VALU3S

Verification and Validation of Automated Systems' Safety and Security

Final report on the results of the standardisation survey

Document Type	Report
Document Number	D6.10
Primary Author(s)	Christoph Schmittner (AIT)
Document Date	2021-04-30
Document Version	1.0 (Final)
Dissemination Level	Public (PU)
Reference DoA	2021-02-26
Project Coordinator	Behrooz Sangchoolie, behrooz.sangchoolie@ri.se, RISE Research Institutes of Sweden
Project Homepage	www.valu3s.eu
JU Grant Agreement	876852

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.

Disclaimer

The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the views or position of the European Commission. The authors, the VALU3S Consortium, and the ECSEL JU are not responsible for the use which might be made of the information contained in here.

Project Overview

Manufacturers of automated systems and the manufacturers of the components used in these systems have been allocating an enormous amount of time and effort in the past years developing and conducting research on automated systems. The effort spent has resulted in the availability of prototypes demonstrating new capabilities as well as the introduction of such systems to the market within different domains. Manufacturers of these systems need to make sure that the systems function in the intended way and according to specifications which is not a trivial task as system complexity rises dramatically the more integrated and interconnected these systems become with the addition of automated functionality and features to them.

With rising complexity, unknown emerging properties of the system may come to the surface making it necessary to conduct thorough verification and validation (V&V) of these systems. Through the V&V of automated systems, the manufacturers of these systems can ensure safe, secure and reliable systems for society to use since failures in highly automated systems can be catastrophic.

The high complexity of automated systems incurs an overhead on the V&V process making it time-consuming and costly. VALU3S aims to design, implement and evaluate state-of-the-art V&V methods and tools to reduce the time and cost needed to verify and validate automated systems with respect to safety, cybersecurity and privacy (SCP) requirements. This will ensure that European manufacturers of automated systems remain competitive and that they remain world leaders. To this end, a multi-domain framework is designed and evaluated with the aim to create a clear structure around the components and elements needed to conduct V&V process through identification and classification of evaluation methods, tools, environments and concepts that are needed to verify and validate automated systems with respect to SCP requirements.

In VALU3S, 12 use cases with specific safety, security and privacy requirements will be studied in detail. Several state-of-the-art V&V methods will be investigated and further enhanced in addition to implementing new methods aiming for reducing the time and cost needed to conduct V&V of automated systems. The V&V methods investigated are then used to design improved process workflows for V&V of automated systems. Several tools will be implemented supporting the improved processes which are evaluated by qualification and quantification of safety, security and privacy as well as other evaluation criteria using demonstrators. VALU3S will also influence the development of safety, security and privacy standards through an active participation in related standardisation groups. VALU3S will provide guidelines to the testing community including engineers and researchers on how the V&V of automated systems could be improved considering the cost, time and effort of conducting the tests.

VALU3S brings together a consortium with partners from 10 different countries, with a mix of *industrial partners* (24 partners) from automotive, agriculture, railway, healthcare, aerospace and industrial automation and robotics domains as well as leading *research institutes* (6 partners) and *universities* (10 partners) to reach the project goal.

Consortium

RISE RESEARCH INSTITUTES OF SWEDEN AB	RISE	Sweden
STAM SRL	STAM	Italy
FONDAZIONE BRUNO KESSLER	FBK	Italy
KNOWLEDGE CENTRIC SOLUTIONS SL - THE REUSE COMPANY	TRC	Spain
UNIVERSITA DEGLI STUDI DELL'AQUILA	UNIVAQ	Italy
INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO	ISEP	Portugal
UNIVERSITA DEGLI STUDI DI GENOVA	UNIGE	Italy
CAMEA, spool. s r.o.	CAMEA	Czech
IKERLAN S. COOP	IKER	Spain
R G B MEDICAL DEVICES SA	RGB	Spain
UNIVERSIDADE DE COIMBRA	COIMBRA	Portugal
VYSOKE UCENI TECHNICKE V BRNE - BRNO UNIVERSITY OF TECHNOLOGY	BUT	Czech
ROBOAUTO S.R.O.	ROBO	Czech
ESKISEHIR OSMANGAZI UNIVERSITESI	ESOGU	Turkey
KUNGLIGA TEKNISKA HOEGSKOLAN	KTH	Sweden
STATENS VAG- OCH TRANSPORTFORSKNINGSINSTITUT	VTI	Sweden
UNIVERSIDAD DE CASTILLA - LA MANCHA	UCLM	Spain
FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	FRAUNHOFER	Germany
SIEMENS AKTIENGESELLSCHAFT OESTERREICH	SIEMENS	Austria
RULEX INNOVATION LABS SRL	RULEX	Italy
NXP SEMICONDUCTORS GERMANY GMBH	NXP-DE	Germany
PUMACY TECHNOLOGIES AG	PUMACY	Germany
UNITED TECHNOLOGIES RESEARCH CENTRE IRELAND, LIMITED	UTRCI	Ireland
NATIONAL UNIVERSITY OF IRELAND MAYNOOTH	NUIM	Ireland
INOVASYON MUHENDISLIK TEKNOLOJI GELISTIRME DANISMANLIK SANAYI VE TICARET LIMITED SIRKETI	IMTGD	Turkey
ERGUNLER INSAAT PETROL URUNLERI OTOMOTIV TEKSTIL MADENCILIK SU URUNLER SANAYI VE TICARET LIMITED STI.	ERARGE	Turkey
OTOKAR OTOMOTIV VE SAVUNMA SANAYI AS - OTOKAR AS	OTOKAR	Turkey
TECHY BILISIM TEKNOLOJILERI DANISMANLIK SANAYI VE TICARET LIMITED SIRKETI - TECHY INFORMATION TECHNOLOGIESAND CONSULTANCY LIMITED COMPANY	TECHY	Turkey
ELECTROTECNICA ALAVESA SL	ALDAKIN	Spain
INTECS SOLUTIONS SPA	INTECS	Italy
LIEBERLIEBER SOFTWARE GMBH	LLSG	Austria
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH	AIT	Austria
E.S.T.E. SRL	ESTE	Italy
NXP SEMICONDUCTORS FRANCE SAS	NXP-FR	France
BOMBARDIER TRANSPORTATION SWEDEN AB	BT	Sweden
QRTECH AKTIEBOLAG	QRTECH	Sweden
CAF SIGNALLING S.L	CAF	Spain
MONDRAGON GOI ESKOLA POLITEKNIKOA JOSE MARIA ARIZMENDIARRIETA S COOP	MGEP	Spain
INFOTIV AB	INFOTIV	Sweden
BERGE CONSULTING AB	BERGE	Sweden

Executive Summary

In this final report on the results of the standardisation survey (methods, tools, concepts suggested by the standards), we evaluate the standardization survey and observe the identified relevant standards based on the reported relevant methods, tools and approaches to give an overview about ongoing developments and foreseeable changes to identify gaps and topics.

