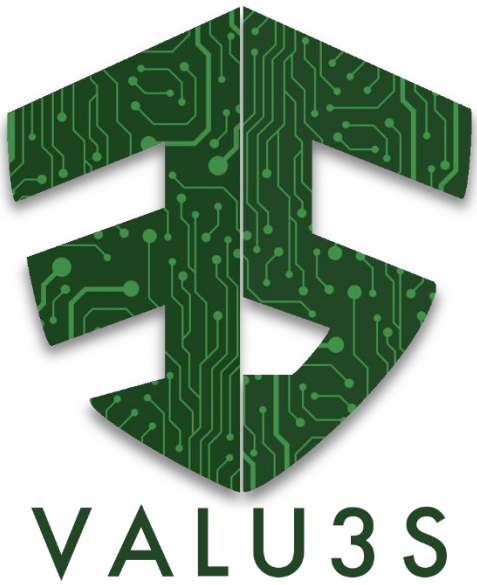


Verification and Validation of Automated Systems' Safety and Security

Report on the Activities Conducted to Disseminate VALU3S Results to Different Standardization Groups

Document Type	Report
Document Number	D6.22
Primary Author(s)	Ricardo Ruiz (RGB)
Document Date	2023-04-28
Document Version	1.3 (Final)
Dissemination Level	Public (PU)
Reference DoA	2022-12-14
Project Coordinator	Behrooz Sangchoolie, behrooz.sangchoolie@ri.se, RISE Research Institutes of Sweden
Project Homepage	www.valu3s.eu
JU Grant Agreement	876852

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 are able to 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 in order 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, 13 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 standardization 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* (25 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, spol. s r.o.	CAMEA	Czech
IKERLAN S. COOP	IKER	Spain
R G B MEDICAL DEVICES	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
CARDIOID TECHNOLOGIES LDA	CARDIOID	Portugal

Executive Summary

This report is written as part of the activities within Task 6.3 which focuses on standardization activities. The objective of this task is to plan and implement all the actions that relate to the establishment of links and interactions with some standardization bodies. Results obtained in VALU3S can be an opportunity to influence the work that the bodies involved in the developments of new standards are carrying out. Some VALU3S partners have been active in several standardization groups related with the industrial implementation of regulations and have therefore contributed to the discussion on the development of new standards with novel approaches, particularly in what concerns the interaction and coordination between safety, security, privacy and performance of Cyber-Physical Systems (CPSs).

An initial identification of relevant standards and corresponding application domains addressed in VALUE3S is presented in Table 22 of the Grant Agreement [1]. The purpose of this deliverable is to make the reader aware of how the activities conducted and reported during this last Y3 year have contributed to obtaining the dissemination of VALU3S results to different standardization groups.

This deliverable also reshapes and finalizes the work presented in previous deliverables:

Deliverable number	Title	Lead beneficiary	Dissemination level	Due month
D6.5	Initial report on the results of the standardisation survey (methods, tools, concepts suggested by the standards)	AIT	CO	4
D6.9	Initial plan on dissemination of VALU3S results to different Standardisation groups	RGB	CO	12
D6.10	Final report on the results of the standardisation survey (methods, tools, concepts suggested by the standards)	AIT	CO	12
D6.17	Final plan on dissemination of VALU3S results to different Standardisation groups	RGB	CO	24

1. D6.5 “Initial report on the results of the standardization survey (methods, tools, concepts suggested by the standards) ” [2] gives an overview about the ongoing survey of standards and standardization related to the work conducted in VALU3S. Based on a list of initially identified standards, a first survey was conducted in D6.5 in order to collect relevant standards and start the evaluation of relevant methods, tools and approaches related to the work.

2. D6.9 “Initial plan on dissemination of VALU3S results to different Standardization groups” [3] defines the initial plan on standardization activities as well as dissemination of the project results to different Standardization groups.
3. D6.10 “Final report on the results of the standardization survey (methods, tools, concepts suggested by the standards)” [4] reviews the status and ongoing trends regarding the relevant methods, tools and concepts of other standards that were identified as important regardless of the ones found in D6.9. The deliverable presents which standards, methods and topics are relevant to the work conducted in VALU3S to identify potential gaps and trends regarding safety and security standards.
4. D6.17 “Final plan on dissemination of VALU3S results to different Standardisation groups” [5] describes the actions that were taken up till month 24 to bring awareness to Standards Development Organizations (SDO) on how the standards could be improved.

In this deliverable, “D6.22 - Report on the activities conducted to disseminate VALU3S results to different Standardization groups”, we document the work plan and activities carried out during the project. For these purposes, this deliverable identifies concepts that emerge from VALU3S works and are relevant to selected standards which are in development or revision. The result of the work is shown in Chapter 3 and describing actions taken to identify proposed actions in order to cause a stronger impact on those standards, by identifying potential gaps in them.

Contributors

Ricardo Ruiz Fernández	RGB	Erwin Kristen	AIT
Ricardo Nolasco	RGB	Stylianos Basagiannis	UTRCI
Behrooz Sangchoolie	RISE	Peter Folkesson	RISE
David Miguel Ramalho Pereira	ISEP	Sina Borrami	BT (ALSTOM)
Antonio González	RGB	Katia Di Blasio	INTECS
Christoph Schmittner	AIT		

Reviewers

Peter Folkesson	RISE	2023-03-24
Christoph Schmittner	AIT	2023-04-10
Behrooz Sangchoolie	RISE	2023-04-21, 2023-04-28
Katia Di Blasio	INTECS	2023-03-24, 2023-04-14

Revision History

Version	Date	Author (Affiliation)	Comment
0.1	13.02.2023	Ricardo Ruiz (RGB)	Table of contents
0.2	06.03.2023	Ricardo Ruiz (RGB)	First incomplete version
0.3	10.03.2023	Ricardo Ruiz (RGB)	Second version
0.4	17.03.2023	Behrooz Sangchoolie	2nd version Commented
0.5	20.03.2023	Ricardo Ruiz (RGB)	Third Version (reviewed)
0.6	08.04.2023	Ricardo Ruiz (RGB)	Corrections after first review
0.7	17.04.2023	Ricardo Ruiz (RGB)	Corrections after second review
0.8	19.04.2023	Ricardo Ruiz (RGB)	Corrections after second review
0.9	21.04.2023	Behrooz Sangchoolie (RISE)	Review of the final draft, while making formatting changes and adding additional comments.
1.0	25.04.2023	Ricardo Ruiz (RGB)	Final Review.
1.1	25.04.2023	Behrooz Sangchoolie (RISE)	Review of the second final draft.
1.3	25.04.2023	Behrooz Sangchoolie (RISE)	Final version of the report to be submitted.

Table of Contents

List of Figures

List of Tables

Acronyms

ANSI	American National Standards Institute
AI	Artificial Intelligence
CAL	Cybersecurity Assurance Level
CEN	Comité Européen de Normalisation. *English:* European Committee for Standardization
CMD	Connected Medical Device
CPS	Cyber-Physical Systems
CS	CyberSecurity
D	Deliverable
GDPR	General Data Protection Regulation
FDA	Food and Drug Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMDRF	International Medical Device Regulators Forum
ISO	International Organization for Standardization
IVDR	In Vitro Diagnostic Medical Devices Regulation
KPI	Key Project Indicator
MDCG	Medical Device Coordination Group
MDD	Medical Devices Directive
MDR	Medical Device Regulation
NIS	Network and Information Systems
RAMS	Reliability, Availability, Maintainability, Safety
RMI	Repair and Maintenance Information
RoSPAV	Report on standardization prospective for automated vehicles
SAMD	Software as a Medical Device
SCP	Safety, Cybersecurity and Privacy
SDO	Standards Development Organization
SME	Small and Medium Enterprises
TAF	Target Attack Feasibility
TC	Technical Committees
TF	Task Force
UL	Underwriters Laboratories
V&V	Verification and Validation

Chapter 1 Introduction

This deliverable describes the actions that have been implemented in relation to the establishment of links and interactions with standardization bodies. VALU3S has shown to be an opportunity to influence ongoing developments in standardization efforts being conducted by the identified bodies. VALU3S partners have surveyed the standardization landscape and have been active in several standards which detail the industrial implementation of regulations and can therefore contribute with novel approaches, particularly in what concerns the interaction and coordination between safety, security and privacy of CPSs.

1.1 Structure of the Deliverable

This deliverable describes the actions carried out in the final year of the project and intends to serve as a motivation to understand how the activities conducted and reported contributed to "disseminate VALU3S results to different standardization groups".

Chapter 2 describes the actions taken by standardization bodies with regards to project related matters.

Chapter 3 has several sections: Section 3.1 comments on the Monthly Communications meetings that have taken place and have served to progress in management issues in relation to WP6 activities; Section 3.2 describes the results of a survey submitted to partners about their participation in standardization works; Section 3.3 describes how work has been continuously performed regarding identifying the standardization landscapes for the application of domains addressed in VALU3S; Section 3.4 refers to training sessions focused on standards. Training sessions have proved to be relevant for increasing the awareness of the consortium towards the importance of incorporating the standard requisites for the future commercial exploitation of its results.

Chapter 4 explains the results of the plans defined for influencing standards and standardisation initiatives, as described in the Conclusions Section of D6.9 [3]. It follows up with the works carried out in Year 3. Chapter 5 concludes this deliverable and summarizes the main achievements of the described work.

Chapter 2 Actions Taken by Standardization Bodies

2.1 Evolution from D6.9 Deliverable

The initial version of the action plan was presented in deliverable D6.9 [3], which, at the same time, got inspiration from D6.10 [4]. Since standardisation is influenced by the ongoing technological, industrial, and societal development, we adapted our plans and we decided to not follow some points included in the initial plans of D6.9, but we included some points that were not initially considered. Besides the changing circumstances, this was also influenced by opportunities in standardisation, e.g., when an SDO decides that a standard will be revised or a new standard needs to be developed, this offers an opportunity to contribute and influence. Moreover, we decided to introduce certain standards as "training sessions" to the consortium as a highly relevant activity to do in the project.

2.2 Conclusions from D6.9 Deliverable

D6.9 [3] describes the achievements from month 12 to month 24 and identifies partners' interest in 41 standards. For 12 of these standards, more than one partner showed interest. Regarding inputs to standards, 13 partners considered they were able to provide inputs to the standardisation work. In that deliverable, concrete conclusions were drawn from the results of the surveys carried out.

