SECREDAS

Product Security for Cross Domain Reliable Dependable Automated Systems

DELIVERABLE REPORT D10.2

"State-of-the-art Analysis and Applicability of Standards"

Document Type	Deliverable
Document Number	D10.2
Primary Author(s)	Lijun Shan
Document Date	26/04/2019
Document Version / Status	v1.0
Distribution Level	Public
Reference DoA	30 April 2018

Project Coordinator	Patrick Pype, NXP Semiconductors, patrick.pype@nxp.com
Project Website	www.secredas.eu (in progress)
JU Grant Agreement Number	783119

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis

CONTRIBUTORS

Name	Organization	Name	Organization
Lijun Shan, Claire Loiseaux	Internet of Trust (IoTR)	Behrooz Sangchoolie, Peter Folkesson, Jonny Vinter	RISE Research Institute of Sweden (RISE)
Erwin Schoitsch	AIT Austrian Institute of Technology (AIT)	Alexander Vasenev, Andre Smulders	Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek (TNO)
Florian Stahl	AVL Software and Functions GmbH (AVL-SF)	Zhendong Ma	AVL List Gmbh (AVL-AT)
Thomas Furtner	Giesecke+Devrient Mobile Security GmbH (GD)	Alper Kocademir	Roche PVT GMBH (Roche PVT)
Respondents to the survey			

FORMAL REVIEWERS

Name	Organization	Date
Zhendong Ma (T10.2 leader)	AVL-AT	18/04/2019
Peter Folkesson (T10.4 leader)	RISE	24/04/2019
Erwin Schoitsch (WP10 leader)	AIT	24/04/2019
Roy Pennings (coordinator)	NXP	25/04/2019
Project Steering Board	N/A	

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
v0.1	03/04/2019	Lijun Shan	Draft version of document
v0.2	17/04/2019	Lijun Shan	Revision after reviews of WP10 partners
v0.3	19/04/2019	Lijun Shan	Revision after review of Zhendong Ma (T10.2 leader)
v0.4	25/04/2019	Lijun Shan	Revision after reviews of Peter Folkesson (T10.4 leader) and Erwin Schoitsch (WP10 leader)
v1.0	26/04/2019	Lijun Shan	Revision after review of Roy Pennings (coordinator)

Executive summary

Viewing standardisation as one major means of exploiting research results of projects in a sustainable manner, Work Package 10 (WP10) “Standardisation, Qualification & Certification” gathers partners’ needs, expertise and involvements in standardisation, qualification and certification work for multi-concern and multi-domain applications. The research in Task 10.2 “State-of-the-art survey of applicable security and safety standards and initiatives” aims to get insights into standards on automated systems and also on the possibilities to influence the evolution of standards. Deliverable 10.2 (D10.2) “State-of-the-art Analysis and Applicability of Standards” is a part of Task 10.2. The main body of this deliverable consists of two sections:

- Section 2 presents an overview of the Safety, Security and Privacy (Sa/Se/Pr) standards applicable to the domains of automotive, rail, and health. After a brief introduction to the development and usage of standards, a number of representative standards on safety, security and privacy are outlined, respectively.
- Section 3 describes a questionnaire-based survey on the applicability of the standards. The questionnaire was designed by Internet of Trust (IoTR) in collaboration with Austrian Institute of Technology (AIT), Research Institutes of Sweden (RISE), TNO and AVL. As a cross-WP work, this questionnaire provides input to not only Task T10.2, but also Task **T2.3** “Security and privacy reference architecture for safe automated systems” and Task **T10.1** “Survey of partners’ involvement in standardisation, use of standards and related activities”. This deliverable reports our analysis results of the 21 received responses from SECREDAS partners.

The results of the study reveal the state-of-the-art of Sa/Se/Pr engineering in terms of the development and practices of standards:

- **Availability of standards:** Safety standards for specific industrial sectors are available as specializations of the basic standard IEC 61508 [1]. A wider range of security standards are applicable while few are targeted to specific industrial sectors. Privacy standards are less numerous and none of them is targeted to specific sectors.
- **Practices of standards**: Security standards ISO 2700X [2] and ISO 15408 [3] are the most applied among all the studied Sa/Se/Pr standards. The practice of security/privacy standards is 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 should be a major concern of research in SECREDAS.
- **Analysis methodologies and software tools** employed in Sa/Se/Pr engineering: FMEA [4], FTA [5] and HARA [6] are commonly used safety analysis methods, and STRIDE [7] and Common Criteria [8] are the most commonly used security analysis methods. Among the COTS tools, MathWorks Simulink and IBM Rational DOORS kit are the most used for safety and security engineering. On privacy engineering, few tools are available and applied in practices.

Table of Contents

1 Background

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 functional safety standards. For example, IEC 61508 *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 also need to meet criteria on information security and user privacy which are specified by security and privacy standards. The practitioners face a wide scope of security/privacy standards which are 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 standardisation organizations, it is not obvious for the practitioners which standards are available or under development, which ones they should comply with, and what are the benefits of conforming to these standards. For the developers of the standards, it is also not evident how well the standards are accepted by the practitioners and other stakeholders.

This report provides a landscape on the applicable standards and their practices in the industry by addressing the following two questions:

(1) What safety, security or privacy (Sa/Se/Pr) standards are applicable to the automotive, rail and health domain?

(2) How are the standards practiced in the industrial sectors and under what motivation?

To answer the 1st question, we studied standardisation activities in general, and a set of typical standards in particular. To answer the 2nd question, we conducted an empirical study in the form of a questionnaire-based survey. The survey solicits the SECREDAS participants' feedback on their perspectives and practices with respect to standards, as well as their employment of analysis methodologies and COTS (commercial off-the-shelf) tools in Sa/Se/Pr engineering. Our analysis over the 21 received responses produces both qualitative and quantitative results. The qualitative result is a collection of applicable standards, methodologies and tools, which reinforces our answer to the 1st question with input of the respondents. The quantitative analysis reveals the most accepted standards and the underlying reasons, as well as the different maturity levels of safety, security and privacy engineering in terms of the development and application of standards.

2 State-of-the-art analysis of standards

This section overviews the Sa/Se/Pr standards applicable in the automotive, rail and health domain. The standards under investigation are those which specify Sa/Se/Pr criteria on automated systems or Sa/Se/Pr engineering processes. Section 2.1 explains how the standards are developed and used. Section 2.2 outlines the representative standards on safety, security and privacy, respectively.

2.1 How standards are developed and used

This section introduces general standardisation activities and basic concepts concerning the practices of standards.

2.1.1 Development of standards

A. Standardisation organizations

Many (inter)national standards concerning Sa/Se/Pr have been published by various standardisation organizations (SDOs). For example, the prestigious international organizations include:

- ISO (International Organization for Standardisation): An international SDO for worldwide technical, industrial and commercial standards.
- IEC (International Electrotechnical Commission): An international SDO for ICT (Information and Communications Technologies) standards.
- SAE (Society of Automotive Engineers): An US-based international SDO for automotive standards.

In Europe, CENELEC (electrical engineering), ETSI (telecommunications) and CEN (other technical areas) form the European system for technical standardisation.

- CENELEC (European Committee for Electrotechnical Standardisation, French: Comité Européen de Normalisation Électrotechnique): The European level SDO in the areas of IEC.
- ETSI (European Telecommunications Standards Institute): An SDO in the telecommunications industry (equipment makers and network operators) in Europe.
- CEN (European Committee for Standardisation, French: Comité Européen de Normalisation): The European level SDO in the areas of ISO.

In certain overlapping areas, e.g. Internet of things (IoT), Artificial intelligence (AI), Cloud computing and Security, there exist Joint Technical Committees or Coordination Groups, e.g. ISO/SAE JWG1 on

Automotive cybersecurity engineering and ISO/IEC JTC1. ISO/IEC JTC 1 is a joint technical committee of ISO and IEC, with the purpose to develop, maintain and promote standards in the fields of information technology (IT) and Information and Communications Technology (ICT). It has many subcommittees, including SC 41 IoT, SC 42 AI, SC 27 Security, cybersecurity and privacy protection, SC 38 Cloud computing and distributed platforms, etc.

B. Standardisation process

The standardisation organizations develop and publish standards following certain process. For example, ISO standards are developed by technical committees (TC) and subcommittees (SC) by a process with six steps, as summarized in Table 2-1.