The initial survey to identify which standards and methods and topics are relevant to the work in VALU3S was conducted as an online survey for the whole consortium. A detailed overview was given in D6.5 [1] and a summary is included here. Relevant standards are IEC 61508 as Basic Safety Standards (BSS) and IEC 62443 as industrial security standard which is also applied in the energy and railways domain. ISO 26262 as safety standard and ISO /SAE 21434 as cybersecurity standard for road vehicles are also included. Methods and topics are risk assessment, system development lifecycle and protective (safety & security) requirements catalogue including failure detection & diagnosis.

In this deliverable we report on the status and ongoing trends regarding the relevant methods and topics in the important standards. We identify potential gaps and trends in the developments regarding safety and security standards covering the same domain based on the different development histories.

Contributors

Contributions to the survey were delivered by the whole consortium. Review and evaluation of the survey was conducted by AIT with the support of the participants in Task 6.3 of the project.

Reviewers

Pierre Kleberger	RISE	2021-04-09
Jonny Vinter	RISE	2021-04-27, 2021-04-30
Silvia Mazzini	INTECS	2021-04-15
Behrooz Sangchoolie	RISE	2021-04-30

Revision History

Version	**Date**	**Author (Affiliation)**	**Comment**
0.1	2021-04-05	Christoph Schmittner, Abdelkader Shaabaan (AIT)	First version
0.2	2021-04-20	Christoph Schmittner (AIT)	Integration of first review comments
0.3	2021-04-29	Christoph Schmittner (AIT)	Integration of second review comments
0.4	2021-04-30	Behrooz Sangchoolie (RISE)	Review of the final draft while making minor formatting changes.
1.0	2021-04-30	Behrooz Sangchoolie (RISE)	Final version to be submitted.

Table of Contents

List of Figures

List of Tables

Acronyms

ASIL	Automotive Safety Integrity Level
BSS	Basic Safety Standards
CVSS	Common Vulnerability Scoring System
ETA	Event Tree Analysis
FMEA	Failure Mode and Effects Analysis
FSR	Functional Security Requirements
FTA	Fault Tree Analysis
HARA	Hazard Analysis and Risk Assessment
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
PAS	Publically Available Specification
QM	Quality Management
SCP	Safety, Cybersecurity and Privacy
SIL	Safety Integrity Level
SL-A	Security Level Achieved
SL-C	Security Level Capabilities
SL-T	Security Level Target
V&V	Verification and Validation

Chapter 1 Introduction

Standardization is an important part of research and development. Standardization, as the development of new standards or the update of existing standards, represents the transmission of results from research and development towards the accepted state of the art. In addition to that, standards are an important input for ongoing research work. Since standards contain the current state of the art, gaps and missing guidance is also contained. The development of standards is driven from industry and society. Therefore, increased standardization activities are also a sign for increased importance.

Based on this, Task 6.3 in VALU3S has the main objective to plan and implement all the actions that relate to the establishment of links and interactions with standardization bodies, for which results obtained in VALU3S can be an opportunity to influence ongoing developments in standardization efforts. In addition to that, we also plan to use this work to support other Tasks aimed at the development of methods and frameworks. For this, we plan to not only identify relevant standardization bodies and standards, but also to develop an overview about the standards, e.g., which methods are used, which methods are missing and if there are reasons why certain methods and approaches are not used.

This document, the final report on the results of the standardisation survey (methods, tools, concepts suggested by the standards) is a continuation and extension of D6.5 Initial report on the results of the standardisation survey [1].

In D6.5 [1], we reported the results of the initial survey which identified standards that are relevant for the project work and standards with an ongoing involvement from project partners.

Based on these initial results, a more thorough investigation of the standards was conducted to identify and evaluate relevant methods and approaches from the relevant standards (see Chapter 3). D6.10 reports the results of the detailed analysis. The focus is on methods and tools which are identified as relevant and to analyse the state of the art. For the overview of which standards and topics are identified as relevant to the work in VALU3S, a summary of the results from D6.5 is included and presented in Chapter 2.

Chapter 2 Summary of Survey Results Presented in D6.5 [1]

D6.5 reported the first assessment of a standardisation survey for the whole consortium. D6.5 had the goal to develop a first overview of the standardization landscape and interest for VALUE3S. D6.10 has the goal to deliver an overview of methods and tools from the standardization landscape which can be used in the project. For this, we give a short summary of the identified standards and methods from D6.5. Main interest / involvement from the project in standards is shown in Table 2.1.

Table 2.1 Standards with the highest number of interested / observing / developing partners

Standard	Comment	Domain	#Feedback	Interested	Observe	Develop
IEC 61508 Functional safety of electrical / electronic / programmable electronic safety-related systems	Domain independent basic safety standard. Security is partially considered (during risk analysis) and a maintenance phase with a discussion about the role of security is ongoing.	Overarching	7	1	4	2
ISO 26262 Road vehicles — Functional safety	ISO 26262 Edition 2 was published in 2018 and focuses on functional safety for automotive systems. It could be applied to vehicles in the farming domain and the interaction with security (e.g., combining V&V) is included.	Road vehicles	7	1	4	2
ISO 13849 Safety of machinery — Safety-related parts of control systems	ISO 13849 provides functional safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems for machinery.	Machinery	4		3	1
IEC 62443-3 Security for industrial automation and control systems	The system level is aimed at Asset Operator and System Integrator and describes necessary activities and processes during the system engineering. Ongoing rework of some subparts.	Industrial / Overarching	4	1	2	1

Standard	Comment	Domain	#Feedback	Interested	Observe	Develop
IEC 62443-4 Security for industrial automation and control systems	The component level is for Product supplier and describes how to develop secure components for the integration in Industrial Automation and Control Systems (IACS). Ongoing rework of some subparts.	Industrial / Overarching	4	1	2	1
ISO/SAE 21434 Road vehicles — Cybersecurity engineering	ISO/SAE 21434 is a still in development standard for automotive cybersecurity engineering. Like ISO 26262 the interface from security to safety is defined.	Road Vehicles	4	1	1	2

We list here all standards where at least four partners reported:

a) interest: partner is interested in a standard (published version)
b) observe: partner is observing the development of a standard
c) develop: partner is active in the development of a standard

Here the difficulty lies in the structural difference of standards. IEC 62443 [2] is divided into four groups of standards with 2-5 parts per group (for an overview see Figure 2.1) which we listed in the survey D6.5, separated due to their different focus.