As a follow up of D6.9, several actions were launched in parallel with the established action plans:

- Raising awareness to relevant standards.
- Participating in related SDOs.
- Generating interest in VALU3S works related to standardization issues.

2.3 Main activities by Standardization Bodies

This deliverable describes the actions taken by standardization bodies with regards to project related matters; some of them are a consequence of VALU3S contributions. The main actions carried out in the project are described in Chapters 3 and 4.

Actions taken by standardization bodies:

- While SAE J3061 [6] had a lifecycle that was directly copied from ISO 26262 [7] and, therefore, also a direct mapping; there were some issues, especially regarding the stronger focus on operations for cybersecurity and the wish to support additional lifecycle, beside the V-Model. ISO/SAE 21434 [8] together with ISO 26262 Ed2 give guidance on potential interaction points. An ISO task force was started on both activities with the goal to support harmonization and coordination in ISO road vehicle standards. IEC TR 63069 (bridging safety and security) started work on the next version in IEC TC65 WG20. In these activities project partners have been

involved and we have presented status and achieved impact regarding standards on co-engineering of safety and cybersecurity.

Actions taken by VALU3S partners in the project:

- We have connected the project demonstrators as well as their methods and tools used to enhance their activities to standards and standardisation activities.
- We have connected the project tools to standards that motivate their usage. For example, if a fault injector is enhanced, the fault injection is recommended in **ISO 26262**.
- Linking of the tools and methods with the included standard list has been carried out in the publicly accessible web-based VALU3S repository [9].
- A description of current services, data and processes has been considered in the medical sector.
- Security standards in the medical sector mainly, but applicable to other domains, have been subject to special attention, particularly those that relate to cybersecurity and safety risk management. A list of standards has been considered and it is presented in Chapter 3.
- The partners' involvement in standardisation initiatives has been monitored and supported and has contributed to the results of Chapters 3 and 4.
- The main focus of the activities described in the submitted standardisation deliverables has been on describing ways to influence positively the development of standards, based on real life cases.
- Regarding awareness of standards, the standardisation training has served their purpose and has been published.
- We have also taken into consideration standards that study the co-engineering of safety and cybersecurity. Here is a some of the details connected to these standards:
    - The automotive security standard, **ISO/SAE 21434** [8].
    - The unofficial predecessor of ISO/SAE 21434, **SAE J3061** [6], include a complete interactive lifecycle, which was easy to develop since the process and lifecycle used by **SAE J3061** [6] was based on **ISO 26262** [7].
    - One of the Task Force (TF) works on harmonization between safety (**ISO 26262**), automated driving (**ISO PAS 21448** [10]) and cybersecurity (**ISO/SAE 21434**). Their work is ongoing to evaluate and harmonize these standards on the level of activities, terminology and work products.
    - In addition to this, on the level of the basic safety standard **IEC 61508** [11] and **IEC 62443** [12]**,** there is an ongoing work on IEC Technical Committee 65 WG 20 on "Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security" which is bridging between **IEC 61508** [11] and **IEC 62443** [12].
    - In the railway domain, the **TS 50701** "Railway applications – Cybersecurity" was published, which connects the pre-existing Reliability, Availability, Maintainability, Safety (RAMS) with cybersecurity. For this, the **TS 50701** [13] gives guidance on the application of the **IEC 62443** [12] in the railway sector and on the connection with Railway Safety Management.

2.4 Task 6.3 in the Context of VALU3S Project

Task 6.3 has received inputs from other tasks and has delivered results to others. Figure 2.1 depicts some connections.

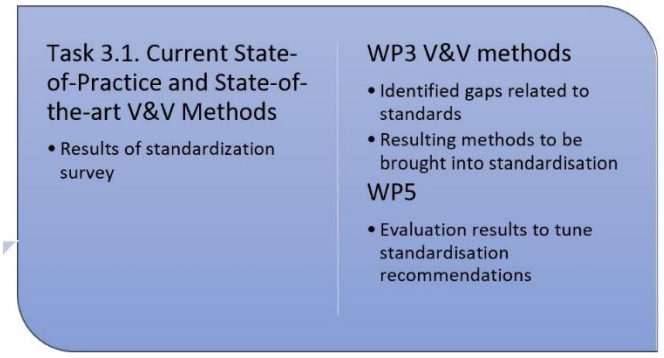


Figure 2.1. VALU3S Inter-Task Connection

The result of the comprehensive gap analysis on SCP V&V methods, tools and concepts detailing strengths and weaknesses of the existing standards shows that there are gaps directly related to standards. This work targets Project Objective 7 and KPI 10, which are further explained below:

- Objective 7 is defined as "to revisit and identify the weaknesses of relevant safety and security standards and develop a concrete strategy to influence the development of new standards. Influence the development of different standards targeting SCP of systems within the domains of the project through an active participation in related standardisation groups. This is complemented by identification of gaps in different Standards with regards to V&V methodology to conduct safety, cybersecurity and privacy- related V&V of automated systems."

- KPI 10 is defined as "VALU3S aims to conduct a comprehensive gap analysis on SCP V&V methods, tools and concepts detailing strengths and weaknesses of the existing standards through active participation in at least 14 standardisation initiatives which are also used as platforms to disseminate the results of VALU3S."

The pursued plans have facilitated the achievement of the above objectives. With coordination meetings and continuous monitoring of standardisation activities, we have achieved the expected progress regarding these project objectives.

Chapter 3 Actions Carried Out in the Final Plan

3.1 Management by the Communication Team

On the 11th of June 2020, the first Communication Team meeting took place, which dealt with standardization and other WP6 tasks (dissemination, communication, and exploitations). The purpose of these meetings has been to cover the communication, dissemination, exploitation, and standardization actions to guarantee the impact of the results obtained in VALU3S. The team has been holding monthly meetings, with the participation of RISE as project coordinator together with the project communication manager, WP6 task leaders and partners responsible for WP6 tasks and deliverables. As a result of these meetings, specific actions have been carried out on (among others) the standardization activities. The meetings have proved to be very useful as brainstorming sessions and have helped bringing new ideas on the subject. So far, 35 communication meetings have taken place.

3.2 Collection of Surveys on Standard Related Issues

Some surveys were distributed to all partners in the elaboration of deliverables D6.5 [2], D6.9 [3] and D6.10 [4]. They proved to be a very useful tool to collect information on particular standard-related issues, such as asking about the partners availability to participate/ influence in a particular SDO, in relation to a particular standard. They have proved to be useful to analyse how a particular standard in a certain domain could be the source of inspiration to complement other standards in other domains (cross-fertilization). These surveys have been used as a tool in the following months to gain deeper knowledge on specific standard related issues.

As a result, two action plans were conducted during the 2nd year of the project:

- The first action plan set the study focus on three standards: ISO 26262 [7], ISO/PAS 21448 [10] and ISO/SAE 21434 [8].
- In the second action plan, a number of standards were selected as a second choice for study. These were ISO 10218-1 [14], ISO 10218-2 [15], ISO 14971 [16], IEC 61508 [11], and IEC 62443 [12]. Note that, in addition to what was already planned for in D6.9, ANSI/UL 4600 [17] and DO-178C [18] were included in our focus study.

These standards were prioritized and have been made aware to the VALU3S community. They have also been analysed in depth for improvements, as VALU3S could bring awareness of gaps and limitations to the SDOs.

In the second action plan, we have identified those standards whose content have proven to be of particular interest to various VALU3S partners. Training sessions have been carried out to bring awareness about them to the rest of partners.

3.3 Description of the Standardization Landscape

The landscape description is conceived to provide an overview from top to bottom of those standards that are most relevant in a particular domain and, also, to show the evolution of the respective standardization landscape. Not all the identified standards are subject to analysis in VALU3S. In the following description, those standards relevant for the scope of VALU3S are presented. We have focused on providing the landscape of each particular domain of interest in the project because it has helped us target the right standardization groups. This has been an ongoing work and we have finally included the standardisation landscape of the pending domains in this deliverable. Besides, in addition to safety standards, we have included cybersecurity standards applicable to the domains. Note that, although it was not the purpose of this deliverable to explain in detail each of the standardization landscapes, here we have presented the general schema and those aspects more related to VALU3S involvement. Some subsections are described in greater detail than others, particularly when a certain aspect like cybersecurity is emphasized. We have noted that standardization challenges are increasingly cross-domain in areas such as Security, AI, or Dynamic and heterogenous systems. Standardization groups are starting to develop awareness of this, such as ISO/IEC JTC 1/SC 42 - Artificial Intelligence [19].

3.3.1 Automotive Standardization Landscape

Figure 3.1 shows the relevant standards for this domain.

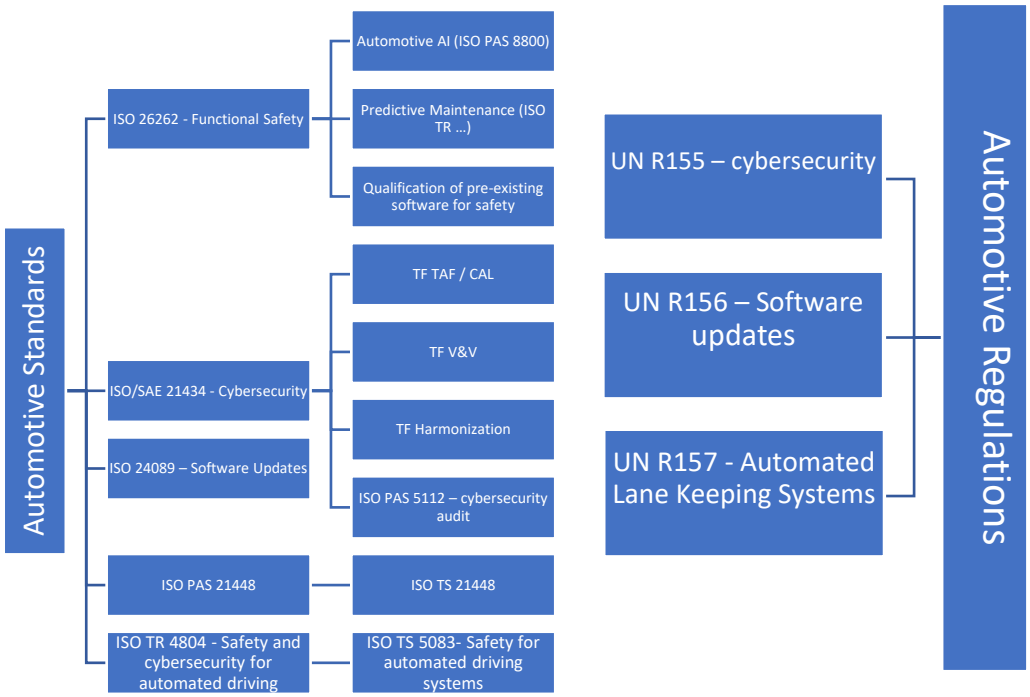


Figure 3.1. Automotive Standardization Landscape

The following points briefly summarize the areas and ongoing developments with VALU3S involvement:

- Automotive AI ISO PAS 8800 [20], safe usage of AI.
- Predictive Maintenance to ensure safe behaviour.
- TAF (Target Attack Feasibility) / CAL (Cybersecurity Assurance Level) (ISO/TC 22/SC 32/WG 11), both topics which were presented as informative parts in ISO/SAE 21434 [8].
- V&V, Harmonization, addressing differences between ISO/SAE 21434, ISO 26262 and other automotive standards regarding lifecycle, terms and definitions.
- ISO 24089 [21] – Software Updates
- ISO PAS 5112 [22] – Cybersecurity audit
- ISO TS 5083 [23] – Safety for automated driving systems

There are also activities with no VALU3S involvement:

- TC22 SC31 [24] – extended vehicle, connected car communication, sensor interfaces, V2X, V2Grid, remote diagnosis, web services (ISO 20078 [25]) Web services next edition), remote repair and maintenance information (RMI).
- WG10 – extended vehicle time-critical applications – RExVeS, ISO TR 23132 [26]
- ISO TC22 AG1 (Automated Driving Ad-Hoc Group) – goal: roadmap.
- ISO TR 4609 [27] – Report on standardization prospective for automated vehicles (RoSPAV)

In the remaining of this subsection, we provide additional details about the security standards related to cybersecurity in the automotive domain.

Section 5.1.3 of UN Regulations No. 155. Cyber security and cyber security management system [28]

The Approval Authority or Technical Service shall refuse to grant the type approval with regard to cyber security where the vehicle manufacturer has not fulfilled one or more of the requirements referred to in paragraph 7.3., notably:

a) The vehicle manufacturer did not perform the exhaustive risk assessment referred to in paragraph 7.3.3.; including where the manufacturer did not consider all the risks related to threats referred to in Annex S. Part A;
b) The vehicle manufacturer did not protect the vehicle type against risks identified in the vehicle manufacturer' s risk assessment or proportionate mitigations were not implemented as required by paragraph 7;
c) The vehicle manufacturer did not put in place appropriate and proportionate measures to secure dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data;
d) The vehicle manufacturer did not perform, prior to the approval. appropriate and sufficient testing to verify the effectiveness of the security measures implemented.

ISO PAS 5112 Road vehicles -Guidelines for auditing cybersecurity (CS) Engineering [22]

- Focused on the organizational and process level.
- Product level not in the scope.
- Based on ISO 19011 "Guidelines for auditing management systems".
- Extends the guidance with automotive domain specific information.
- Aims to audit processes based on ISO/SAE 21434 and gives guidance on audit process, requirements, and qualifications.

Cybersecurity Assurance - 1S0/IEC 5888 [29]; Approach based on ISO/IEC 15408 Common Criteria [30]

Challenges

- Common Criteria aims at system and process, automotive industry differentiates.
- Common Criteria defines a "standardized" target of evaluation, high variability on item level.
- Common Criteria is static and does not consider safety.

Opportunities

- Established approach, existing experts and assessment schemes.
- Well suited for core cybersecurity elements.

Cybersecurity Assurance – ISO/SAE 8475 [31]

- TAF (target attack feasibility) means to express expected strength of CS controls in cybersecurity requirements.
- CAL (cybersecurity assurance levels) means to describe requirements on development rigor and on cybersecurity assurance.
- Open issues: Decomposition and composition; Relation to Risk and stability vs. dynamic behaviour.

3.3.2 Medical Standardization Landscape

The European regulation for healthcare sector has changed from old directives to new regulations. Figure 3.2 shows these changes and identifies the specific regulations.

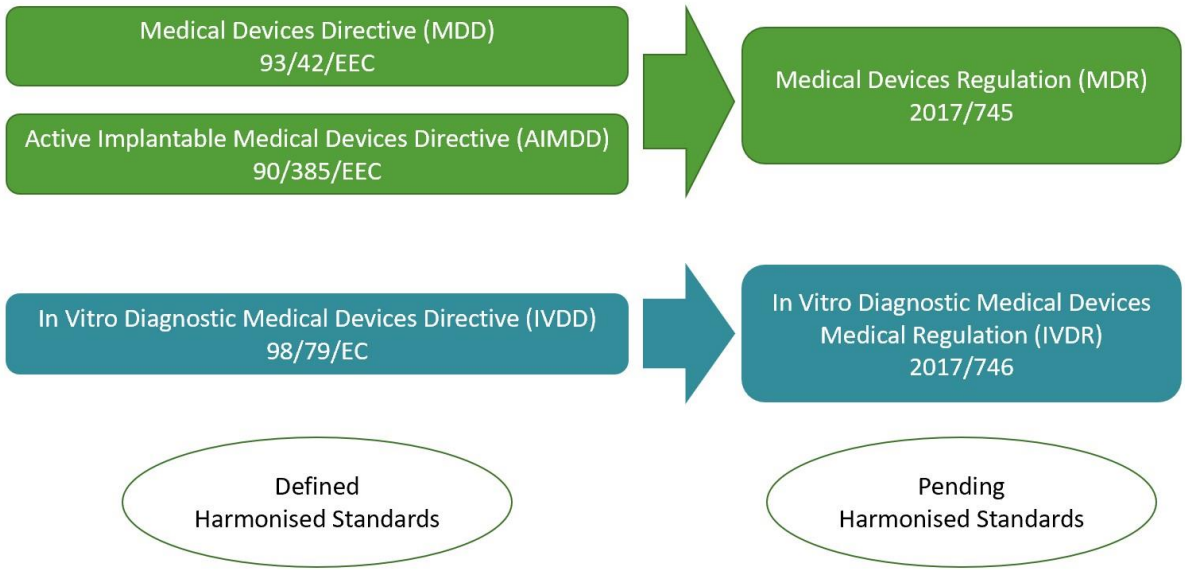


Figure 3.2. Healthcare Regulation Change

The Medical Devices Directive (MDD) 93/42/EEC has been effective until May 26th, 2017. Since then, the new Medical Devices Regulation (MDR) 2017/745 [32] applies, although there is a transitory period in which all certificates issued under the MDD before the MDR fully applies may remain valid under certain conditions. From that date, all devices placed on the market must be in conformity with the MDR.

The 26th of May 2021 was the date of application of the Medical Device Regulation (MDR), which marks an important milestone for the medical devices sector. The new regulation for medical devices provides additional benefits including a strengthened notified body system, a new database enabling more transparency, a unique device identification system facilitating supply chain traceability, stricter clinical evidence requirements and more. "The new regulations are welcomed by the industry as these will strengthen patient safety and the existing robust approval system of our sector", says Serge Bernasconi, CEO of MedTech Europe. The challenges this industry currently faces include:

- Non-harmonised interpretation and application of MDR rules across the EU,
- Limited capacity among Notified Bodies, especially for certification of new and innovative devices,
- Uncertainties with regards to pending discussions on the rules and agreements between the EU and other countries, especially Switzerland, a key supplier of medical devices to the European Union, and
- Unpredictable recognition of MDR certifications at international level vis-à-vis regulatory approvals from other jurisdictions.

Until these challenges are resolved, roadblocks will continue to limit this sector ability to seamlessly supply certified devices under the new rules. This is especially true for many small and medium enterprises (SME), who contribute to a significant portion of Europe medical device innovations. Such challenges need ongoing attention and work by the EU Commission and Member States if Europe is to ensure a workable system in the long-term.

There is a transition period for devices certified according to the old Directives. In vitro diagnostic products are those reagents, instruments, and systems intended for use in diagnosis of disease or other conditions, including a determination of the state of health, in order to cure, mitigate, treat, or prevent disease or its sequelae.

The Amending Regulation (EU) 2023/607 [33] has been recently published in the Official Gazette of the EU, by which Regulations (EU) 2017/745 [32] and (EU) 2017/746 - In Vitro Diagnostic Medical Devices Regulation (IVDR) - [34] , are modified with regard to the transitional provisions that enters into force with immediate effect.

This Amending Regulation has the following effects:

1. **Extension of the MDR transition period until December 31, 2027 and until December 31, 2028** depending on the risk class of the legacy devices that will be determined in accordance with the MDR classification rules. The extension is subject to several conditions.
2. **Extension of the validity of the certificates provided that the conditions for the extension of the transitional period are met**. Likewise, certificates that have already expired after May 26, 2021 may be considered valid if additional conditions are met.
3. **Transfer of appropriate surveillance to MDR Notified Bodies by 26 September 2024 at the latest.**
4. **Introduction of a temporary exception until May 26, 2026 from the requirement of the quality management system certificate for class III implantable custom products,** subject to conditions.
5. **Suppression of the product marketing deadline ("sell off" clause) from both the MDR and the IVDR**, which will allow products that have been placed on the market before or during the transition periods and that remain in the supply chain remain available without a time limit.

Changes to the MDR/IVDR introduced by the Amending Regulation will allow more time to transition to the Regulations under certain conditions. These "short-term" measures are intended to address immediate emergencies and as such are not intended to address all challenges facing the industry. Nor do they mark the end of planned actions to "make our regulatory systems work".

Medium and long term actions

As the European Commission stated to the Health Ministers during the EPSCO meeting on March 14 2023 [35], medium and long-term actions are now planned. These include (by 2027 at the latest) a broader assessment of regulatory frameworks to ensure their sustainability, but also include:

1. Increased capacity and number of notified bodies.

2. Continued implementation of measures to enhance the capacity of notified bodies and ensure the availability of medical devices and in vitro diagnostic medical.
3. Pilot project on scientific advice for clinical development strategies for high-risk products.
4. Tailor-made solutions for orphan products - work has already started at the Medical Device Coordination Group (MDCG) level
5. Creating a regulatory environment that encourages innovation and helps SMEs: Commission surveys under EU4Health are expected to start shortly.