Table 2-1: Stages in the development process of an ISO standard

Stage	Associated document name	Abbreviations
0 Preliminary	Preliminary work item	PWI
1 Proposal	New work item proposal	NP or NWIP
2 Preparatory	Working draft or drafts	• AWI (Approved new Work Item) • WD (Working Draft)
3 Committee	Committee draft or drafts	• CD • PDTR (Proposed Draft Technical Report) • PDTS (Proposed Draft Technical Specification)
4 Enquiry	Enquiry draft	• DIS (Draft International Standard) • FCD (Final Committee Draft), DTR, DTS
5 Approval	Final draft	• FDIS (Final Draft International Standard) • PRF (Proof of a new International Standard), • FDTR (Final Draft Technical Report)
6 Publication	International Standard	• ISO • TR (Technical Report), • TS (Technical Specification), • IWA (International Workshop Agreement)

Despite that the publications of the standardisation organizations are often simply called standards, these publications belong to different types. For example, the types of ISO publications [9] are summarised in Table 2-2.

Table 2-2: Types of ISO publications

Type	Description
International Standards (IS)	An IS provides rules, guidelines or characteristics for activities or for their results, aimed at achieving the optimum degree of order in a given context.
Technical Specification (TS)	A TS addresses work still under technical development, or where it is believed that there will be a future, but not immediate, possibility of agreement on an International Standard. The aim is that it will eventually be transformed and republished as an International Standard.
Technical Report (TR)	A Technical Report contains information of a different kind from that of the previous two publications. It may include data obtained from a survey, for example, or from an informative report, or information of the perceived "state of the art ".
Publicly Available Specification (PAS)	A PAS responds to an urgent market need, representing either the consensus of the experts within a working group, or a consensus in an organization external to ISO. PASs have a maximum life of six years, after which they can be transformed into an International Standard or withdrawn.
International Workshop Agreements (IWA)	An IWA is a document developed outside the normal ISO committee system to enable market players to negotiate in an "open workshop" environment. An IWA has a maximum lifespan of six years, after which it can be either transformed into another ISO deliverable or is automatically withdrawn.
Guides	Guides help readers understand more about the main areas where standards add value. Some Guides talk about how, and why, ISO standards can make it work better, safer, and more efficiently.

The title of an ISO publication indicates its type and its status in the development process by using the abbreviations shown in Table 2-2 and Table 2-1, respectively.

A similar process is followed in IEC. IEC also publishes IS (International standard), TS (Technical specifications) and TR (Technical report), with different rigidness concerning (mandatory) requirements. This is elaborated more in D10.1., Standardisation report.

2.1.2 Conformance to standards

Technical standards establish uniform engineering or technical criteria, methods, processes, and practices. Applying such standards helps to improve engineering methods or process of an organization by unifying the way of working, to improve the quality of products or services by making features of products measurable and comparable, and to facilitate certification and qualification of processes, products and systems.

The application of a standard can be driven by different motivations, e.g. required by customers, required by regulation, guideline for performance, assurance of quality of product/service, or as a marketing instrument in the case of non-obligatory standards. A standard can be applied in various activities, e.g. product/service development, research project, testing service, assessment service, consultancy service, and training.

In the case of applying some standards, there are different manners to evaluate the conformance to the standards. According to ISO[1]:

> *"Conformity assessment involves a set of processes that show your product, service or system meets the requirements of a standard. The main forms of conformity assessment are testing, certification, and inspection."*

Conformance evaluation can be self-evaluation or 3rd-party evaluation. The latter includes Qualification and Certification. Certification programs are operated by impartial third-party organizations called Certification Bodies (CB), who are accredited by an Accreditation Body (AB) or by public authorities to perform the auditing, assessment and testing work.

2.2 Overview of standards

This section summarises the Sa/Se/Pr standards applicable to automotive, rail or health.

2.2.1 Functional safety standards

According to IEC[2], ***Safety*** mean

> *"Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment."*

Automated systems become so complex that by a misbehaviour of their intended function, a safety issue will arise. Safety has to be ensured by an explicit design of electrical and electronic (E/E) elements to

[1] https://www.iso.org/conformity-assessment.html

[2] https://www.iec.ch/functionalsafety/explained/

prevent an unsafe situation caused by the system itself. Such E/E elements are called ***functional safety*** elements. According to IEC, ***functional safety***

> *"… is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the consequence of the hazardous event."*

Note that the definitions of *safety* and *functional safety* may slightly differ in different standards. The following two subsections outline the basic functional safety standard IEC 61508 [1] and its derivations for specific industrial sectors, respectively.

A. Basic Functional Safety standard: IEC 61508

IEC 61508 [1], titled "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)", is the basic functional safety standard applicable to various industry sectors. It specifies safety management throughout the entire life of a system, from initial conception to decommissioning. A fundamental principle of the standard is that safety requirements should be based on analysis of the risks posed by the equipment under control (EUC) and its control system. The standard defines the safety integrity level (SIL), which is "a discrete level (one of 4) for specifying the safety integrity requirements of safety functions". A risk assessment effort yields a target SIL for each safety function, based on a probabilistic value of acceptable risk.

IEC 61508 certification programs have been established by several global Certification Bodies, e.g. exida, TÜV Rheinland, TÜV Süd, TÜV Nord and RISE.

B. Variants of IEC 61508

Based on IEC 61508, a number of standards have been developed for specific industrial sectors, including:

- Automotive: ISO 26262 [6], titled "Road vehicles – Functional safety", is an international standard for functional safety of electrical and/or electronic systems in production automobiles.
- Railway applications: IEC 62279 [10], sometimes better known as EN 50128, titled "Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems", is intended to cover the development of software for railway control and protection including communications, signalling and processing systems.

- Process industries: IEC 61511 [11], titled “Functional safety - Safety instrumented systems for the process industry sector”, is a technical standard which sets out practices in the engineering of systems that ensure the safety of an industrial process through the use of instrumentation. The process industry sector includes many types of manufacturing processes, such as refineries, petrochemical, chemical, pharmaceutical, pulp and paper, and power.
- Machinery: IEC 62061 [12], titled “Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems”, provides requirements that are applicable to the system level design of all types of machinery safety-related electrical control systems and also for the design of non-complex subsystems or devices.

Other domain-specific standards derived from IEC 61508 do exist for the sectors of medical device, nuclear power, Programmable logical controllers. Some more details see D10.1.

2.2.2 Security standards

In contrast to the safety standards mentioned above which have the same root, security standards often have more varied origins and are published by more diverse standardisation organisations. The following subsections overview the security standards which are applicable to the domains addressed in SECREDAS.

A. Security management: ISO/IEC 27000 series

The ISO/IEC 27000 series [2] (also known as the “ISMS Family of Standards” or “ISO27K” for short) comprises information security standards. The series provides best practice recommendations on information security management - the management of information risks through information security controls - within the context of an overall Information security management system (ISMS).

The series is deliberately broad in scope, covering not only privacy, confidentiality and IT/technical/cybersecurity issues, but also human factors, organisational and physical measures. It is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information risks, then treat them (typically using information security controls) according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information risk and security, the ISMS concept incorporates continuous feedback and improvement activities to respond to changes in the threats, vulnerabilities or impacts of incidents.

B. Industrial automation and control systems: IEC 62443

IEC 62443 [13] is a series of standards including technical reports to secure Industrial Automation and Control Systems (IACS). Similar to the IEC 61508 [1] which defines safety lifecycle, IEC 62443 defines secure development lifecycle (SDL) requirements related to cyber security for products intended for use in the IACS environment, and also provides guidance on how to meet the requirements described for each element. Using the techniques described in IEC 62443, industrial stakeholders can assess the cybersecurity risks to each system and decide how to address those risks.

Similar to IEC 61508 [1] which defines safety levels, IEC 62443 defines five security levels (SLs) by the level of effort needed for a successful attack: from SL 0 (no security) to SL 4 (resistant against nation-state attacks). IEC 62443 identifies seven fundamental requirements (FR):

(1) Identification and authentication control (IAC)

(2) Use control (UC)

(3) System integrity (SI)

(4) Data confidentiality (DC)

(5) Restricted data flow (RDF)

(6) Timely response to events (TRE)

(7) Resource availability (RA)

IEC 62443 certification schemes have been established by several global Certification Bodies, including NIST (US), ENISA (EU), UL, exida, TÜV Rheinland, TÜV Süd, TÜV Nord, and SGS-TÜV Saar. Each has defined their own scheme or propose such schemes, based upon the referenced standards and procedures which describes their test methods, surveillance audit policy, public documentation policies, and other specific aspects of their program.

C. Security certification: ISO/IEC 15408 (Common Criteria)

The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) [8] provides a framework for defining and verifying security policies and security requirements of a product. This is adaptable for different levels of security called EALs (Evaluation Assurance Levels), ranging from EAL 1 (lowest level) to EAL 7 (highest level).