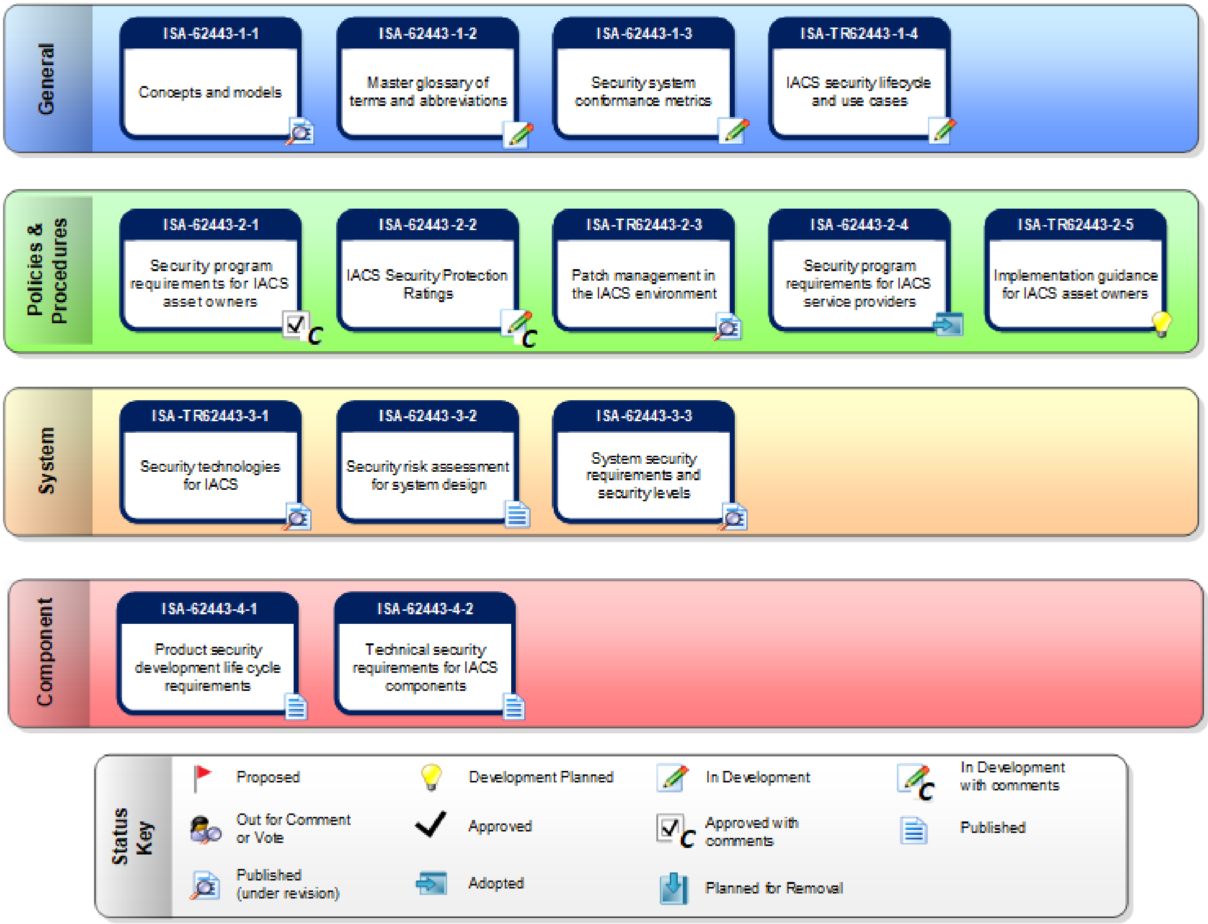

General
ISA-62443-1-1
Concepts and models
ISA-62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
Security system conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS Security Protection Ratings
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program requirements for IACS service providers
ISA-TR62443-2-5
Implementation guidance for IACS asset owners
System
ISA-TR62443-3-1
Security technologies for IACS
ISA-62443-3-2
Security risk assessment for system design
ISA-62443-3-3
System security requirements and security levels
Component
ISA-62443-4-1
Product security development life cycle requirements
ISA-62443-4-2
Technical security requirements for IACS components
Status Key
Proposed
Development Planned
In Development
In Development with comments
Out for Comment or Vote
Approved
Approved with comments
Published
Published (under revision)
Adopted
Planned for Removal

Figure 2.1 IEC 62443 Series of Industrial Security Standard – Overview[1]

Comparing this with ISO 26262 [3], which consists of 12 parts but is not divided into groups (see Figure 2.2), we had for ISO 26262 only one entry in the survey. Altogether there was a similar feedback to most parts of IEC 62443, ranging from 3-4.