Other key points and messages to manufacturers:

- Art. 97 of the MDR, described in document 2022-18 of the MDCG, is no longer an option today.
- Strongly recommendation to actively submit dossiers under the MDR and IVDR and not wait until May 2024.
- It is important to monitor the success of the implementation of the amendment throughout the EU: please contact us in this regard and especially if you encounter any difficulties (e.g., validity of certificates, conditions to benefit from the extension of the deadline, etc)
- The European Commission will shortly publish a question-and-answer document in which aspects of the application of the modifications will be clarified.

For the old directives, there are defined harmonised standards. However, for the new regulations the harmonization process is currently in progress. The standards are similar, but normally the new editions of the standards will be harmonised with the new regulations. Figure 3.3 shows the relevant standards for devices used in the healthcare area.

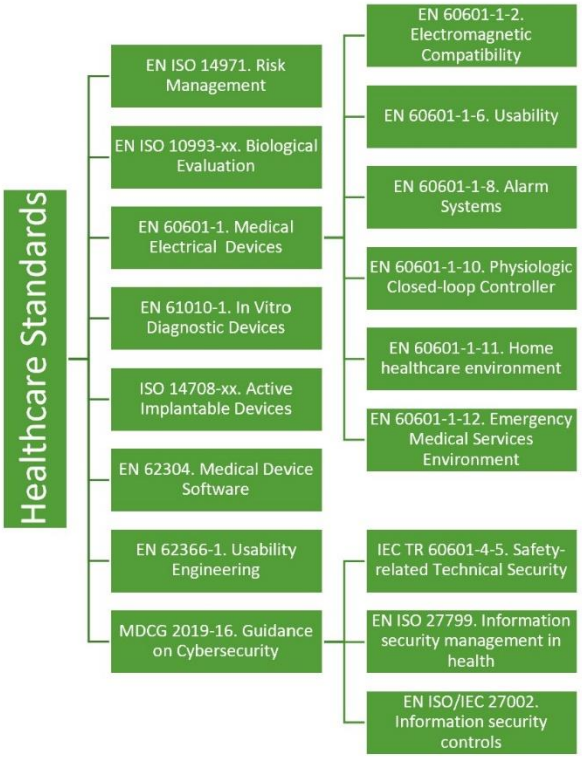


Figure 3.3. Medical Standardization Landscape

The following bullet points briefly describe those standards related to VALU3S:

- MDCG 2019-16 [36]. Guidance on Cybersecurity for Medical Devices.
- EN ISO 14971 [16]. Risk Management.
- EN 60601-1 [37]. Medical Electrical Devices.
- EN 62304 [38]. Medical Device Software.
- EN 62366-1 [39]. Usability Engineering.

The following sub-sections extends the description of the standards directly or indirectly related to cybersecurity in the medical domain.

Standards with Impact on Cybersecurity

In Year 3, we have been working on reviewing and identifying the main standards that could have relevant impact on cybersecurity requirements. Particularly in the Medical domain, but not only. The new MDR and IVDR bring EU legislation into line with technical advances, changes in medical science and progress in law-making. We have structured (e.g., considering requirements for manufacturers and operators) summarizing key aspects found in MDCG 2019-16 rev. 1 (July 2020) as well as in MDR/IVDR Regulations (especially Annex I), also providing pointers to other relevant regulations (GDPR [40], NIS2, Cybersecurity Act [41]).

- There are no harmonized standards on cybersecurity, but it is a requirement of 2017/45 regulation.
- European Union has issued a guidance on cybersecurity that includes references to relevant standards.
- IEC TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices. This standard provides detailed technical information for security features in medical devices used in medical IT networks.
- ISO 27799 standard [42] gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s). By implementing ISO 27799, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

In year 3, one of our main objectives has been to focus on cybersecurity aspects and:

- Collect, analyse and synthesize project requirements for cybersecurity aspects from a technical, legal, clinical and ethical perspective.
- Perform a study of the state of the art regarding the cybersecurity baseline, as to identify gaps and possible areas of improvement.
- Define a set of end-user, functional and non-functional requirements for contributing to the future (outside VALU3S scope) overall objective of developing the cybersecurity tools (also in connection with legal and ethical requirements traced in WP2), so that it is user-friendly, trustworthy, reliable and scalable.

Cybersecurity Requirements in the MDR

MDR requests manufacturers of medical devices to consider the state of the art when designing, developing and upgrading medical devices across their life cycle. Manufacturers should demonstrate state-of-the-art within their decisions (based on applicable standards, guidance, their own proprietary knowledge and publicly available scientific/technical information) while demonstrating appropriateness to proportionally address security risk.

Figure 3.4 shows the MDR requirements applied on cybersecurity and other related regulations.

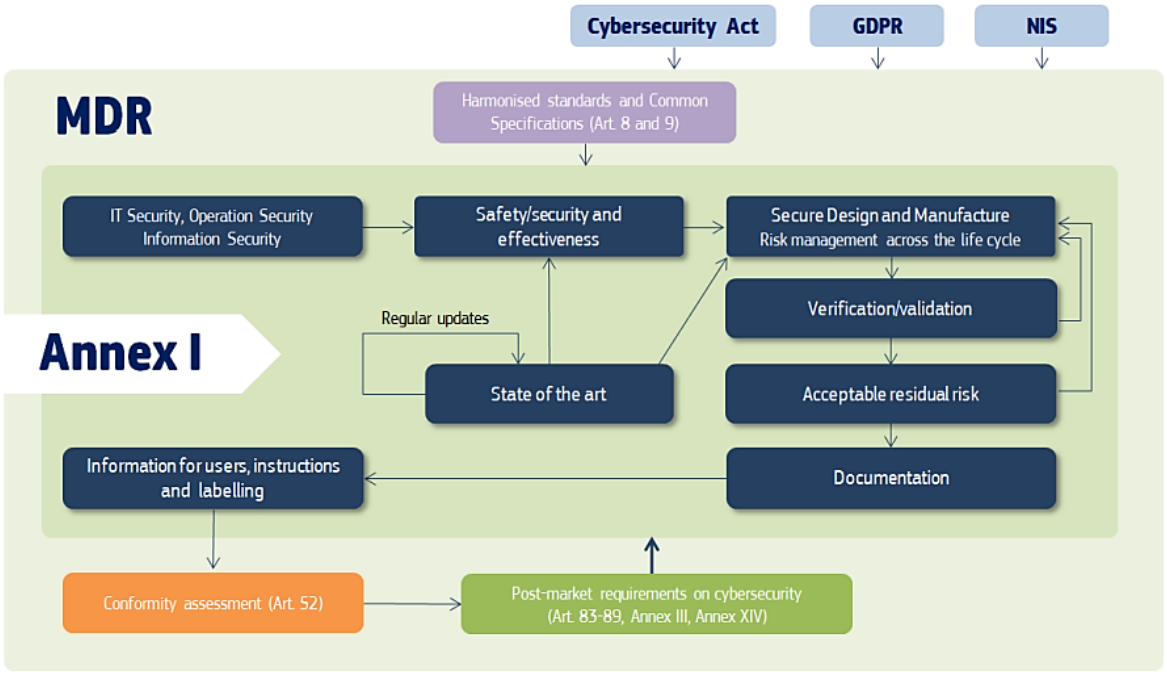


Figure 3.4. MDR Requirements on Cybersecurity

The manufacturer should be particularly aware of the following MDR provisions in the context of cybersecurity:

- Privacy and data protection: Article 62.4(h): General requirements regarding clinical investigations conducted to demonstrate conformity of devices.
- Conformity assessment procedures: Article 52.
- Post-market surveillance system of the manufacturer: Article 83.
- Post-market surveillance plan: Article 84.
- Post-market surveillance report: Article 85.
- Periodic safety update report: Article 86.
- Reporting of serious incidents and field safety corrective actions: Article 87.
- Trend reporting: Article 88.
- Analysis of serious incidents and field safety corrective actions: Article 89.
- Technical documentation: Annex II.
- Technical documentation on post-market surveillance: Annex III.
- Clinical evaluation and post-market follow-up: MDR Chapter VI and Annex XIV.

Table 3.1 shows the above listed MDR requirements separated between pre-market and post-market activities.

Table 3.1. MDR Requirements on Cybersecurity

Pre-market activities	Post-market activities
Risk management (Annex 1)	Risk management (Annex I)
Establish Risk Control Measures (Annex 1)	Modify Risk Control Measures /Corrective Actions/Patches (Annex 1)
Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex 1)	Validation, Verification, Risk Assessment, Benefit Risk Analysis (Annex 1)
Technical Documentation (Annex II and III)	Maintain and update a Post-market Surveillance Plan and Post-market Surveillance System (Article 83 and 84)
Conformity Assessment (Article 52)	Trend Reporting (Article 88)
Establish a Post-market Survellance Plan and Post-market Surveillance System (Article 83 and 84)	Analysis of Serious Incidents (Article 89)
Clinical evaluation process (Chapter VI)	Post-Market Surveillance Report (Article 85)

MDR/IVDR General Safety and Performance Requirements

In the EU, both the MDR and IVDR requirements mandate consideration of medical device cybersecurity, and the MDCG 2019-16 guidance directs manufacturers on how to fulfil all the relevant general safety and performance requirements from Annex I of the MDR 2017/745 [32] and IVDR 2017/746 [34] with regard to cybersecurity. Figure 3.5 shows these requirements.