Common Criteria allows computer system users to specify their Security Functional Requirements and Security Assurance Requirements (SFRs and SARs respectively) in a Security Target (ST), which may be taken from Protection Profiles (PPs). Vendors can then implement or make claims about the security attributes of their products, and testing laboratories can evaluate the products to determine if they actually meet the claims. In summary, Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

D. Automotive: SAE J3061

Published in January 2016, J3061 [14] is the world's first automotive cybersecurity guidebook. It defines a risk-based, process-driven approach to address the cybersecurity threats the automotive environment is experiencing, and provides guidance on how to integrate cybersecurity into their product development lifecycle. Consistent with Process Framework for the vehicle functional safety standard ISO 26262 [6], SAE J3061 establishes relationships between cybersecurity and safety on multiple aspects:

(1) Comparison of scope: Scope of cybersecurity is broader. All safety-critical systems are cybersecurity-critical systems, but not all cybersecurity-critical systems are safety-critical.

(2) Integration of engineering processes: Potential communication paths between activities of safety engineering process and cybersecurity engineering process are specified.

(3) Analogies between engineering methods: The standard describes analogies between system safety and system cybersecurity engineering, e.g. TARA vs. HARA, Attack Tree Analysis vs. Fault Tree Analysis.

(4) Differences: The standard describes unique aspects of system safety and system cybersecurity, e.g. accidents or faults vs. purposeful malicious attacks.

Currently, there is no further development of SAE J3061 due to the fact that SAE is joining ISO on the development of ISO/SAE 21434, which is a cybersecurity engineering standard for road vehicle scheduled to be published at the end of 2020.

2.2.3 Privacy standards

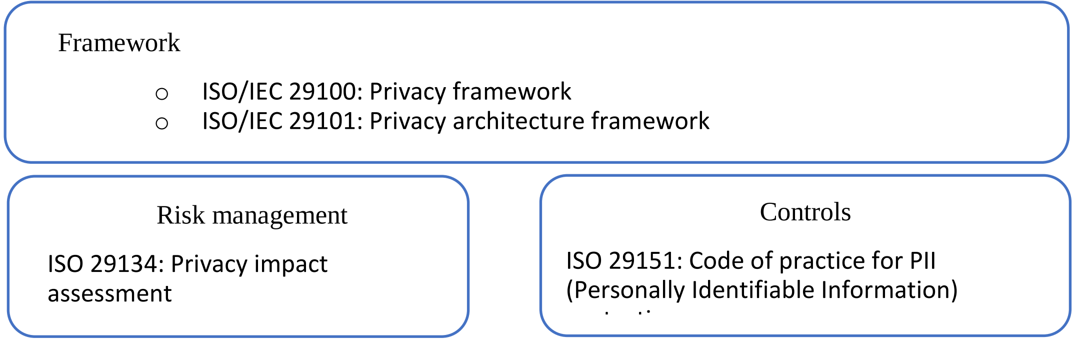
Framework
○ ISO/IEC 29100: Privacy framework
○ ISO/IEC 29101: Privacy architecture framework
Risk management
ISO 29134: Privacy impact assessment
Controls
ISO 29151: Code of practice for PII (Personally Identifiable Information)

Figure 2-3: Privacy standards

Information privacy is an emerging requirement on automated systems. Currently the major privacy standards are the ISO/IEC 29100 series, whose structure is illustrated in Figure 2-3.

A. ISO/IEC 29100 Privacy framework

In 2011, ISO developed the ISO/IEC 29100 [15] "Privacy framework" and ISO 29101 [16] "Privacy framework architecture" to provide a higher-level framework for securing Personally Identifiable Information (PII) with Information and Communication Technology (ICT) systems. Organizations can use these standards to design, implement, operate and maintain their ICT systems that will allow the protection of PII and improve organization's privacy programs through industry best practices.

ISO/IEC 29100 [15] provides a privacy framework which specifies a common privacy terminology. The standard:

(1) defines the actors and their roles in processing personally identifiable information (PII);

(2) describes privacy safeguarding considerations;

(3) and provides references to known privacy principles for information technology.

This framework should be used to protect personal information using specific controls to mitigate significant risks from the treatment.

B. ISO/IEC 29101 Privacy architecture framework

ISO/IEC 29101 [16] describes a high-level architecture framework and associated controls for the safeguarding of privacy in information and communication technology (ICT) systems that store and process personally identifiable information (PII). The standard:

(1) provides a consistent, high-level approach to the implementation of privacy controls for the processing of PII in ICT systems;

(2) provides guidance for planning, designing and building ICT system architectures that safeguard the privacy of PII principals by controlling the processing, access and transfer of personally identifiable information;

(3) and shows how privacy enhancing technologies (PETs) can be used as privacy controls.

ISO/IEC 29101 builds on the privacy framework provided by ISO/IEC 29100 to help an organization define its privacy safeguarding requirements as they relate to PII processed by any ICT system.

C. ISO/IEC 29134: Guidelines for privacy impact assessment

ISO/IEC 29134:2017 [17] gives guidelines for

(1) a process on privacy impact assessments, and

(2) a structure and content of a Privacy Impact assessment (PIA) report.

It is applicable to all types and sizes of organizations, including public companies, private companies, government entities and not-for-profit organizations. ISO/IEC 29134:2017 is relevant to those involved in designing or implementing projects, including the parties operating data processing systems and services that process PII.

D. ISO/IEC 29151: Code of practice for personally identifiable information protection

ISO/IEC 29151:2017 [18] establishes control objectives, controls and guidelines for implementing controls, to meet the requirements identified by a risk and impact assessment related to the protection of personally identifiable information (PII). ISO/IEC 29151:2017 is applicable to all types and sizes of organizations acting as PII controllers (as defined in ISO/IEC 29100), including public and private companies, government entities and not-for-profit organizations that process PII.

In particular, ISO/IEC 29151 specifies guidelines based on ISO/IEC 27002 [19], taking into consideration the requirements for processing PII that may be applicable within the context of an organization's information security risk environment(s).

3 Applicability of standards

To investigate the applicability of the standards, we designed a questionnaire with all participants of SECREDAS as the target audience. The questionnaire is given in the Appendix.

The questionnaire is a cross-WP work and a co-product of Internet of Trust (IoTR), Austrian Institute of Technology (AIT), Research Institutes of Sweden (RISE), TNO and AVL. Surrounding the theme of the practices of Sa/Se/Pr standards, the questionnaire addresses three interrelated topics of three tasks from WP2 and WP10, respectively:

- To provide input to task **T2.3** “Security and privacy reference architecture for safe automated systems”, questions are raised on the value chain of the partners (i.e. their major customers/clients) in order to get an overall picture of the ecosystems. The analysis of the answers addressing this aspect is mainly reported in the section “Business architecture” of deliverable **D2.3.1** “Reference Architecture”.
- To provide input to task **T10.1** “Survey of partners’ involvement in standardisation, use of standards and related activities”, questions are raised on the partners’ participation in standardisation activities. The analysis over the answers addressing this aspect is mainly reported in deliverable **D10.1** “Survey on partners’ involvement in and use of standards”.
- To provide input to task **T10.2**, the questionnaire solicits feedback on how practitioners apply the safety, security or privacy (Sa/Se/Pr) standards in the daily work, as well as how they employ Sa/Se/Pr analysis methodologies and software tools to meet such criteria. The analysis over the answers addressing this aspect is mainly reported in this section of **D10.2**.

In the following, we report the research method and the analysis results. The results of the survey can help practitioners, researchers, standardisation 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 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.

3.1 RESEARCH METHOD

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

3.1.1 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 [14], 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 [20], TVRA [21], OCTAVE [22] and HEAVENS [23]. Nevertheless, such methodologies can be applied independent of the standard, and vice versa.

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

- ***RQ1***. What standards are applicable for Sa/Se/Pr engineering of dependable automated systems and what are the differences (if any) between safety, security and privacy standardisation?
- ***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?

3.1.2 Survey design

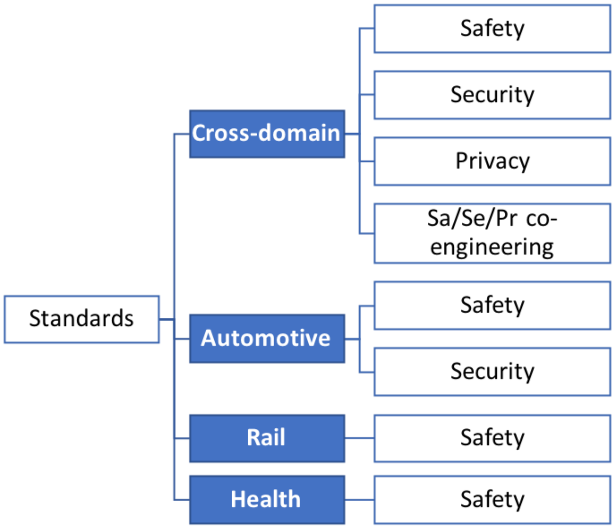

Figure 3-1: Categories of standards in the questionnaire

Our questionnaire consists of an introduction to the purpose of the study and 5 sections with 17 questions in total. The standards are grouped into 8 categories according to the targeted industrial sectors and their subjects in terms of Sa/Se/Pr, as shown in Figure 3-1, 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 today only partially addressed in these domains. It should be mentioned that evolving standards in these domains are addressing security aspects as well, similar to automotive and IACS.