[1] Accessed 2021-04-22: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

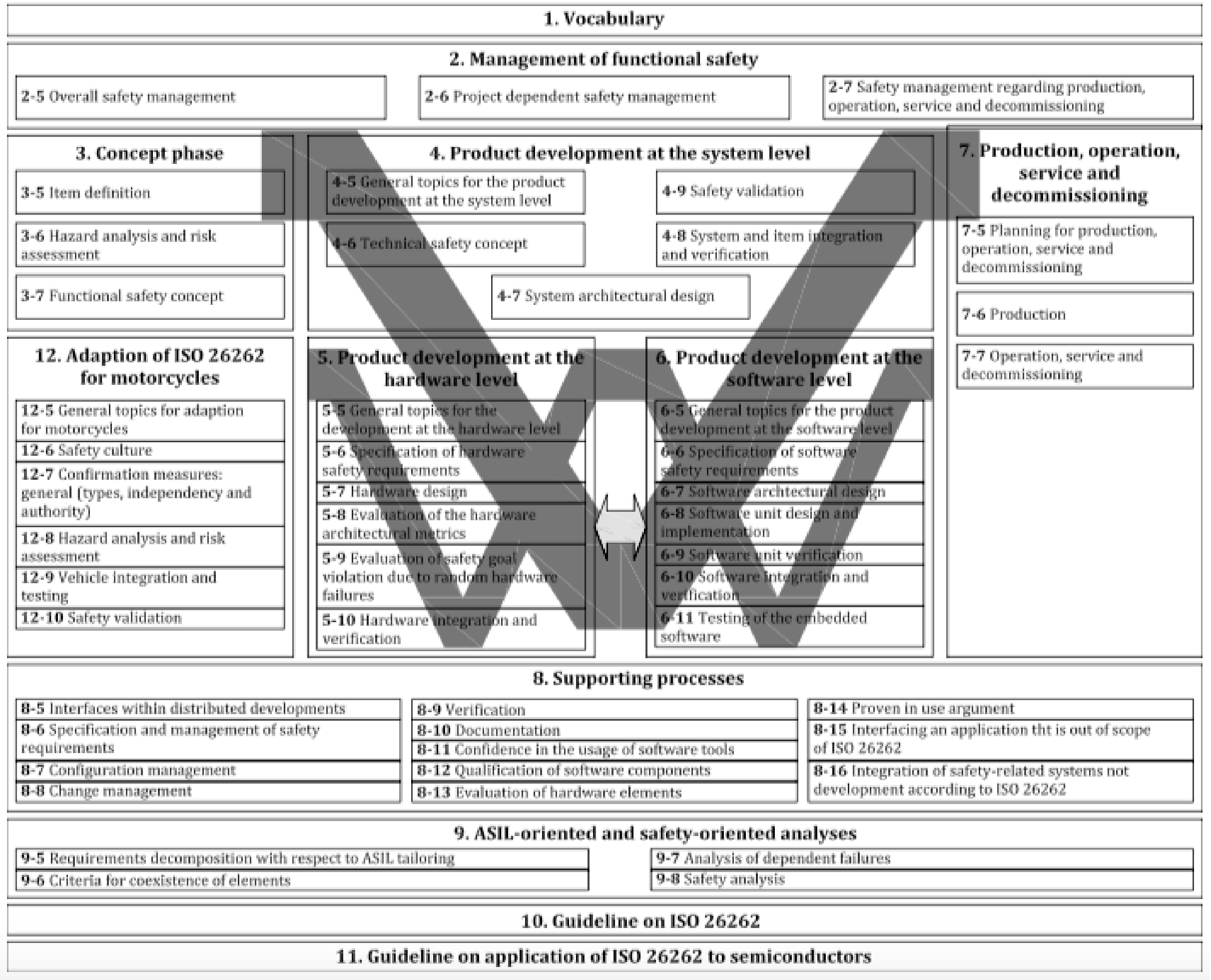

1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Project dependent safety management
2-7 Safety management regarding production, operation, service and decommissioning
3. Concept phase
3-5 Item definition
3-6 Hazard analysis and risk assessment
3-7 Functional safety concept
4. Product development at the system level
4-5 General topics for the product development at the system level
4-9 Safety validation
4-6 Technical safety concept
4-8 System and item integration and verification
4-7 System architectural design
7. Production, operation, service and decommissioning
7-5 Planning for production, operation, service and decommissioning
7-6 Production
7-7 Operation, service and decommissioning
12. Adaption of ISO 26262 for motorcycles
12-5 General topics for adaption for motorcycles
12-6 Safety culture
12-7 Confirmation measures: general (types, independency and authority)
12-8 Hazard analysis and risk assessment
12-9 Vehicle integration and testing
12-10 Safety validation
5. Product development at the hardware level
5-5 General topics for the development at the hardware level
5-6 Specification of hardware safety requirements
5-7 Hardware design
5-8 Evaluation of the hardware architectural metrics
5-9 Evaluation of safety goal violation due to random hardware failures
5-10 Hardware integration and verification
6. Product development at the software level
6-5 General topics for the product development at the software level
6-6 Specification of software safety requirements
6-7 Software archtectural design
6-8 Software unit design and implementation
6-9 Software unit verification
6-10 Software integration and verification
6-11 Testing of the embedded software
8. Supporting processes
8-5 Interfaces within distributed developments
8-6 Specification and management of safety requirements
8-7 Configuration management
8-8 Change management
8-9 Verification
8-10 Documentation
8-11 Confidence in the usage of software tools
8-12 Qualification of software components
8-13 Evaluation of hardware elements
8-14 Proven in use argument
8-15 Interfacing an application tht is out of scope of ISO 26262
8-16 Integration of safety-related systems not development according to ISO 26262
9. ASIL-oriented and safety-oriented analyses
9-5 Requirements decomposition with respect to ASIL tailoring
9-6 Criteria for coexistence of elements
9-7 Analysis of dependent failures
9-8 Safety analysis
10. Guideline on ISO 26262
11. Guideline on application of ISO 26262 to semiconductors

Figure 2.2 ISO 26262 Automotive Functional Safety Standard – Overview[2]

Besides the standards on its own, there was also a focus on what methods or tools are suggested by a specific standard. Taking both already mentioned standards into account, both cover lifecycles and provide requirements, guidance and methods for the lifecycle.

While ISO 26262 depicts its intended lifecycle and how the different parts give input for their respective position in this lifecycle in the overview picture, this is not as clearly visible for IEC 62443. IEC 62443 divides between the operator of an industrial network (Asset Owner) which identifies a set of requirements necessary to secure it (Security Level Target, SL-T). This is then taken by a system integrator with the goal to integrate components with certain security capabilities (Security Level Capabilities, SL-C) to provide an industrial network with a certain achieved level of security (Security Level Achieved, SL-A). An overview of the process is shown in Figure 2.3.

[2] Accessed 2021-04-22: https://www.iso.org/obp/ui/#iso:std:iso:26262:-12:ed-1:v1:en

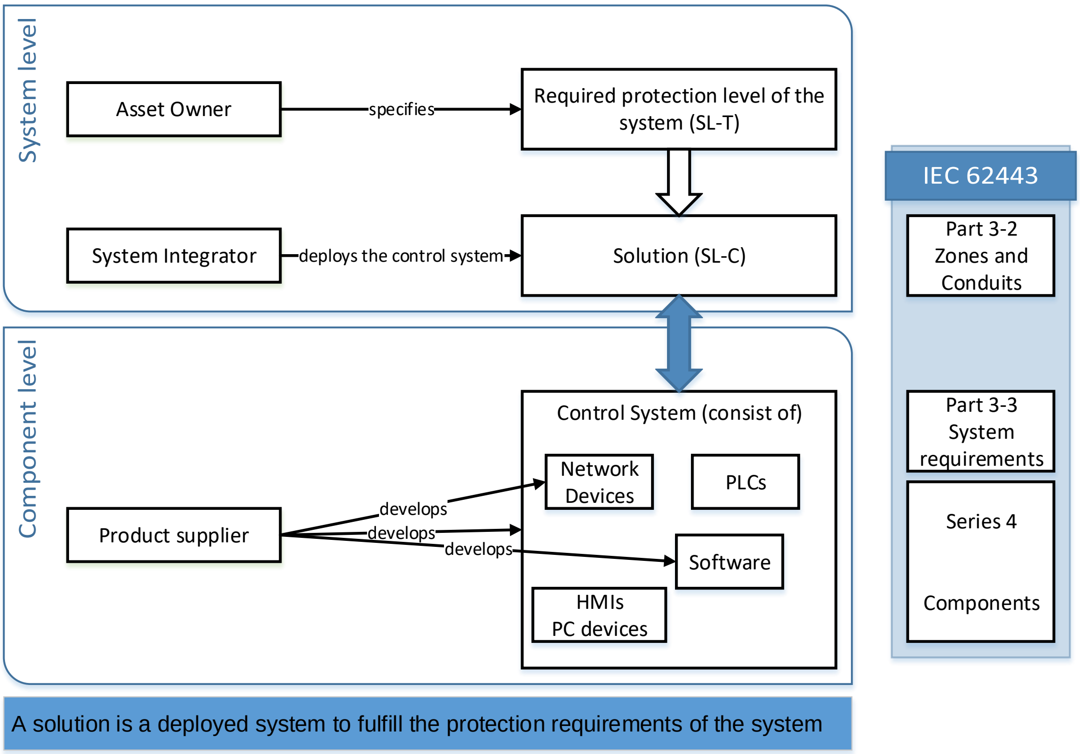


Figure 2.3 IEC 62443 approach

Additional parts give insight into the operation and management for such a secured industrial network. We identified therefore in the survey also which methods are utilized or interesting. For this an open question "What is applied (Method)" was included in the survey. Here the responses ranged from methods to aspects to phases in a lifecycle which might be addressed by multiple methods. Table 2.2 provides the results. This is not restricted to the standards with the highest number of interested / observing / developing partners but considers all received information.