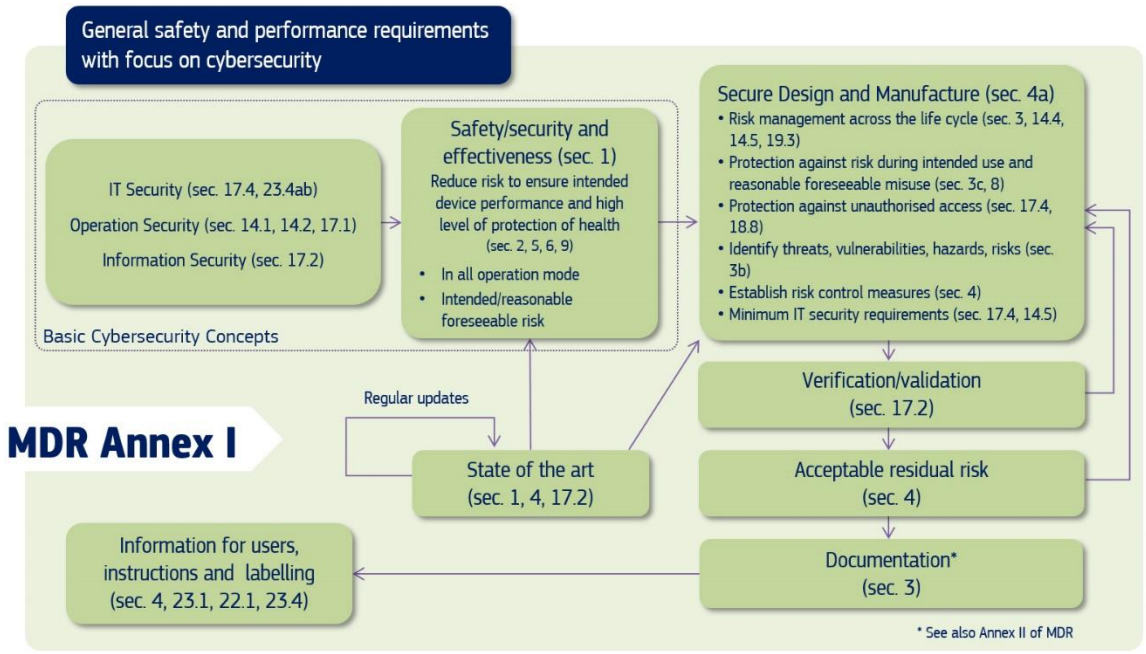


Figure 3.5. MDR Annex I Requirements on Cybersecurity

Table 3.2 lists the relevant general safety and performance requirements from Annex I of the MDR 2017/745 [32] and IVDR 2017/746 [34] with regard to cybersecurity.

Table 3.2. Annex I Requirements on Cybersecurity

Main Topic	Section number MDR Annex1	Section number IVDR Annex 1
Device Performance	1	1
Risk reduction	2	2
Risk management system	3	3
Risk control measures	4	4
Minimisation of foreseeable risks, and any undesirable side-effects	8	8
Combination/connection of devices/systems	14.1	13.1
Interaction between software and the IT environment	14.2.d	13.2.d
Interoperability and compatibility with other devices or products	14.5	13.5
Repeatability, reliability and performance	17.1	16.1
Development and manufacture in accordance with the state of the art, taking into account the principles of development life cycle, risk management, including information on security verification and validation	17.2	16.2
Minimum IT requirements	17.4	16.4
Unauthorised Access	18.8	
Lay persons	22.1	
Residual risks: (information supplied by the manufacturer}	23.1.g	20.1.g
Warnings or precautions (information on the label)	23.2.m	20.2.m
Residual risks, contra-indications and any undesirable side-effects, (information in the instructions for use)	23.4.g	
Minimum IT requirements: (information in the instructions for use)	23.4.ab	20.4.1.ah

Other Requirements Sources

The content of this section is extracted from chapter 6 of MDCG 2019-16 guidance.

At EU level, the following legislative acts are relevant to the cybersecurity of medical devices or to operators dealing with protecting or processing of personal data stored in medical devices and might apply in parallel to the Medical Devices Regulations:

- Network and Information Systems (NIS) Directive [43]. It provides legal measures to boost the overall level of cybersecurity in the EU. See also Annex I of MDCG 2019-16 "Mapping of IT security requirements to NIS Directive Cooperation Group measures".
- General Data Protection Regulation (GDPR) [40]. It regulates the processing by an individual, a company or an organisation of personal data relating to individuals in the EU.
- Cybersecurity Act [41] [44] [45]. It introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes.

Other cybersecurity guidance can be useful for comparison to find gaps in MDCG 2019-16 guidance:

- US FDA "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" [46]
- IMDRF Medical Device Cybersecurity Guide [47]

Cybersecurity and Safety Risk Management

Figure 3.6 is included in Annex IV of MDCG 2019-16 guidance, and shows the relationship between Processes for Cybersecurity Risk Management and Safety Risk Management.

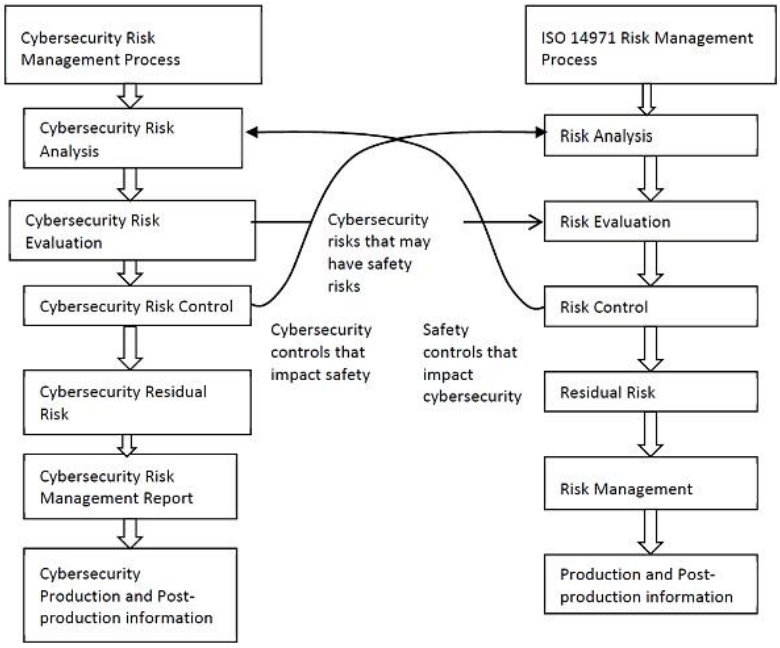


Figure 3.6. Relationship between Cybersecurity and Safety Risk Management

Current Services: Data / Services / Processes

- The need for cybersecurity standards is clear: large volumes of data stored and maintained in healthcare organisations.
- Accelerated digital transformation of healthcare systems.
- Healthcare - Top 5 sector most affected by cybersecurity threats in 2021.
- Threat Groups: Ransomware, Malware, Threats against data, threats against availability.
- A methodological and technical cybersecurity framework designed for healthcare services that use Connected Medical Devices (CMDs). Such a framework is aligned with the MDR and IVDR regulations, but strengthens the adherence to requirements concerning safety, performance and

IT security. This is also relevant in other domains, and some of the standards mentioned have a multi domain approach.

- In particular, cybersecurity standards will make necessary to:
  1. Identify gaps and introduce new safety and security requirements based on evidence, adapting such requirements to novel technologies (e.g., cloud computing, artificial intelligence).
  2. Identify security-related hazard categories and risk acceptance criteria according to the classification of medical devices.
  3. Promote a risk assessment framework built on risk-benefit analyses that responds to the identified requirements and gaps and considers the impacts of novel scenarios on risks (e.g. safety, performance and environmental differences of in-hospital with respect to, remote monitoring of patients).
  4. Provide tools that help mitigate risks and the increase of safety, security and performance of healthcare services relying on CMD /IVD (In Vitro Diagnostic) /SaMD (Software as a Medical Device) with consideration to challenges involving legacy devices.

Other Applicable Standards

Annex III of MDCG 2019-16 includes the following list with other standards than can be relevant:

- EN ISO 14971 Risk Management (Product).
- EN 62304 Software Lifecycle.
- EN ISO 31000 Risk Management (Organisation) or particular standards under ISO 31xxx.
- EN ISO/IEC 27000 Information technology — Security techniques — Information security management systems (ISMS) — Overview and vocabulary.
- EN ISO/IEC 27001 Information Technology – Security techniques – Information Security management Systems – Requirements.
- EN ISO/IEC 60601-1-x.
- IEC 82304-1 Health Software Part 1: General requirements for Product Safety.
- ISO/IEC 80001-1 Application of Risk Management for IT networks Incorporating Medical Devices.
- ISO/IEC 80001-5-1 Application of Risk Management for IT networks incorporating medical device – Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software – Part 5-1: Activities in the product life-cycle.
- IEC/TR 80001-2-2 Application of Risk Management for IT networks Incorporating Medical Devices Part 2-2: Guidance for the Disclosure and Communication of Medical Device Security Needs, Risks and Controls.
- IEC/TR 80001-2-8 Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2.
- ISO/IEC 80001-xx including IEC/TR 80001-2-1, IEC/TR 80001-2-3, IEC/TR 80001-2-4.
- IEC/TR 80001-2-5, ISO/TR 80001-2-6, ISO/TR 80001-2-7 or other.
- EN ISO 62366 / ISO 60601-4 Usability Engineering.

- IEC 62443-4-2 Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.
- IEC 62443-4-1 Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements.
- IEC/TR 60601-4-5 Medical Electrical Equipment – Part 4-5. Safety related technical security specifications for medical devices.

3.3.3 Railway Standardization Landscape

Figure 3.7 shows the relevant standards for devices used in the Railway domain, that are:

- EN 50126-1 Generic RAMS process.
- EN 50126-2 RAMS-System approach to safety.
- EN 50155 Rolling stock – Electronic equipment.
- EN 50129 - Safety related electronic systems for signalling.
- EN 50159 communication in transmission systems.
- EN 50128 – Software for railway control and protection systems.

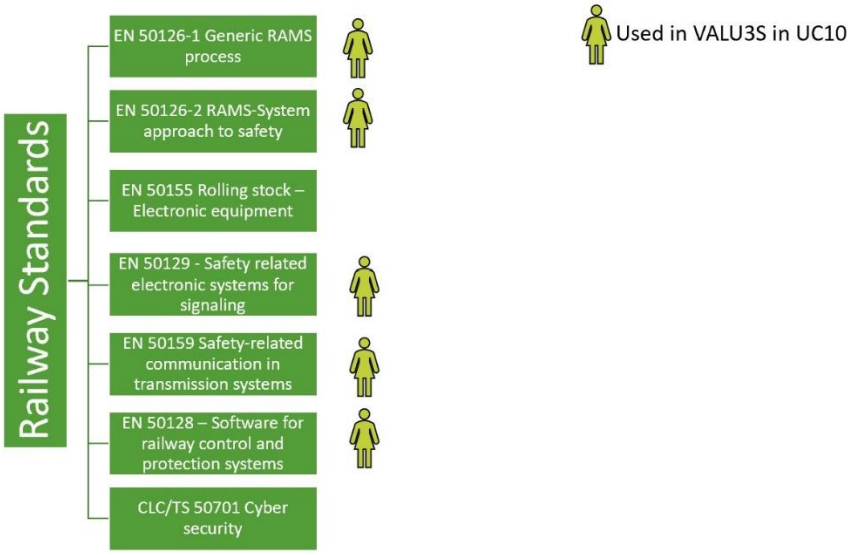


Figure 3.7. Applicable Railway Standards

Figure 3.8 shows possible standards in which areas of improvement can be found in the Railway domain.