3.1.3 Data collection

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

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

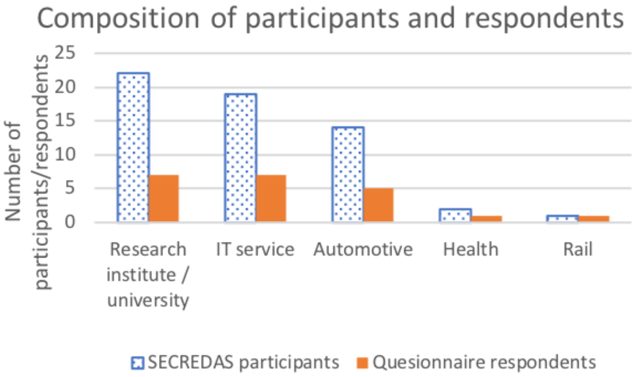

Figure 3-2: Compositions of SECREDAS consortium and respondents to questionnaire

Figure 3-2 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. Note that the five categories of SECREDAS participants shown in Figure 3-2 are not mutually exclusive in terms of their work domains, as research institutes/universities are also active in the domains of automotive, rail and health.

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.

3.1.4 Threats to Validity

Validity in qualitative research means "appropriateness" of the tools, processes, and data. Whether the research question is valid for the desired outcome, the choice of methodology is appropriate for answering the research question, the design is valid for the methodology, the sampling and data analysis is appropriate, and finally the results and conclusions are valid for the sample and context [24]. Validity threats are potential risks that are involved in the design and execution of empirical studies [25].

A. 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 of standards/methodologies/tools was mitigated by allowing respondents to complement the lists with whatever they consider as relevant. Typical options of answers were suggested to certain questions, to help respondents to understand the questions. The threat of providing an incomplete list of options was mitigated by allowing respondents to give any answer to any question instead of restricting them to the given options.

B. 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.

3.2 QUALITATIVE ANALYSIS

To answer RQ1, this section presents the qualitative results with a focus on the applicable standards, including both the ones enumerated in the questionnaire and the ones complemented by the respondents.

A set of functional safety standards have been published as variants of IEC 61508 [1] for specific industrial sectors. Figure 3-3 shows those listed in the questionnaire plus ISO 25119 [26] which was supplemented by respondents. Note that this list is not comprehensive. Some safety standards are not explicitly listed but are used in industry, e.g. IEC 61511 [27], EN 50657 [28].

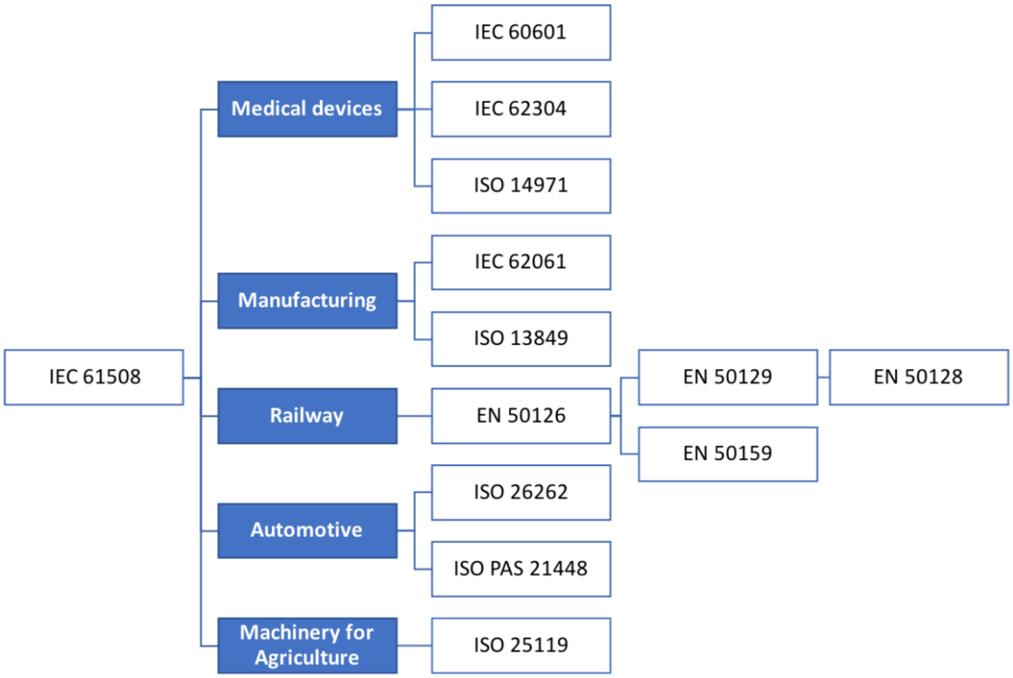

Figure 3-3: Safety standards

Table 3-4: Security/privacy standards: given and complemented

	Given	Complemented
Cross-domain (Security)	• IEC 62443 [13] • ISO 2700X [2] • ISO 15408 [3] • NIST 800 [29]	• GlobalPlatform specifications [30] • ETSI TS 101 733 [31] • ETSI TS 101 903 [32] • ETSI TS 102 204 [33] • eIDAS Security Regulation [34] • RFC cryptographic standards [35] • VDA TISAX [36] • VDA ISA [37] • ETSI TS 103 532 [38] • BSI Grundschutz [39]
Cross-domain (Privacy)	• ISO 29100 [15] • ISO/IEC PDTR 27550 [40]	GlobalPlatform Privacy framework [41] ISO/IEC 19286 [42] GDPR [43]

		Standard Data Protection Model [44]
Automotive (Security)	• SAE J3061 [14] • ISO/SAE CD 21434 [45]	/

Table 3-4 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 standardisation associations. A few security standards are targeted to specific industrial sectors, notably SAE J3061 [14] and ISO/SAE CD 21434 [45] for automotive. We observed that compared to the given standards which are on a higher level, some of the standards complemented by the respondents 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 [46], and no standard was supplemented by the respondents. Besides, existing standards are evolving towards Sa/Se/Pr co-engineering. In IEC 61508 Edition 2 (2010), a requirement to think of cybersecurity if it impacts safety was included. IEC 62443 [13] is the complementary security standard to IEC 61508 in Industrial Automation and Control Systems.

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 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.

3.3 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.

3.3.1 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:
  - (i) Required by regulation;
  - (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.

A. Application of standards and motivations

Figure 3-5 presents our analysis result concerning questions RQ2.1 and RQ2.2. The figure shows that cross-domain security standards ISO 2700X [2] and ISO 15408 [3] 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, Figure 3-5 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.

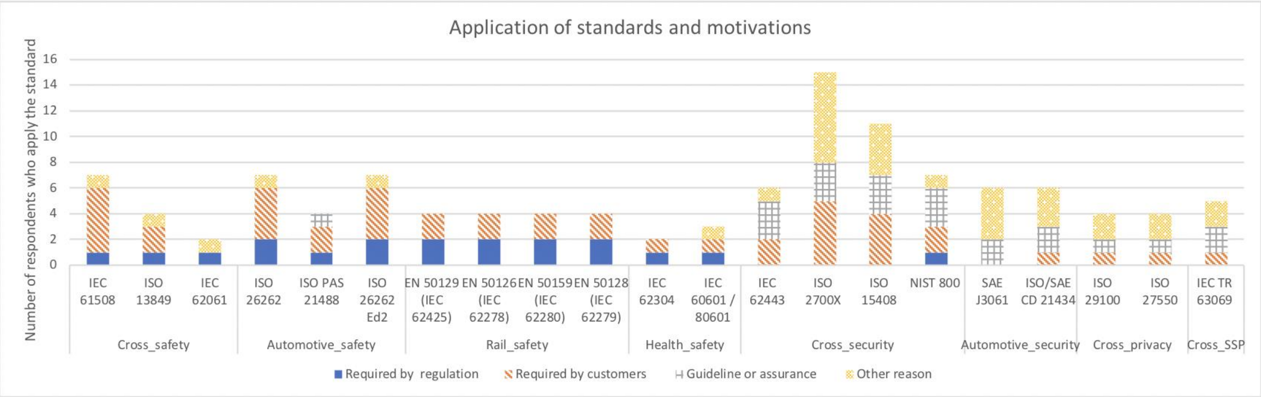

Figure 3-5: Application of standards and motivations

From a legal point of view, regulations are mainly in effect for the railway and the aircraft domain, or enforced by European Directives e.g. in domain of machinery and medical devices. The basic safety standard IEC 61508 [1] and the automotive safety standard ISO 26262 [6] 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 *da facto* mandatory and required by customers on all tier x levels. Not all respondents seem to have had a clear view on this issue.

