris, France
lijun.shan@internetoftrust.com

Behrooz Sangchoolie, Peter Folkesson, Jonny Vinter
RISE Research Institutes of Sweden
Borås, Sweden
{behrooz.sangchoolie, peter.folkesson, jonny.vinter}@ri.se

Erwin Schoitsch
Austrian Institute of Technology
Vienna, Austria
erwin.schoitsch@ait.ac.at

Claire Loiseaux
Internet of Trust
Paris, France
claire.loiseaux@internetoftrust.com

***Abstract*—Safety-critical systems are required to comply with safety standards as well as security and privacy standards. In order 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, we conducted a questionnaire-based survey. This paper summarizes our major analysis results of the received responses.**

***Index Terms*—safety, security, privacy, standards, dependable systems**

I. Introduction

In safety-critical industrial sectors such as automotive, rail and health, automated systems need to conform to safety criteria specified in safety standards, such as IEC 61508 [1]. As products in such domains are increasingly computerized, networked and personalized, they also need to meet criteria on information security and user privacy which are specified in security and privacy standards.

To gain insights into such practitioners' usage and perspectives regarding the standards on safety or security or privacy (Sa/Se/Pr), we conducted an empirical study in the form of a questionnaire-based survey[1] 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 sectors of automotive, railway and health. The consortium consists of 69 academic or industrial partners from 15 countries. The questionnaire was published via emails on 05 Nov 2018 and the survey data was collected since then until 10 Feb 2019. This paper summarizes our analysis results over the 21 received responses. Readers are referred to [3] for more details of the survey.

II. Research Method

The survey covers three inter-related themes on Sa/Se/Pr engineering of dependable systems: technical standards, evaluation methodologies, and COTS (commercial off-the-shelf) software tools. Within the scope of this paper, we formulated the following research questions (RQs):

- ***RQ1.*** What standards are applicable and is there any difference between the availability of safety, security and privacy standards?
- ***RQ2.*** How are the Sa/Se/Pr standards practiced?
- ***RQ3.*** Which methodologies are applied for Sa/Se/Pr evaluation?
- ***RQ4.*** Which tools are employed in Sa/Se/Pr engineering?

According to the targeted industrial sectors and the subjects, the standards under study are grouped into 8 categories: Cross-domain Safety, Cross-domain Security, Cross-domain Privacy, Cross-domain Sa/Se/Pr co-engineering, Automotive Safety, Automotive Security, Rail Safety, and Health Safety. Here cross-domain means applicable to various industrial sectors.

III. Analysis Results

The questionnaire listed typical standards in each of the 8 categories and requested respondents to supplement additional standards used in their daily work. The responses significantly enriched the lists of security and privacy standards. Concerning the availability of standards, the answer to *RQ1* is as follows.

> ***RQ1-Answer***: Safety standards for specific industrial sectors are available, as specializations of one basic standard IEC 61508 [1]. Security standards with different origins address different themes, while few are targeted to specific industrial sectors. Privacy standards are less numerous than safety/security standards, and there is no privacy standard targeted to specific sectors.

Concerning the application of standards, in the questionnaire the following three questions are posed over each standard as a 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: (i) Required by regulation;

This work was partly supported by the SECREDAS project with the JU Grant Agreement number 783119.

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

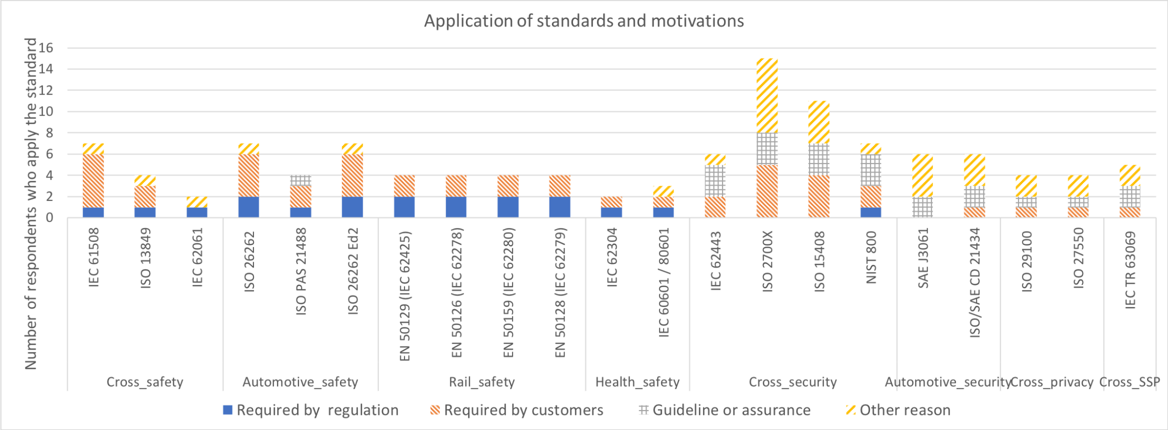

Fig. 1. Application of standards and the motivations

(ii) Required by customer; (iii) As guidelines of product/service development;

- ***RQ2.3*** How is the conformance of the standard evaluated? Suggested options include: (i) 3rd-party evaluation, e.g. qualification or certification; (ii) Self-evaluation.

We conducted quantitative analysis over the responses. For example Fig. 1 shows the analysis results regarding *RQ2.1* and *RQ2.2*. The overall answer to *RQ2* is as follows.

RQ2-Answer**:** ISO 2700X [4] and ISO 15408 [5] are the most applied standards among all the studied standards. The application of safety standards is significantly more often imposed by customers and regulators than that of security/privacy standards. The conformance to safety standards is slightly more rigorously evaluated than that of security/privacy standards.

Concerning the practitioners' employment of Sa/Se/Pr analysis methodologies and software tools, our analysis produced the following results. Here only COTS tools are discussed, while in-house tools are excluded for anonymizing the respondents.

RQ3-Answer**:** Among safety analysis methodologies, FMEA [6], FTA [7] and HARA (Hazard Analysis and Risk Assessment) [8] are commonly used. Among security analysis methodologies, the STRIDE model [9] and the Common Criteria [10] are the most commonly used ones. The usage of security analysis methodologies is less convergent than of safety ones.

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

IV. Conclusion

Our survey 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. 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. Concerning COTS tools, the availability and employment of tools for privacy engineering are still weak.

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 remain interesting analysis angles for future work, for example, whether the popularity of a standard is related to its age or the adoption by regulatory bodies, and whether the application of standards differs between different sectors.

References

[1] IEC 61508:2010 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] Lijun Shan, Behrooz Sangchoolie, Peter Folkesson, Jonny Vinter, Erwin Schoitsch, and Claire Loiseaux. A survey on the applicability of safety, security and privacy standards in developing dependable systems. In *14th International ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS) at SAFECOMP 2019, Turku, Finland*, 2019.

[4] ISO/IEC 27000 family - Information security management systems. Standard, International Organization for Standardization (ISO), 2018.

[5] ISO/IEC 15408:2009 Information technology – Security techniques – Evaluation criteria for IT security. Standard, International Organization for Standardization (ISO), 2015.

[6] Diomidis H Stamatis. *Failure mode and effect analysis: FMEA from theory to execution*. ASQ Quality press, 2003.

[7] Clifton A Ericson. Fault tree analysis. In *System Safety Conference, Orlando, Florida*, volume 1, pages 1–9, 1999.

[8] ISO 26262:2018 Road vehicles – Functional safety. Standard, International Organization for Standardization (ISO), 2018.

[9] Adam Shostack. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[10] Common Criteria. https://www.commoncriteriaportal.org. Accessed: 2019-04-03.