Table 2.2 Feedback on methods / aspects / tools which are applied or interesting

Method / Topic / Aspect	Responses	%
Risk assessment	13	24%
Systems development lifecycle	12	22%
Protective (Safety&Security) Requirements catalogue, failure detection & diagnosis	9	16%
Formal methods	5	9%
Functional safety certification	4	7%
Verification and validation	4	7%
Assurance of quality of product/service	2	4%
Requirements for collaborative robot system applications	2	4%
safety flow	1	2%

Method / Topic / Aspect	Responses	%
Workflow process to establish zones and conduits	1	2%
Cybersecurity Audit	1	2%
Statistical Tests for Random Number Generators	1	2%
	55	100%

Risk assessment was overall the topic, which was received as the most important, followed by system development lifecycle and Protective (Safety&Security) Requirements catalogue, failure detection & diagnosis. It should be remarked that some responses in the survey were adapted to fit in a category, e.g., systems development lifecycle includes responses for software development lifecycle.

Chapter 3 Method / Topic / Aspect Survey

In this Chapter, we present a survey of reported standards by consortium members, based on their feedback regarding methods / aspects / tools which are applied or are interesting. State of standardization and ongoing standard developments were evaluated to identify developments in the methods / aspects / tools.

3.1 Risk Assessment

Risk assessment is a very broad topic applied in a multitude of domains, from insurance to banking to engineering. In general, risk is defined as a combination of an impact and a likelihood.

3.1.1 Contributing Factors

Impact describes the effect level of a risk and this can be expressed in a quantitative or qualitative way. The impact also depends on the category of effect. For a monetary effect it might be possible to give a certain monetary value. Effects on human health are more difficult to quantify and here an abstract scale is usually used, one example is the proposed usage of an injury scale in ISO 26262 [3]. Usage of scales is also an approach to define ranges of effects, e.g., if a risk cannot be quantified a range can be given instead.

Likelihood describes the probability of occurrence. Here different approaches are utilized. In general, likelihood descriptions can also be divided into quantitative or qualitative descriptions. There are differences what is exactly described in the likelihood, notably is as example the usage of controllability as a factor in Likelihood in ISO 26262. To differentiate between a quantitative and qualitative scale, probability is used for a quantitative value (e.g., survival function) and likelihood is used for a quantitative or unspecified description (e.g., chance of happening is high).

If impact and likelihood are described in a quantitative way risks can be calculated. If qualitative descriptions are used approaches like risk matrixes are used, where quantitative assessments of impacts and likelihoods are mapped into a risk (in accordance to a defined risk matrix for the specific analysis method).

Quantitative assessments are mainly used for hardware based topics or topics which are influenced by reliability, were a statement based on historical data can be given. For systems, software and security, risk assessments are mainly given in qualitative statements, although there are approaches to also define quantitative statements [4].

3.1.2 Level of Application

Risk assessment are conducted on different detail levels, from concept to system and even implementation. Most risk-based standards foresee an initial analysis on the concept level to determine the overall need for risk management. If the initial risk assessment results in a high risk, the rigour of subsequent steps also need to be higher. One example of such an approach is the SIL (Safety Integrity Level) and ASIL (Automotive Safety Integrity Level) used in IEC 61508 and ISO 26262 respectively. With ASIL risks are rated from QM (no specific risk treatment needed) to A (lowest level of safety risks), B, C and D (highest level of safety risks). The goal here is to reduce all risks to a tolerable level, which requires more effort for higher risks (due to the larger degree of required risk reduction). Figure 3.1 gives an overview about the ASIL based approach. The overall goal is to reduce all risks below the tolerable risk level.

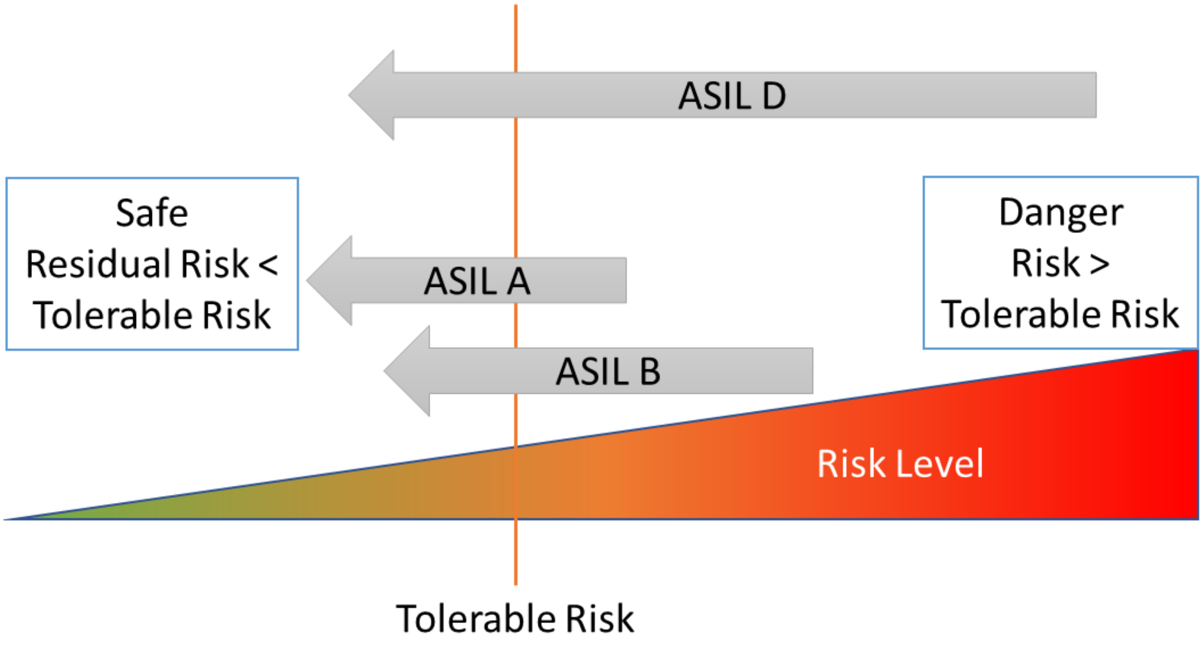
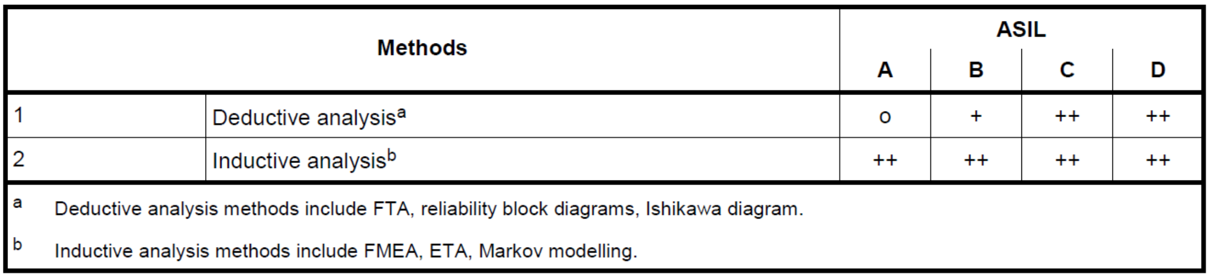