Figure 3-5 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 [29]. *Guidelines or assurance* and *Other reasons* dominate for security/privacy standards. A common motivation for using Sa/Se/Pr standards is *Required by customers*, except for SAE J3061 and IEC 62061.

B. 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. Figure 3-6 shows the analysis 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*. Figure 3-6 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.

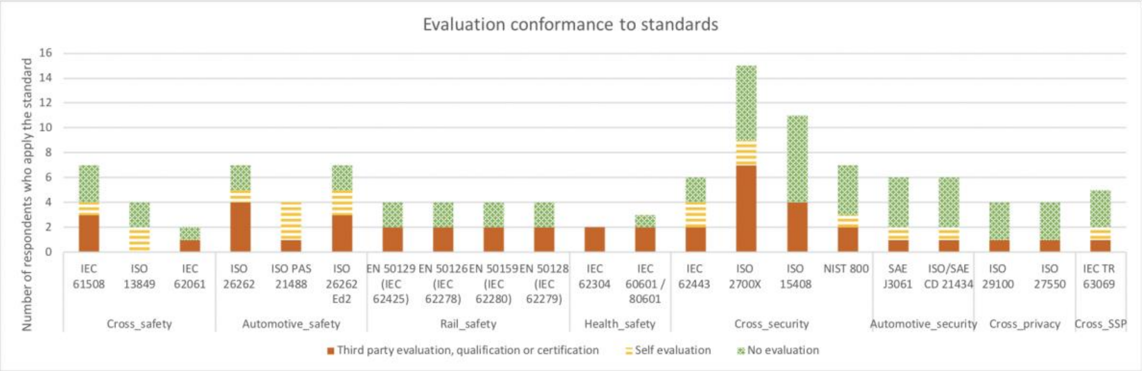

Figure 3-6: Evaluation conformance to standards

C. 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 [46], the only standard in the category of "Sa/Se/Pr co-engineering standards" in the questionnaire, is rarely practiced, probably because it is under publication first half of 2019. This standard is only well known to the partner active in this standardisation committee IEC TC65 WG20, and less known to general practitioners. The result of this survey indicates that the multi-concern co-engineering challenge needs more consideration, which could give some direction to the research work in SECREDAS in this respect.

Besides, standards are evolving towards Sa/Se/Pr co-engineering. The latest versions of the basic safety standard IEC 61508:2010 [1] and automotive safety standard ISO 26262:2018 [6] include requirements to consider cybersecurity throughout the lifecycle, if cybersecurity has impact on safety as result of the risk/hazard analysis. These two standards did not prescribe concrete countermeasure, and left it to security standards IEC62443 [13] and ISO/SAE 21434 [45]. IEC 61508 is complemented by security standards IEC 62443 [13] , and ISO 26262 is by the evolving ISO/SAE CD 21434 [45], respectively. ISO/SAE CD 21434 is already referenced in the draft regulation of UNECE for vehicle cybersecurity [47], which will be the future basis for road vehicles approval.

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.

3.3.2 Practices of analysis methodologies

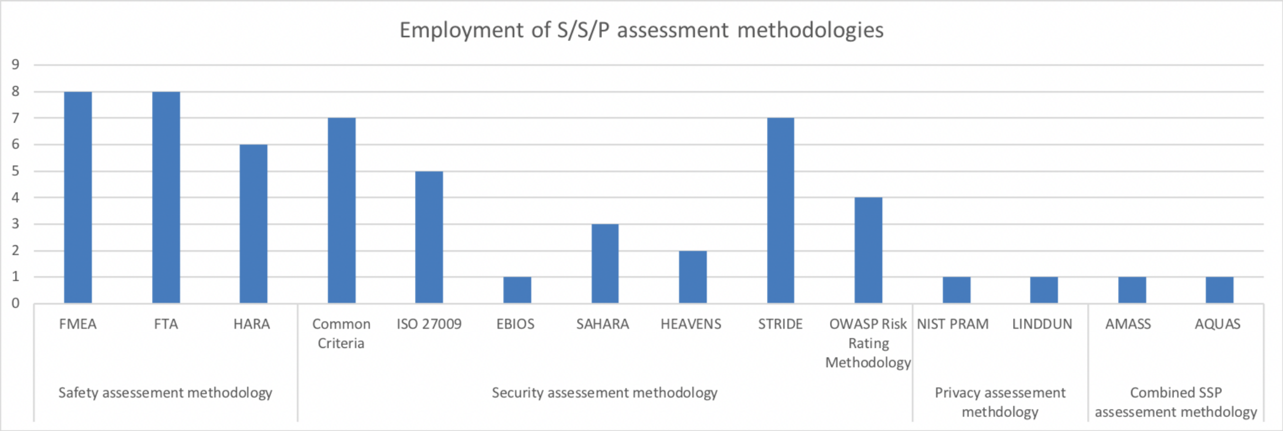

Figure 3-7: Usage of Sa/Se/Pr analysis methodologies

To evaluate the Sa/Se/Pr level 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. Figure 3-7 shows the number of responses which claim using each methodology. For example, 8 respondents apply FMEA [4]. 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.

RQ3-Answer: Concerning safety analysis methodologies, FMEA [40], FTA [42] and HARA (Hazard Analysis and Risk Assessment) [2] are commonly used. Concerning security analysis methodologies, the STRIDE model [41] and the Common Criteria [8] are the most commonly used methods. The usage of security analysis methodologies is more diverse than of safety ones.

3.3.3 Usage of COTS tools

The survey investigates the practitioners' employment of software tools for meeting Sa/Se/Pr requirements, and which properties each tool serves. Table 3-8 summarizes the COTS tools listed in the questionnaire and those complemented by respondents.

Table 3-8: 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
Complemented	• Enterprise Architect • Axivion Suite • Code Composer MISRA 2004 • Coverity (static code analysis) • BugSeng ÉCLAIR • 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

Figure 3-9 shows the number of usage of COTS tools in Sa/Se/Pr engineering. For example, 4 respondents use *IBM Rational DOORS kit* for safety engineering, 3 use it for security engineering, and 1 for other purpose. Note that a respondent may use one tool for multiple purposes. Therefore, the number of respondents who use *IBM Rational DOORS kit* is less or equal to 8. Figure 3-9 indicates that *MathWorks Simulink* and *IBM Rational DOORS kit* seem to be the most used tools for both safety and security engineering. The result of our statistical analysis shows that, in total, about 38% of the respondents employ some software tools to support safety engineering, and 24% for security engineering. On privacy engineering, *PTC integrity* is the only tool used by only one respondent. Note that *PTC Integrity* is not dedicated for privacy engineering. The respondent used it as a development tool for requirements engineering, which includes privacy requirements. The survey indicates that there is not yet an integrated solution on privacy engineering activities, including automation support for marking of PII, anonymization / pseudo-anonymization, differential privacy etc.