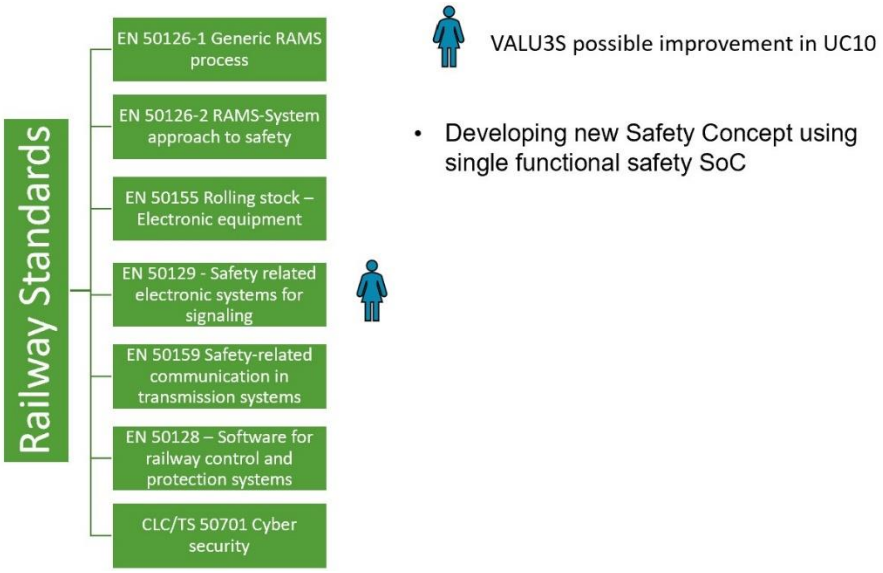


Figure 3.8. Railway Standards Possible Improvement

3.3.4 Industrial Robotic Standardization Landscape

Figure 3.9 shows the relevant standards for devices used in the Industrial Robotic domain.

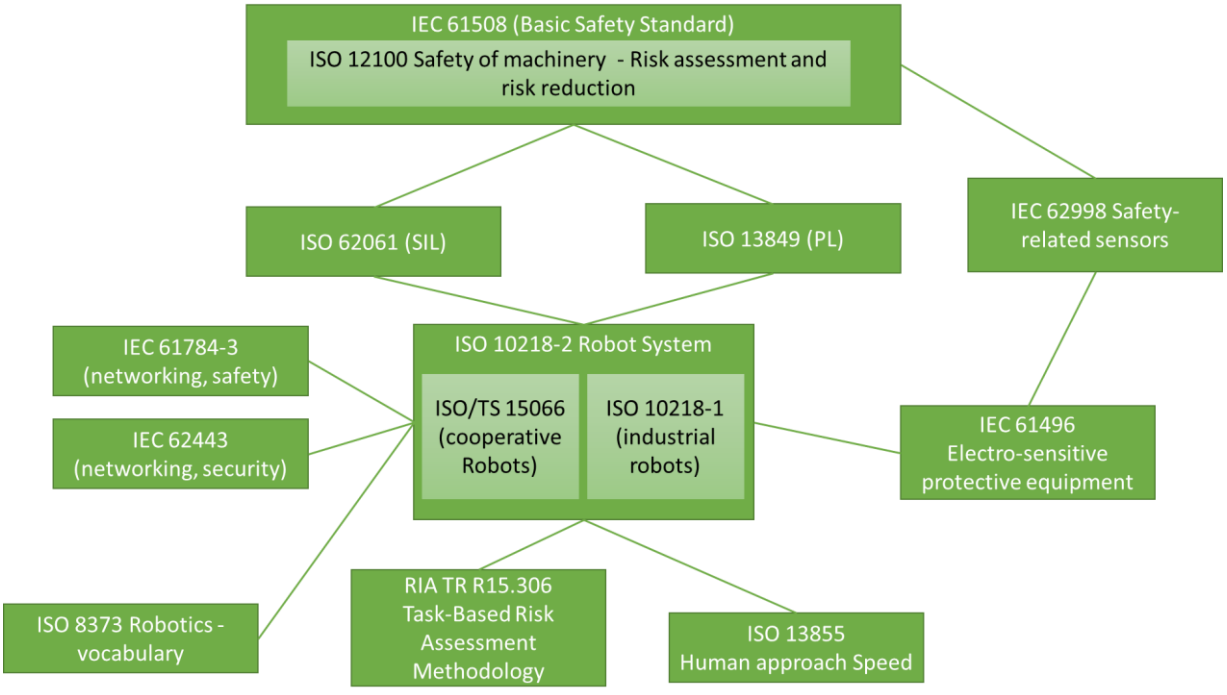


Figure 3.9. Applicable Industrial Robotic Standards

We focus here on industrial robotics, as one of the identified areas of interest for the VALU3S project. The different types of robots are defined in ISO 8373. An industrial robot is defined as "automatically controlled, reprogrammable multipurpose manipulator, programmable in three or more axes, which

can be either fixed in place or fixed to a mobile platform for use in automation applications in an industrial environment". Regarding robotics it needs to be remarked that there are many domains specific standards, partially to integrate robotics into domain specific standard landscapes, partially to address domain specific characteristics and requirements. Examples include IEC 60601-1 [37] which contains safety and performance requirements for medical robots or related, ISO 13482 [48] for personal care robotics.

Regarding industrial robots, an important point is on the integration in the industrial environment for which the terminology of industrial robot system, industrial robot cell and industrial robot line are defined. To summarize this concept:

- an industrial robot system includes the industrial robot and necessary end effectors and machinery, equipment, devices, external auxiliary axes or sensors supporting the robot performing its task.
- an industrial robot cell includes one or more industrial robot systems and extends this with the necessary safeguarded space and protective measures.
- an industrial robot line combines multiple industrial robot cells.

The robot inside the robot system can also be a cooperative robot, e.g., if the task is conducted guided or in interaction with a human. In addition, additional standards like IEC 61496 [49] and IEC 62998 [50] need to be considered regarding the safety related part of sensorics (e.g., light curtain or similar electric safety systems) and regarding the risk assessment there is a linkage trough safety of machinery to the basic safety standard IEC 61508. In addition, besides safety related aspects of networking, also security is increasingly required, e.g., compliance to IEC 62443.

3.3.5 Aerospace Standardization Landscape

Figure 3.10 shows the aerospace standardization landscape.

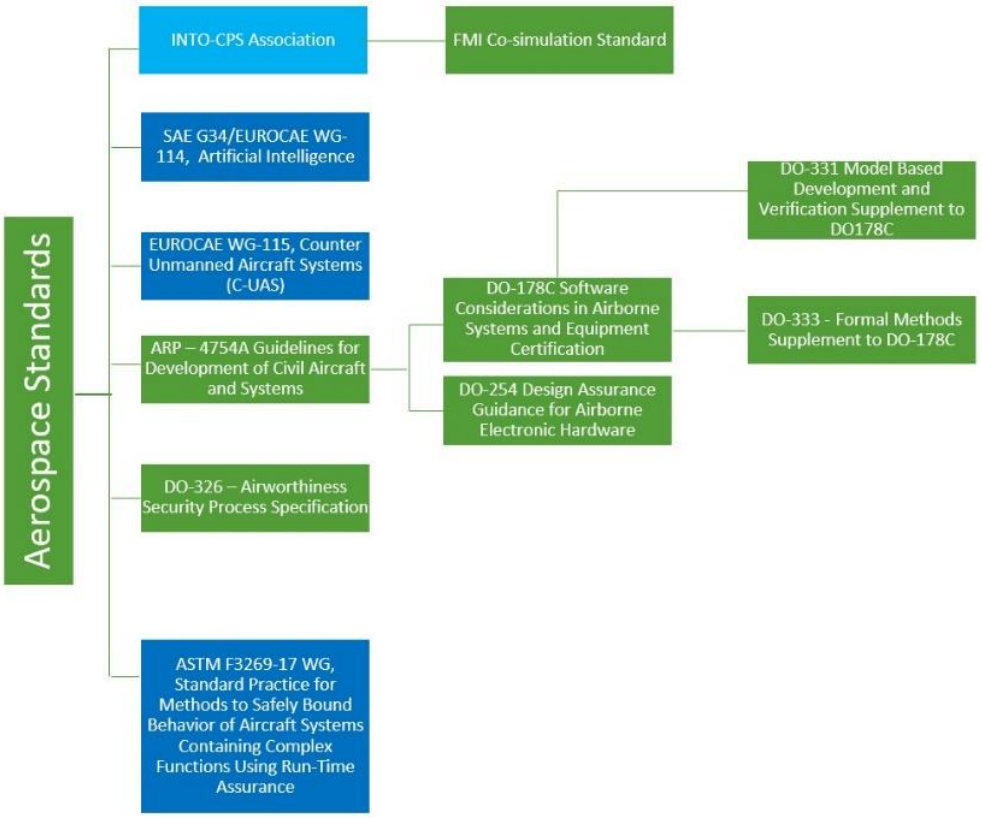


Figure 3.10. Aerospace Standardization Landscape

Figure 3.11 show the main VALU3S involvement in aerospace standardization landscape.