Figure 3.1 Risk managment based on ASIL

Regarding methods and tools for risk assessments in standardization, there is an ongoing trend towards describing a framework rather than a concrete method. An example for this can be seen in the changes from ISO 26262:2011 [5] to ISO 26262:2018 [3]. ISO 26262 does contain approaches towards risk assessment on multiple levels. Depending on the risk level for the system level, inductive and deductive analysis are required. This was done due to their complementary nature and to ensure a better coverage for risk identification. While the table is completely the same in ISO 26262:2011 (see Table 3.1) and ISO 26262:2018 (see Table 3.2), Notes to the entries were changed in order to avoid giving examples of methods.

Table 3.1 System design analysis from ISO 26262-4:2011 [5]

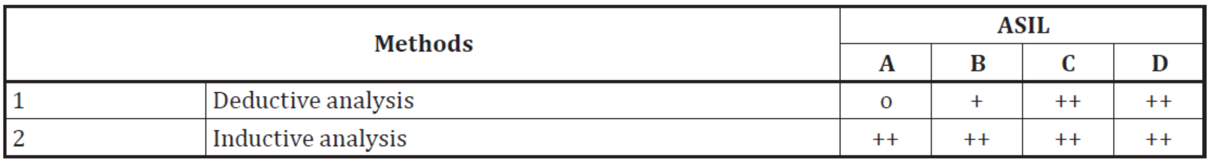


Methods		ASIL			
		A	B	C	D
1	Deductive analysis[a]	o	+	++	++
2	Inductive analysis[b]	++	++	++	++

[a] Deductive analysis methods include FTA, reliability block diagrams, Ishikawa diagram.

[b] Inductive analysis methods include FMEA, ETA, Markov modelling.

Table 3.2 System design analysis from ISO 26262-4:2018 [3]



Methods		ASIL			
		A	B	C	D
1	Deductive analysis	o	+	++	++
2	Inductive analysis	++	++	++	++

This change was done due to the observation that the informative note leads to the usage of only the mentioned methods. Reason for this is in the necessary argumentation for applied methods and tools. If safety experts utilized the methods given as example in ISO 26262:2011, they could always refer to the note to the entries in ISO 26262:2011 why these methods were chosen. With new methods available and an increasing degree of complexity, software-dependency and automation in the automotive domain, there was a long discussion during the development of the ISO 26262:2011 about which new methods to add to this note. In the end, it was decided that instead of adding methods, the best course of action was to remove the note. Instead of describing specific methods a framework is given. This means the standard does not recommend or mention a specific method, but instead gives a list of objectives which must be achieved or requirements to which the used method must be compliant. In this sense there is still a set of perimeters and descriptions for methods without restricting the applicable methods.

Concerning risk assessment, approaches in standards can be divided into the following categories:

- quantitative / qualitative
- level of application (Concept / System / Implementation)
- method / framework

This allows to analyse standards for their risk assessment approaches and give feedback on described methods. Table 3.3 - Table 3.6 contain a summarized overview of the risk assessment approaches described in the standards identified as most relevant for the work in VALU3S.

Table 3.3 Overview of risk assessment described in IEC 61508 [6]

Standard	IEC 61508 [6]
Quantitative / Qualitative	IEC 61508 follows a qualitative risk assessment approach for most of its phases. While for hardware historical data is used to identify probabilities this is not applied for concept and system-level or software. Here, likelihoods are mostly based on expert judgments with a qualitative scale. Impacts are only rated on a quantitative scale. This is due to the difficulties to give a clear impact assessment for safety related impacts.
Level of application	IEC 61508 contains guidance on risk assessment for all phases, with a strong focus on the hazard and risk analysis for the concept phase. This initial risk assessment and the design decision conducted based on this are checked after the conclusion of important phases.

Standard	**IEC 61508** [6]
Method / Framework	The main part of IEC 61508 defines a framework for risk assessment without prescribing a specific method or set of methods. An additional part, IEC 61508-5 "Examples of methods for the determination of safety integrity levels" gives detailed guidance and examples of methods which may be used. Here the foreword explicitly mentions that the methods presented are only intended as examples and source material and suitability needs to be investigated before their application. For the risk determination quantitative approaches (fault tree) and qualitative approaches (risk graphs) are presented.

Table 3.4 Overview of risk assessment described in ISO 26262 [3]

Standard	**ISO 26262** [3]
Quantitative / Qualitative	Like IEC 61508, ISO 26262 follows for most parts a qualitative approach. Only for the assessment of hardware, where historical data is of use, quantities approaches are utilized. The topic of likelihood during the concept phase (in the HARA) is handled by assuming that the failure will always happen. Considered factors in the likelihood are therefore the likelihood to a) being in a situation where the failure leads to a hazard and b) not being able to control the failure. This is used as an initial input in the rigorous of the process and required risk reduction. The initial assessment is checked at specific points during the process. In addition to that, reuse supports an impact analysis where an assessment can be conducted if the initial risk assessment is still valid or needs a rework.
Level of application	While there is guidance on the application of ISO 26262 to software, hardware and even the semiconductor level, there is a strong focus on the initial risk assessment of an (at least assumed) function at the vehicle level. Subsequent steps are done based on this initial risk assessment and based on the automotive safety integrity level resulting from the initial HARA.
Method / Framework	As shown in Table 3.1 and Table 3.2, ISO 26262 made for its second edition the decision to focus on the definition of a risk assessment framework and reduce the mentioning or guidance on methods. ISO 26262-9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analyses contains an overview of methods, divided into qualitative, quantitative and in top-down (Deductive, start from a known effect and identify possible causes) / bottom-up (Inductive, start from known causes and identify possible effects) approaches.