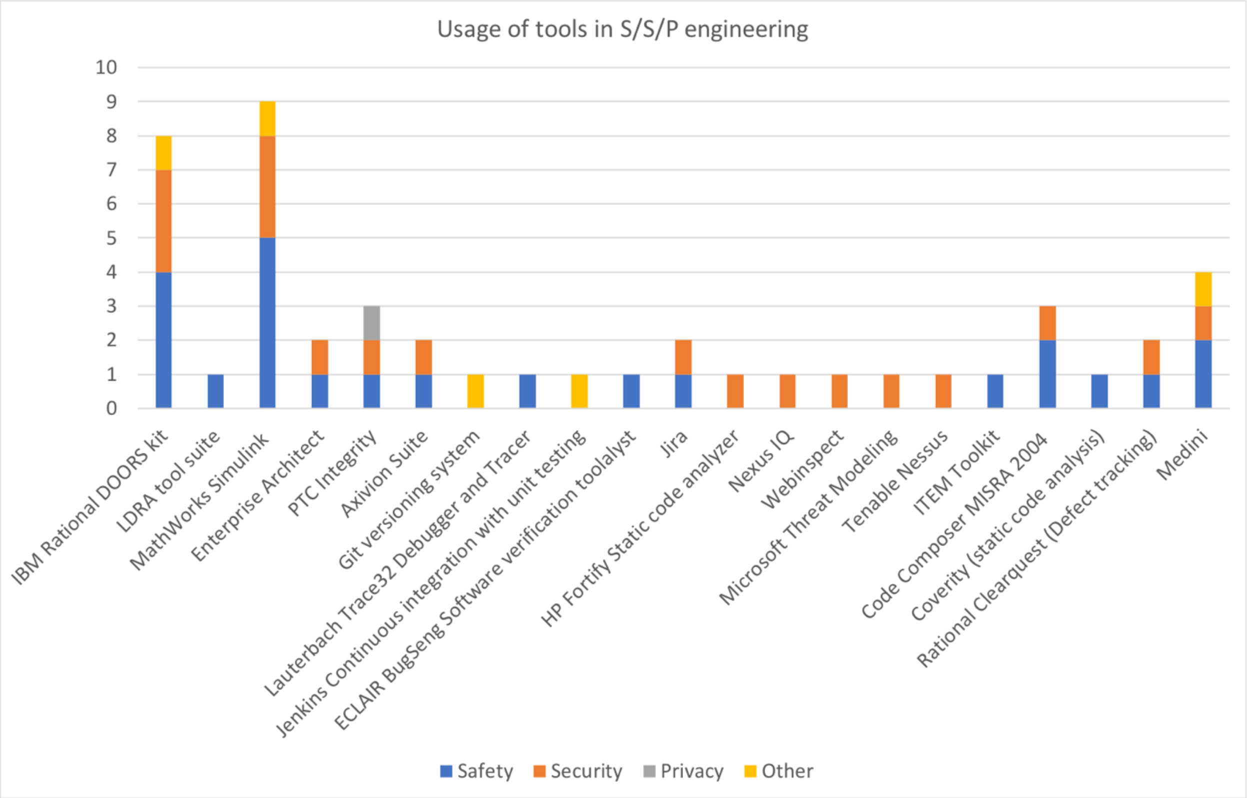

Figure 3-9: Usage of COTS tools in Sa/Se/Pr engineering

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.

4 Conclusions

This deliverable reports our survey on Sa/Se/Pr standards and their usage by practitioners. To the best of our knowledge, there is little empirical study on the industrial sectors' practices of Sa/Se/Pr standards. The report fills this gap by gathering feedback from the practitioners in real-world settings.

In addition to T10.2, our questionnaire-based survey contributes to two other tasks in WP2 and WP10, respectively:

- **T2.3** "Security and privacy reference architecture for safe automated systems": The questionnaire contains questions on the value chain of the partners in order to get an overall picture of the ecosystems. The analysis on this aspect is mainly reported in the section "Business architecture" of deliverable **D2.3.1** "Reference architecture".
- **T10.1** "Survey of partners' involvement in standardisation, use of standards and related activities": The questionnaire contains questions on the partners' participation in standardisation activities. The analysis on this aspect is mainly reported in deliverable **D10.1** "Survey on partners' involvement in and use of standards".

In the context of **T10.2** "State-of-the-art survey of applicable security and safety standards and initiatives", the following observations are drawn based on the SECREDAS partners' responses:

- Concerning the **availability of standards**, safety standards for specific industrial sectors are available as specializations of the basic standard IEC 61508 [1]. A wider range of security standards from different origins are applicable, 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 **practices of standards**, cross-domain security standards ISO 2700X [2] and ISO 15408 [3] are the most applied among all the studied Sa/Se/Pr standards. 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. 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. 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 and should be a major concern of research in SECREDAS.

- Regarding the application of **analysis methodologies**, FMEA [4], FTA [5] and HARA [6] are commonly used safety analysis methodologies. The STRIDE model [7] and the Common Criteria [8] are the most commonly used security analysis methods.
- On the subject of **COTS tools**, 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. Overall speaking, among the three aspects i.e. safety, security and privacy engineering, privacy engineering is less mature than safety and security in terms of the availability and usage of standards, analysis methodologies and software tools, reflecting the fact that privacy engineering is an emerging concern for practitioners.

The survey described in this report is part of a larger research effort aimed at devising integrated Sa/Se/Pr evaluation framework for safety-critical system development. The insights gained from the survey are a stepping stone for our future work activities, which aims to integrate the best-practices of Sa/Se/Pr assessment into the engineering lifestyle and to motivate SECREDAS partners to become involved in standardisation.

Figures and Tables

References

[1] “IEC 61508:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems,” International Electrotechnical Commission (IEC), 2010.

[2] “SO/IEC 27000 family - Information security management systems,” International Organization for Standardization (ISO), 2018.

[3] “ISO/IEC 15408:2009 Preview Information technology -- Security techniques -- Evaluation criteria for IT security,” International Organization for Standardization (ISO), 2009.

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

[5] C. A. Ericson, “Fault tree analysis,” in *System Safety Conference*, Orlando, Florida, 1999.

[6] “ISO 26262:2018 Road vehicles – Functional safety,” International Organization for Standardization (ISO), 2018.

[7] A. Shostack, Threat modeling: Designing for security, John Wiley & Sons, 2014.

[8] “Common Criteria,” [Online]. Available: https://www.commoncriteriaportal.org. [Accessed 03 04 2019].

[9] ISO. [Online]. Available: https://www.iso.org/deliverables-all.html. [Accessed 2 4 2019].

[10] “IEC 62279:2015 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems,” International Electrotechnical Commission (IEC), 2015.

[11] “IEC 61511:2018 SER Series Functional safety - Safety instrumented systems for the process industry sector - ALL PARTS,” International Electrotechnical Commission (IEC), 2018.

[12] “IEC 62061:2005 Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems,” International Electrotechnical Commission (IEC), 2005.

[13] “IEC 62443:2018 Security for industrial automation and control systems.,” International Electrotechnical Commission (IEC), 2018.

[14] “SAE J3061-2016 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,” Society of Automotive Engineers (SAE), 2016.

[15] “ISO/IEC 29100:2011 Information technology -- Security techniques -- Privacy framework,” International Organization for Standardization (ISO), 2011.

[16] “ISO/IEC 29101:2018 Information technology -- Security techniques -- Privacy architecture framework,” International Organization for Standardization (ISO), 2018.

[17] “ISO/IEC 29134:2017 Information technology -- Security techniques -- Guidelines for privacy impact assessment,” International Organization for Standardization (ISO), 2017.

[18] “ISO/IEC 29151:2017 Preview Information technology -- Security techniques -- Code of practice for personally identifiable information protection,” International Organization for Standardization (ISO), 2017.

[19] “ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls,” International Organization for Standardization (ISO), 2013.

[20] A. R. H.´. S.´. B. W. M. W. a. T. W. Olaf Henniger, “Securing vehicular on-board IT systems: The EVITA project.,” *VDI/VW Automotive Security Conference,* 2009.

[21] “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),” European Telecommunications Standards Institute (ETSI), 2017.

[22] C. J. A. a. A. Dorofee, Managing information security risks: the OCTAVE approach, Addison-Wesley Longman Publishing Co., 2002.

[23] “HEAling Vulnerabilities to ENhance Software Security and Safety (HEAVENS) project,” 03 04 2019. [Online]. Available: https://research.chalmers.se/en/project/5809.

[24] L. Leung, “Validity, reliability, and generalizability in qualitative research,” *Journal of family medicine and primary care,* vol. 4, no. 3, p. 324, 2015.

[25] P. R. M. H. M. O. B. R. A. W. C. Wohlin, “Experimentation in Software Engineering: An Introduction,” in *Kluwer Academic Publishers*, 2000.

[26] “ISO 25119:2018 Tractors and machinery for agriculture and forestry – Safety-related parts of control systems,” International Organization for Standardization (ISO), 2018.

[27] IEC, “IEC 61511: Functional safety - Safety instrumented systems for the process industry sector,” IEC .

[28] CENELEC, “EN 50657 Railways Applications - Rolling stock applications - Software on Board Rolling Stock,” CENELEC, 2017.

[29] “NIST Special Publication 800-series,” National Institute of Standards and Technology (NIST), 2018.

[30] “GlobalPlatform Specifications.,” GlobalPlatform, 03 04 2019. [Online]. Available: https://globalplatform.org/specs-library/.

[31] “ETSI TS 101 733 V2.2.1 (2013-04) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES),” European Telecommunications Standards Institute (ETSI), 2013.

[32] “ETSI TS 101 903 V1.4.1 (2009-06) XML Advanced Electronic Signatures (XAdES),” European Telecommunications Standards Institute (ETSI), 2009.

[33] “ETSI TS 102 204 V1.1.4 (2003-08) XML Advanced Mobile Commerce (M-COMM); Mobile Signature Service; Web Service Interface,” European Telecommunications Standards Institute (ETSI), 2003.

[34] “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,” The European Parliament and the Council of the European Union, 2014.

[35] “RFCs Internet cryptographic,” Federal Information Processing Standards (FIPS).

[36] “Trusted Information Security Assessment Exchange (TISAX),” German Association of the Automotive Industry (VDA), 2017.

[37] “Information Security Assessment,” German Association of the Automotive Industry (VDA).

[38] “ETSI TS 103 532 V1.1.1 (2018-03) CYBER; Attribute Based Encryption for Attribute Based Access Control,” European Telecommuni- cations Standards Institute (ETSI), 2018.

[39] “BSI IT-Grundschutz,” German Federal Office for Information Security (BSI), 2015.