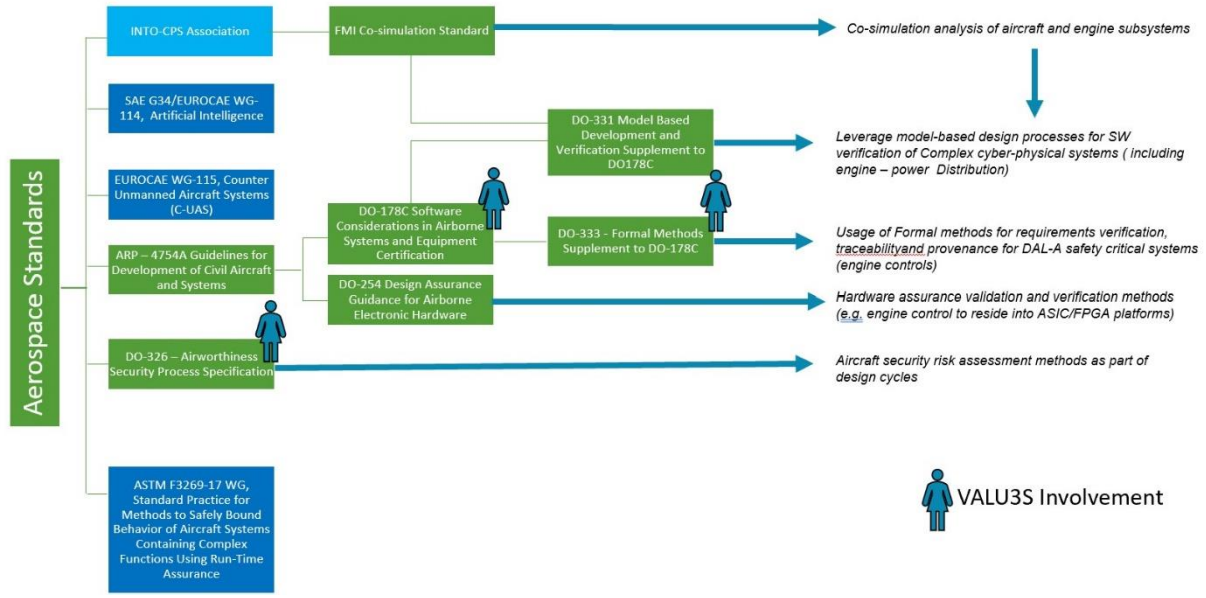


Figure 3.11. Aerospace Standardization Landscape – VALU3S Involvement

Figure 3.12 shows with red stars those standards in which there are opportunities to exploit VALU3S results into ongoing working groups/standardization efforts.

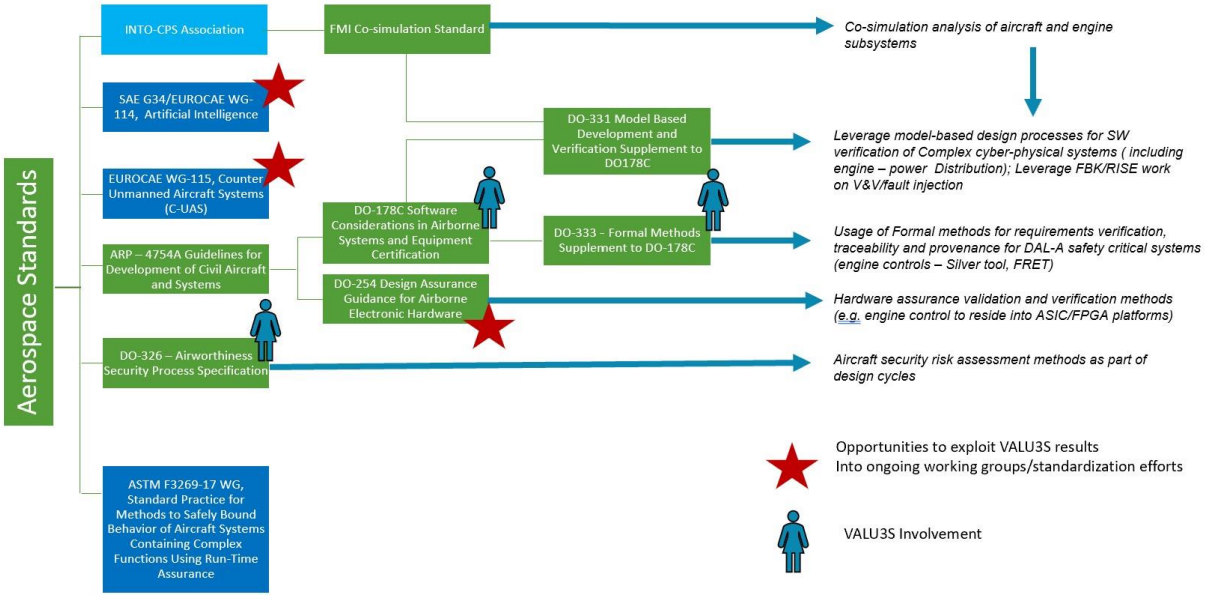


Figure 3.12. Aerospace Standardization Landscape - VALU3S Opportunities

Figure 3.13 show standards in which there are opportunities to present further dissemination of VALU3S results.

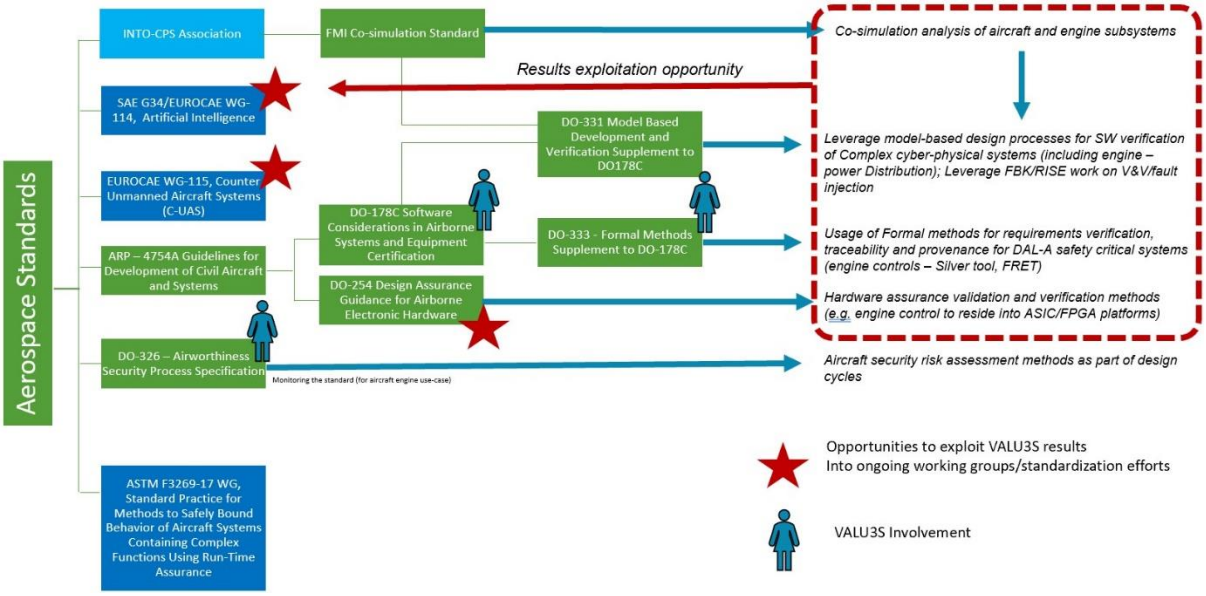


Figure 3.13. Aerospace Standardization Landscape – VALU3S Result Exploitation

Four dissemination events occurred internally in Raytheon Corporation led by Collins Aerospace (UTRC) during the VALU3S project time frame:

- Event included engineers and Fellows (involved in standardization activities) from Collins Aerospace US, Pratt & Whitney, Raytheon Intelligence Space.
- Presentation to the INTO-CPS association in the board of association meeting; validate results and feedback to FMI-standard committee through the association.
- Participation of Collins Aerospace Ireland in SAE technical reports towards new standardization efforts (WG 115, SAE for blockchain applications in aerospace).

The completed actions were:

- Further dissemination and exploitation of results in ongoing standardization working groups.
- Leverage VALU3S project results into new EU funded initiatives of higher TRL level (Innovation Actions) in order to mature VALU3S technology and enable transition to the business units.

3.3.6 Agricultural Standardization Landscape

Figure 3.14 shows the relevant standards for agricultural domain.

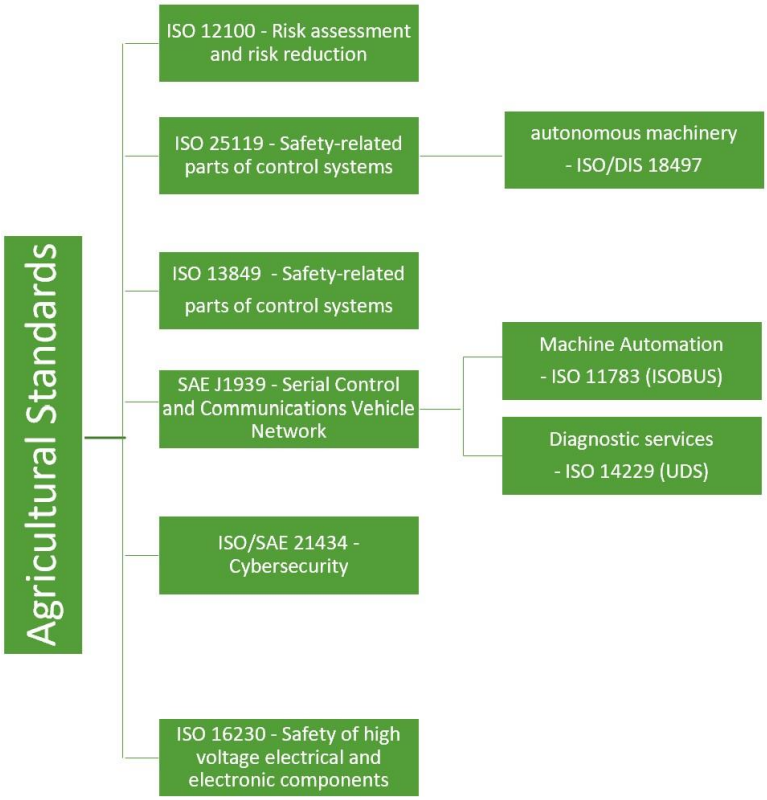


Figure 3.14. Agricultural Standardization Landscape

Standards from other domains are used in agricultural area, as indicated in Figure 3.15.