Table 3.5 Overview of risk assessment described in IEC 62443 [2]

Standard	**IEC 62443** [2]
Quantitative / Qualitative	Compared to the safety standards IEC 61508 and ISO 26262, IEC 62443 does not contain guidance on how to rate risks. While there is guidance for the risk assessment process, there is a disconnect from the risk assessment to the assignment of the protective needs (Security Level Target, SL-T). There are some risk matrixes given in the informative part of IEC 62443, but there is no scale for impact given and the likelihood rating is not defined. This can be explained by the fact that different organization might have a different level of accepted risks and due to the less universal impact categories of financial damage and confidentiality of industrial secrets an organization might accept a higher risk. All informative guidance is only on the quantitative scale.

Standard	IEC 62443 [2]
Level of application	IEC 62443 contains two stages for the risk assessment. The Initial cyber security risk assessment is used to identify the worst-case risks, based on the major impacts. This can be used to divide the system into zones and conduits. A zone is structuring systems with similar risk profiles and conduits describe the connections between zones. In addition, the initial risk is compared to the organization's tolerable risk. If the initial risk is higher than the organization's tolerable risk, a detailed cyber security risk assessment needs to be conducted. For the detailed analysis, IEC 62443 points to other standards like ISO 31000, NIST SP 800-39, and ISO/IEC 27005.
Method / Framework	IEC 62443 has a very strong focus on the framework aspect. For methods, only references to other standards are given. Regarding the framework, a detailed flow with steps, inputs and outputs is defined. Here, a focus is on identification of threats and vulnerabilities, and evaluation of impact and likelihood. The process is iterative and needs to be repeated until the risk level is below the tolerable risk level

Table 3.6 Overview of risk assessment described in ISO/SAE 21434 [7]

Standard	ISO/SAE 21434 [7]
Quantitative / Qualitative	Regarding ISO/SAE 21434 the trend from IEC 62443 is continued. Where safety standards utilize at least for some parts a quantitative scale, this is not used at all for security. There are first approaches like FAIR [4] but this is not yet state of the art. ISO/SAE 21434 follows a complete qualitative approach. Impact assessment is divided into at least the four categories safety, financial, operational and privacy. Regarding likelihood there are different approaches proposed, depending on the detail level, e.g., where during concept phase approaches based on attack potential are proposed later more detailed approaches utilizing Common Vulnerability Scoring System (CVSS) are presented
Level of application	ISO/SAE 21434 prescribes a set of activities which can be combined to identify the aspects of risks, impact and likelihood, depending on the level different aspects can be utilized, e.g., at the beginning likelihood might be determined as abstract attack potential, where later an assessment based on known vulnerabilities and potential attack paths is conducted
Method / Framework	ISO/SAE 21434 only contains a framework. Compared to IEC 62443 even the flow is left open. For the activities input, output and objectives are defined, but the additional steps are left open. Regarding impact levels for safety impact ISO/SAE 21434 proposed to utilize severity and controllability from ISO 26262.

Summarized, most observed standards adapt a more framework / objective based description of their risk assessment. This gives an opportunity since new approaches and tools can be easier integrated.

In addition, there is a gap between security and safety risk assessments. Security risk assessments are without a standardized risk rating scheme, since tolerable and intolerable risks depends on organizational values. For example, if an organization is willing to accept a higher risk, lower security measures can be chosen than for a company with less risk acceptance. For standards, were security for safety-critical systems is considered, this leads to the challenge of how to transfer and exchange results. In most cases, the tolerance of safety risks depends not an organizational view, but rather on a societal view.

3.2 System Development Lifecycle

Regarding the lifecycle (independent of system, software or hardware), there is the difficulty to define a reference model that is flexible enough to adapt to newer approaches towards system development while maintaining a rigorous set of activities and ensuring a review of certain processes. We see here an increase in flexibility towards newer development lifecycles.

Considering the Software part of ISO 26262, the 2011 version did not mention agile development at all. This was changed in the 2018 version of ISO 26262. Both versions contain a software reference process model based on the V-Model which is shown in Figure 3.2.

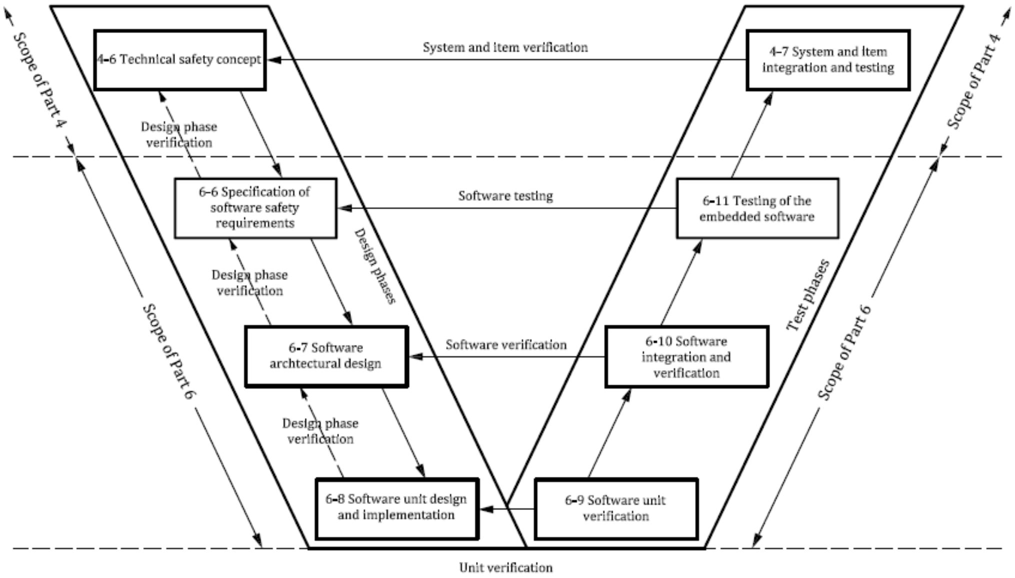

Scope of Part 4
4-6 Technical safety concept
System and item verification
4-7 System and item integration and testing
Scope of Part 4
Design phase verification
6-6 Specification of software safety requirements
Software testing
6-11 Testing of the embedded software
Design phases
Design phase verification
Test phases
Scope of Part 6
6-7 Software archtectural design
Software verification
6-10 Software integration and verification
Scope of Part 6
Design phase verification
6-8 Software unit design and implementation
6-9 Software unit verification
Unit verification

Figure 3.2 Reference phase model for the software development (From ISO 26262-6) [3], [5].

ISO 26262-6:2011 contained the following requirement:

> **5.4.2** *The tailoring of the lifecycle for product development at the software level shall be performed in accordance with ISO 26262-2:2011, 6.4.3.4, and based on the reference phase model given in Figure 3.2.*

This meant that the process how to develop software needed to be based on the given process model which is shown in Figure 3.2 and was therefore mostly based on the V-Model. If another software reference model was used it had to be argued why a model which was not based on the reference model was more suitable and why requirements 5.4.2 did not have to be fulfilled. Therefore, in ISO 26262:2018, this requirement was removed and instead the following note was added to the figure:

> ***NOTE 1*** *Development approaches or methods from agile software development can also be suitable for the development of safety-related software, but if the safety activities are tailored in this manner, ISO 26262-2:2018 6.4.5 is considered. However, agile approaches and methods cannot be used to omit safety measures or ignore the fundamental documentation, process or safety integrity of product rigour required for the achievement of functional safety*

This change allows more freedom but also makes the checking of rigour engineering processes more complex. Where in the past, a workflow based on a standard could be developed and checked, we need to consider now a more open approach where the fulfilment and compliance with objectives and conduction of certain activities are checked.