[40] “ISO/IEC PDTR 27550 Information technology -- Security techniques -- Privacy engineering,” International Organization for Standardization, under development.

[41] “GlobalPlatform Privacy Framework v1.0,” GlobalPlatform, 2017.

[42] “ISO/IEC 19286:2018 Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services,” International Organization for Standardization (ISO), 2018.

[43] “General Data Protection Regulation (GDPR),” European Parliament and Council of the European Union, 2018.

[44] “Standard Data Protection Model (SDP Model),” German Federal and State Commissioners, 2017.

[45] “ISO/SAE CD 21434 Road Vehicles -- Cybersecurity engineering,” International Organization for Standardization (ISO), under development .

[46] “IEC TR 63069 ED1: Industrial-process measurement, control and automation- Framework for functional safety and security,” International Electrotechnical Commission (IEC), under development.

[47] “Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 GRVA,” United Nations Economic Commission for Europe (UNECE), 2018.

Appendix

"Questionnaire on Safety/Security/Privacy Standards"

Document Type	Project Internal
Document Number	
Primary Author(s)	Internet of Trust
Document Date	05 Nov 2018
Document Version / Status	1.0
Distribution Level	All SECREDAS partners
Reference DoA	

Project Coordinator	Roy Pennings, NXP Semiconductors, roy.pennings@nxp.com
Project Website	https://www.ecsel.eu/projects/secredas
JU Grant Agreement Number	783119

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis

CONTRIBUTORS

Name	Organization
Claire Loiseaux, Lijun Shan	IoTR
Erwin Schoitsch	AIT
Peter Folkesson, Behrooz Sangchoolie, Jonny Vinter	RISE
Andre Smulders, Alexandr Vasenev	TNO
Florian Stahl	AVL

FORMAL REVIEWERS

Name	Organization	Date
Erwin Schoitsch	AIT	31/10/2018

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
V0.1	06/09/2018	IoTR	Creation
V0.2	04/10/2018	IoTR	Revision taking comments from Andre Smulders and Alexandr Vasenev (TNO), comments from Behrooz Sangchoolie, Peter Folkesson and Jonny Vinter *et al* (RISE), and comments from Erwin Schoitsch (AIT)
V0.8	10/10/2018	AIT, RISE	Extension of the questionnaire by AIT and RISE to meet generalized goals of the standardisation survey
V0.9	24/10/2018	IoTR	Revision with comments from TNO and AVL.
V1.0	05/11/2018	IoTR	Final version after review by E. Schoitsch (AIT)

Executive Summary

For studying the state-of-the-art of Safety, Security and Privacy (S-S-P) standards, we designed this questionnaire for all participants of SECREDAS. As a co-work of Internet of Trust (IoTR), Austrian Institute of Technology (AIT), Research Institutes of Sweden (RISE), TNO and AVL, the questionnaire aims to obtain an overview on the standards which interest the SECREDAS partners. It is combined with a planned general survey on standardisation and serves as a single source of information for the first deliverable of WP10.

The survey intends to reveal the acceptance of existing (inter)national standards in both industry and academia, the application of standardized or proprietary S-S-P engineering methodologies, and the maturity of the available S-S-P technologies with respect to the standards. We also solicit feedbacks about your involvement in the related standardisation activities with respect to (highly) automated systems, your preview on evolving standardisation activities in the international standardisation organizations, as well as the challenges and opportunities you see for influencing standardisation, either in maintenance of existing standards or even proposing new work item proposals.

We will present the result of the survey to all SECREDAS participants in a WP10 deliverable and also in the 6-month consortium meeting, so that you could see a landscape of related standards. Any information from your reply which involves individual persons or organization will not be published without consent. Only aggregated and anonymized data will be presented in SECREDAS deliverables.

The survey should take about 15 minutes. Please kindly reply to us before **12 Nov 2018**. If you have any questions, please email us: Lijun.shan@internetoftrust.com and claire.loiseaux@internetoftrust.com. For returning your reply, please indicate your organization in the file title i.e. “Secredas Questionnaire on Standards - XXX”.

We really appreciate your input!

1 About you and your organization

Question	Answer [3]
Your name and title	
Name of your organization	
Domain of your organization (e.g. auto, health, rail, IT, etc.)	
Type of your organization (e.g. OEM/Tier 1/Tier2, service, research institute, plus[4] SME if applicable)	
Your main participation in SECREDAS (WPs or tasks)	
Your contribution to SECREDAS in terms of solutions, technology, products or services	
Type of your main clients	
Type of your main suppliers	
Type of your main research cooperators	
Geographic zone of your clients or your product deployment or your research cooperation (e.g. Europe, Asia, US, etc.)	
In which country/countries (or Europe) do you (intend to) qualify/certify your products or services	

[3] Please write “N/A” if not applicable.

[4] “plus” means you can give two answers addressing the “plus” topic as well.

2 Overview of standards

This section investigates your application of Safety Security Privacy (S-S-P) standards and your interest or participation in the development of standards. The standards listed below are from our state-of-the-art study. Please feel free to add any standards which interest you, including those under development.

2.1 Standards and standardisation

The following subsections are oriented to SECREDAS partners according to their domains: subsection 0 is for all partners; subsections B – D are devoted to partners which are active in automotive, rail and health domains, respectively. Please specify your answers in the corresponding columns of each subsection:

(1) **Develop or observe**: Do (or will) you participate in or observe the development of certain standards? Please specify *Participate* (please also indicate your role[5] and the relevant WG/TC/SC), *Will participate* or *Observe*, if applicable.

(2) **Apply standards in**: In which activity of your daily work do (or will) you apply certain standards? Please specify *Product/service development*, *Research project*, *Testing service*, *Assessment service*, *Consultancy service*, *Training*, or other activity, if applicable.

(3) **Evaluate conformance by**: In the case of applying some standards, how do you evaluate the conformance to the standards? Please specify *Self-evaluation*, *3rd party evaluation*, *Qualification* and/or *Certification*, if applicable.

(4) **Why apply**: What is your reason of applying certain standards? Please specify *Required by customers*, *Required by regulation*, *Guideline for performance*, *Assurance of quality of product/service*, or other, if applicable.

(5) **Why didn't apply**: What is the reason of not applying certain standards? Please specify *Irrelevant*, *Not mandatory*, *Too demanding*, *Too costly*, *No available tool*, *No benefit expected*, or other, if applicable.

[5] Please indicate your role:

- *A* = Active member (taking part in F2F meetings etc.) of a Work Group (WG)/Technical Committee (TC)/Sub Committee (SC)
- *M* = Member of a WG/TC/SC
- *C* = Convener, Leader, Chair of a WG/TC/SC

A. Cross-domain standards

Standards			Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn’t apply
Safety	IEC 61508	Functional safety					
	ISO 13849	Safety of machinery -- Safety-related parts of control systems					
	IEC 62061	Safety of machinery – E/E/PE control systems					
	Others, please specify						
Security	IEC 62443	Industrial network and system security					
	ISO 27000 family	Information security					
	ISO 15408	Common criteria					
	NIST 800	Computer security					
	Others, please specify						
Privacy	ISO 29100	Privacy framework					
	ISO 27550	Privacy engineering					
	Others, please specify						
Safety Security Privacy co-engineering	IEC TR 63069	Framework for functional safety and security					
	Others, please specify						
Dependability	IEC 62853	Open systems dependability					
	IEC 62741	Demonstration of dependability requirements					
	Others, please specify						
Enterprise IT architecture	TOGAF	Architecture framework					
	IEC 62541	OPC unified architecture					
	Others, please specify						
Internet of Things	ISO/IEC 30141	Internet of things - Reference architecture					

		Others, please specify						
	Others cross-domain standards, please specify							
E.g.	*Security*	*ISO 15408*	*Common criteria*	*Participate (A, ISCI)*	*Consultancy service*	*3rd party evaluation by licenced CC labs*	*Required by Customers, for certifying their products e.g. Secure Elements*	*N/A*

B. Automotive

Standards			Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn't apply
Safety	ISO 26262	Road vehicles – Functional safety					
	ISO PAS 21488	Road vehicles – Safety of the intended functionality					
	ISO 26262 Ed2	Road vehicles – functional safety					
	ISO 20077	Extended vehicle (ExVe)					
	Others, please specify						
Security	SAE J3061	Cybersecurity guidebook for cyber-physical vehicle systems					
	ISO / SAE CD 21434	Road vehicles – Cybersecurity engineering					
	Others, please specify						
ECU software architecture	AUTOSAR	Automotive open system architecture					
	Others, please specify						
Other types of standards, please specify							

C. Rail

Standards			Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn’t apply
Safety	EN 50129 (IEC 62425)	Safety related electronic systems for signaling					
	EN 50126 (IEC 62278)	Reliability, availability, maintainability and safety (RAMS)					
	EN 50159 (IEC 62280)	Safety related communication in transmission systems					
	EN 50128 (IEC 62279)	Software for railway control and protection					
	Others, please specify						
Others, please specify							

D. Health

Standards			Develop or observe	Apply standards in	Evaluate conformance by	Why apply	Why didn’t apply
Safety	IEC 62304	Medical device software - Software life cycle processes					
	IEC 60601 / 80601	Medical electrical equipment					
	Others, please specify						
EU medical device directive	Directive 90/385/EEC	Active implantable medical devices (AIMD)					
	Directive 93/42/EEC	Medical devices (MDD)					
	Directive 98/79/EC	In vitro diagnostic medical devices (IVDD)					
	Others, please specify						
Others, please specify							

2.2 Your expectation on future standards

- What do you expect from the in-progress standards?
- What standards are still missing in your opinion?

Standards				Content you expect or have interest
Under progress	Safety	IEC 62879 ED1	Human factors and functional safety	
		IEC 61508 ED3	Functional safety	
		ISO 20078	Extended Vehicle (ExVe) – web services	
		Others, please specify		
	Security	ISO/SAE 21434	Road vehicles -Cybersecurity engineering	
		Others, please specify		
	Safety Security Privacy co-engineering	IEC 63069 ED2	Framework for functional safety and security	
		Others, please specify		
	Artificial Intelligence, Machine Learning	ISO/IEC WD 23053	Framework for AI systems using Machine Learning (ML)	
		Others, please specify		
	Smart Manufacturing	IEC JWG21	Smart manufacturing reference model(s)	
		Others, please specify		
	Internet of Things (IoT)	ISO/IEC21823	Interoperability of IoT systems	
		ISO/IEC 30147	IoT – Methodology for Trustworthiness of IoT system/service	
		Others, please specify		
	Others, please specify			
Missing	Safety			
	Security			
	Privacy			
	S-S-P joint assessment			
	Others, please specify			

E.g.

Under progress	*S-S-P joint assessment*			*Ethical considerations w.r.t. highly automated systems*

3 Your usage of standards in building products or services

This section investigates standardized or proprietary methodologies for Safety, Security and Privacy engineering.

3.1 Your products or services

The following subsections are oriented to organizations with certain roles, assuming that each SECREDAS participant plays one or multiple roles:

- **Section 3.1.1**: for S-S-P technology providers, e.g. Service or Research Institute, who apply S-S-P standards to develop Safety, Security and Privacy technologies, products or services.
- **Section 3.1.2**: for S-S-P technology integrators, e.g. OEM / Tier1 / Tier2 in auto industry, medical industry and rail industry, who apply the standards to specify S-S-P requirements or to evaluate the solutions which integrate S-S-P technologies.
- **Section 3.1.3**: for S-S-P evaluators, e.g. service or research institute, who apply the standards to provide consultancy, or to performs 3rd party assessment, qualification or certification.

3.1.1 For technology developers

The technologies listed below as examples are cited from SECREDAS D3.1 Initial Common Technology Element List. Compared to SECREDAS WP3 which is concerned with the partners' technology contribution to the project, this subsection aims to reveal the usage of standards in daily work of SECREDAS partners. Please feel free to complement the technologies listed in the following table.

- What technology, solution, service or product do you develop or research?
- What are their possible applications? E.g. vehicle sensing, vehicle connectivity, IVN, VCU, health, rail, etc.

Type of your technology	**Possible application areas of your technology**
Key distribution protocol	
Cryptographic libraries	
Hardware isolation technology	
Hypervision technology	
Secure elements	
Secure OS / Trusted Execution Environment	
Authentication and authorization	
Identity management	
Trusted anchor	
Firewall	
Certificate management	
Differential privacy	
Transport layer security	
Distributed ledger technologies	
VPN	
Security or safety testing	
Intrusion detection systems	
Others, please specify (incl. proprietary)	
E.g. *Secure OS*	*Security software stack in V2X, gateway in IVN*

3.1.2 For technology integrators

- In which product, solution or service do you integrate Security, Safety or Privacy technologies?
- What technologies do you apply or integrate for satisfying S-S-P requirements? E.g. hypervision, trusted anchors, TEE, secure elements, authentication & authorization, etc.

Area of your solution	Your product or service	S-S-P technologies you applied
Vehicle Sensing		
Vehicle Connectivity		
IVN & VCU		
Health		
Rail		
Others, please specify		
E.g. *Vehicle Connectivity*	*Telematics*	*Authentication & authorization*

3.1.3 For service providers

- What services do you provide on Security, Safety or Privacy?
- In which domain do you provide such services?

Type of service	Your services	Applied domains
Assessments		
Testing services		
Consultancy		
Qualification / Certification		
Others, please specify		
E.g. *Assessments*	*Security analysis*	*Automobile infotainment systems*

3.2 Your usage of methodologies, tools and models

3.2.1 Safety Security Privacy engineering methodologies

- What standardized or 3rd party or proprietary engineering methodologies or process are applied in your daily work for satisfying Safety, Security or Privacy requirements?

	Standardized	**3rd party**	**Proprietary**
Safety			
Security			
Privacy			
Other concerns, please specify			
E.g. *Security risk analysis*	*ISO 27005 – EBIOS based*	*N/A*	*In-house customized security risk analysis methodology for IoT systems*

3.2.2 Safety Security Privacy engineering tools

- What COTS or proprietary tools do you (plan to) apply to meet Safety, Security or Privacy requirements, and which properties the tools servers? The tools listed below are only examples. Please feel free to add any tools which interest you, including in-house ones.

	Software Tools		**Safety**	**Security**	**Privacy**	**Other Concerns**
	COTS tools	Ansys SCADE code generators				
		Cadence Automotive Functional Safety Kits				
		IBM Rational DOORS kit				
		Mentor Graphics Veloce hardware emulation platform				
		Parasoft C/C++test				
		LDRA tool suite				
		MathWorks Simulink				
		Other, please specify				
	Proprietary tools					
	Others, please specify					
E.g.	*COTS tools*	*MathWorks Simulink*	*X*	*X*	*N/A*	*N/A*

3.2.3 Safety Security Privacy models

- Do you use specific quantitative or qualitive Safety Security Privacy models?
- What purpose do the models serve in your work?

		Model	Purpose of usage
	Security threat and risk modelling	STRIDE	
		OWASP	
		others, please specify	
	System security engineering models	Cyber Resiliency Engineering Framework	
		others, please specify	
	Other, please specify		
E.g.	*Security threat and risk modelling*	*STRIDE*	*Security threat analysis in automotive IVN systems*

4 Your usage of standards in assessment activities

This section investigates your application of Safety Security Privacy assessment methodologies, either standardized or proprietary. Please feel free to add applicable methodologies, including in-house ones.

	Methodology	**For self-assessment**	**For 3rd party assessment**	**For qualification / certification**
Safety	FMEA (Failure Mode and Effects Analysis)			
	FTA (Fault Tree Analysis)			
	HARA (Hazard and Risk Assessment)			
	Others, please specify			
Security	Common Criteria			
	ISO 27005			
	EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)			
	SAHARA (Security-Aware Hazard Analysis and Risk Assessment)			
	HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety)			
	STRIDE			
	OWASP Risk Rating Methodology			
	Others, please specify			
Privacy	NIST PRAM (Privacy Risk Assessment Methodology)			
	LINDDUN			
	Others, please specify			
Combined Safety Security Privacy methods *(incl. proprietary)*	AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)			
	AQUAS (Aggregated Quality Assurance for Systems)			
	Others, please specify			
Other concerns, please specify				
E.g. *Security*	*Common Criteria*	*X*	*X*	*X*

5 Open questions

5.1 On reuse and patterns

(1) As architect or designer or engineer, at which abstraction level do you consider reuse? E.g. domain-specific design or assets (i.e. platforms, items or products), domain-related architecture or asset architecture, safety/security/privacy reference architecture.

[Your Answer]

(2) What standards do you apply for improving the reusability at certain levels?

[Your Answer]

5.2 On quality assurance

(1) What is your impression on approaches to jointly consider safety-security-privacy?

[Your Answer]

(2) How do you obtain a cross-domain view in your development or research, so that your solution or product or service would work for various domains e.g. auto, rail and health?

[Your Answer]

(3) How do you maintain the safety or security level of your solution (product or service) during its evolution?

[Your Answer]

(4) What is lacking in the related standardisation?

[Your Answer]

5.3 Other concerns or comments

[Your Answer]

www.secredas.eu

mail@secredas.eu

Social media @secredas.eu

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

European Commission

Horizon 2020
European Union funding
for Research & Innovation

SECREDAS
Digital Privacy
Safety & Security

SECREDAS has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement nr.783119. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Germany, Finland, Hungary, Italy, The Netherlands, Poland, Romania, Sweden and Tunis