Table 3.7 contains an overview of the lifecycles presented in the identified project-relevant standards. This is based on an investigation into the identified standards and knowledge from ongoing discussion regarding the development of standards.

Table 3.7 Overview of lifecycles in standards

Standard	Lifecycle
IEC 61508	Does not contain a lifecycle model, especially since there is the goal of a basic safety standard, e.g., to be applicable to multiple domains. Discussion is ongoing if the next version should contain informative guidance towards the connection between safety and systems engineering, including a lifecycle.
ISO 26262	Contains in the latest (2018) version a reference lifecycle model based on the V-Model with notes and guidance if other lifecycles or approaches are to be used.
IEC 62443	Contains a lifecycle model for the development of industrial applications. Regarding component and system development guidance is not existing.
ISO/SAE 21434	Lifecycle is based on ISO 26262 with points where security might require a more iterative and adaptive approach.

There is a trend towards on the one side a stronger integration from safety and security towards system engineering, on the other hand, less strict requirements regarding the applied lifecycle model. Especially with the emerging safety-oriented agile and security-oriented DevOps approaches, we assume that this trend will continue. This makes the development of workflow management tools more difficult but also requires more tool interaction which is currently not yet supported.

3.3 Protective (Safety & Security) Requirements Catalogue, Failure Detection & Diagnosis

In most cases, standards try to stay technological neutral and therefore no guidance on protective (safety & security) requirements are given (see Figure 3.3). The notable exception here is IEC 62443, which contains a set of functional security requirements (FSR). The assumption is that in most cases the lifetime of a standard is longer than the validity of guidance on protective (safety & security) requirements. While ISO/SAE 21434 does not contain any guidance at least for failure detection & diagnosis, IEC 61508 and ISO 26262 do contain guidance. Here, the important topic of fault reaction is approached by defining a minimum time for fault reaction and dividing this into the time required for fault detection and fault handling. To summarize, while no standard contains technical requirements regarding their topics, the degree of guidance is ranging from none to functional requirement level.

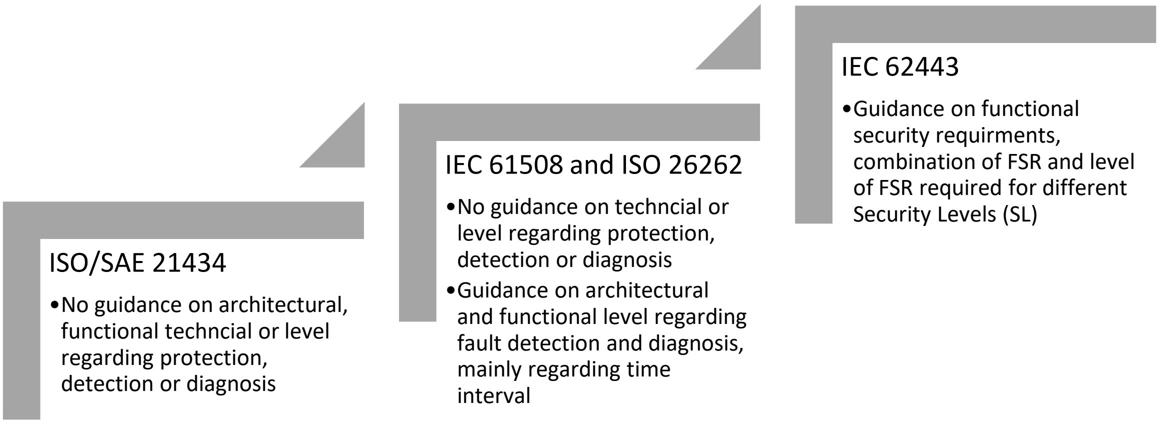

ISO/SAE 21434
•No guidance on architectural, functional techncial or level regarding protection, detection or diagnosis
IEC 61508 and ISO 26262
•No guidance on techncial or level regarding protection, detection or diagnosis
•Guidance on architectural and functional level regarding fault detection and diagnosis, mainly regarding time interval
IEC 62443
•Guidance on functional security requirments, combination of FSR and level of FSR required for different Security Levels (SL)

Figure 3.3 Protection, detection or diagnosis requirements in standards.

In general, we see here one challenge of safety and security standardizazion, the goal to provide a strong framework for the achievement of safe and secure systems, which needs to be balanced with allowing technical progress and being on a level where the described content stays “state of the art” for a substantial amount of time.

Chapter 4 Conclusion

We currently see a strong movement in safety and security standards. This is caused by new approaches towards system engineering and new technologies which require a greater flexibility and automation. But even considering these changes in standardization there are still gaps caused by:

- Risk assessment approaches at different levels between safety and security and transferability in the case of multi-concern systems are not supported. In addition, risk assessment is mainly based on qualitative approaches and new approaches regarding quantitative assessment [4] are not yet taken up for standardization.
- Lifecycle approaches in standardization change from strict requirements to more flexible references. There is the challenge to keep up with the ongoing evolution towards more flexible lifecycles without losing any rigour.
- Protection, detection and diagnosis requirements are difficult to integrate in standardisation due to the different speeds of technical evolution compared with standardization. Still guidance in this direction is required and there are considerations if faster forms of publications can be used for such topics. As example for the ISO/SAE 21434 [7], ISO and SAE are developing supportive documents as PAS (Publically Available Specification) which collects information in a faster way which can be updated more frequently.

References

[1] VALU3S Consortium, "Deliverable D6.5 - Initial report on the results of the standardisation survey (methods, tools, concepts suggested by the standards)." VALU3S Consortium, Aug. 30, 2020.

[2] International Electrotechnical Commission, *IEC 62443: Industrial communication networks – Network and system security*.

[3] International Organization for Standardization, *ISO 26262:2018 Road vehicles - Functional safety (FDIS)*. 2018.

[4] Jack Freund and Jack Jones, *Measuring and Managing Information Risk - A FAIR Approach*. Elsevier, 2015.

[5] International Organization for Standardization, *ISO 26262:2011 Road vehicles - Functional safety*. 2011.

[6] International Electrotechnical Commission, *IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems*. 2010.

[7] ISO/TC 22/SC 32, *ISO/SAE DIS 21434 Road vehicles — Cybersecurity engineering*. ISO - International Standardization Organization, 2020.

www.valu3s.eu

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.