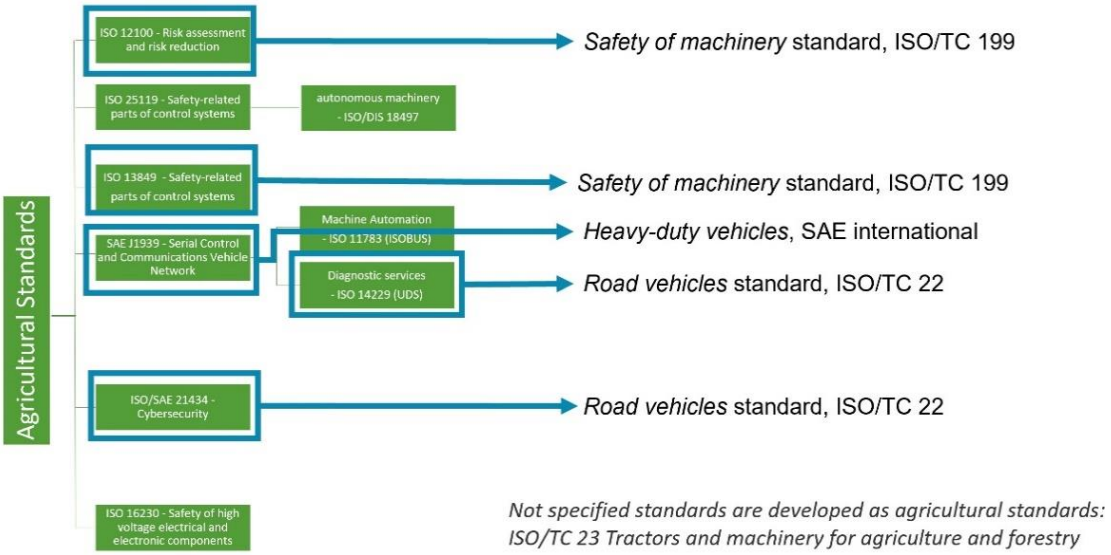


Figure 3.15. Agricultural Standardization Landscape – Using Standards from other Domains

Figure 3.16 shows the application field of the specified standards.

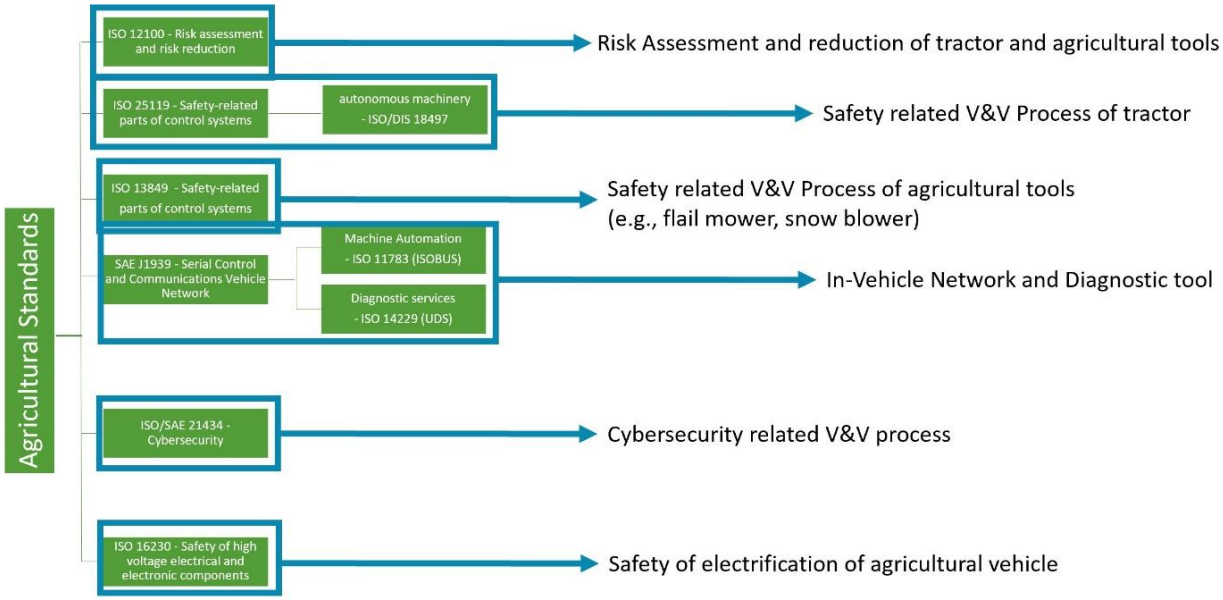


Figure 3.16. Agricultural Standardization Landscape – Standards Usage

The following bullet points briefly describe the areas of VALU3S involvement:

- ISO 12100 [51]- Risk assessment and risk reduction
- ISO 25119 [52]- Safety-related parts of control systems
- ISO/SAE 21434 [8]- Cybersecurity

Figure 3.17 indicates the VALU3S involvement for the ISO 25119 standard [52].

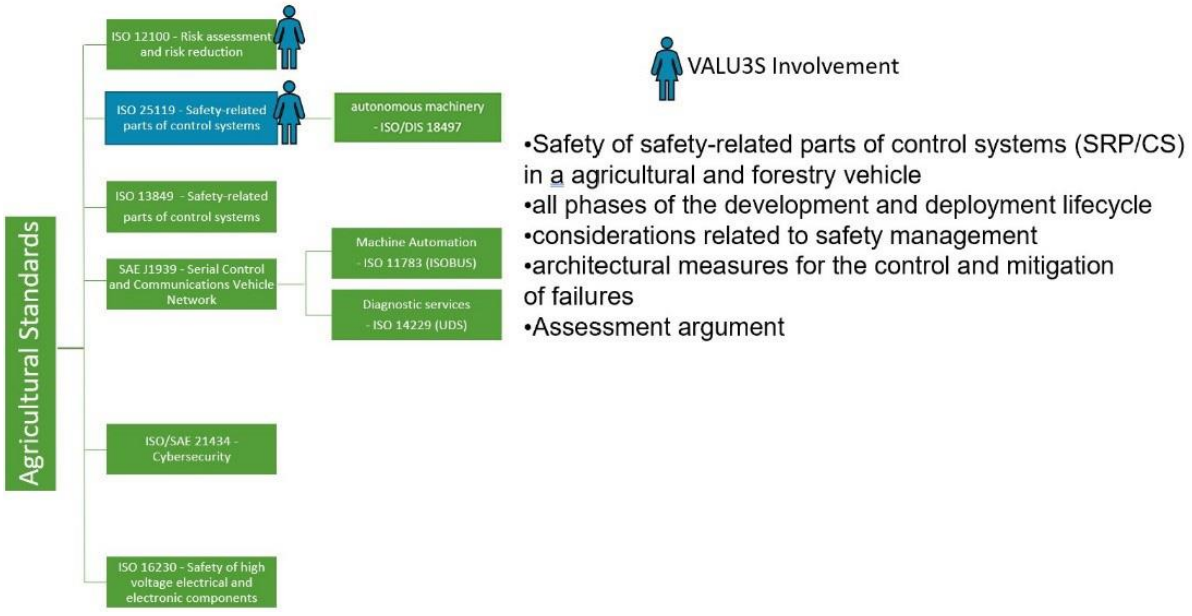


Figure 3.17. Agricultural Standardization Landscape – ISO 25119 VALU3S Involvement

Figure 3.18 indicates the VALU3S involvement for the ISO/SAE 21434 standard.

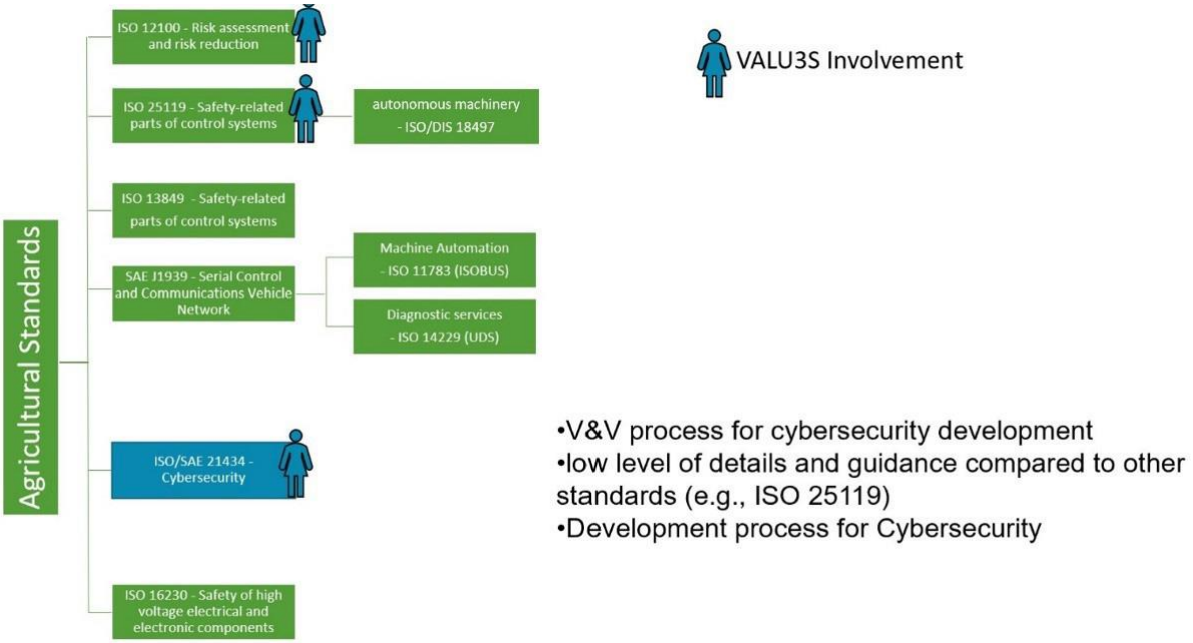


Figure 3.18. Agricultural Standardization Landscape – ISO/SAE 21434 VALU3S Involvement

3.4 Training Sessions about Relevant Standards

The consortium has been allocating time and effort on a series of training sessions on relevant standards used in different domains, in order to bring awareness to VALU3S partners about the existence of such standards, to give some insights into ongoing development and topics addressed. Invitations to a standardization presentation have been sent at least 2 weeks in advance. The purpose has been to try to collect as many attending partners as possible. One of the most interesting outcomes of these meetings has been to receive feedback from the rest of the partners about the way a standard could be applicable in a particular domain, and to promote the active participation of partners in the SDOs. These sessions were recorded and made available for project partners who could not join and used for dissemination purposes.

Table 3.3 lists the training session activities carried out between months M12 and M24.

Table 3.3. Training Sessions about Relevant Standards – Year 2

Date	Description of activity
09/2021	**Title**: Standardisation Training Session 1 - CEN ISO/IEEE 11073: Health informatics - Medical / health device communication standards **YouTube link**: https://youtu.be/7jYzd9oO680 **LinkedIn text used for promoting the training session**: Medical Devices are key for improved wellbeing within our society, and growing to become more and more automated and address ever growing challenging task in medical treatments. Learn more about CEN ISO/IEEE 11073, a standard focused on medical device communication, by watching this VALU3S training session. **Twitter text used for promoting the training session**: Get to know more about communication standards for medical devices by watching this VALU3S training session.
10/2021	**Title**: Standardisation Training Session 2 - ISO/SAE 21434: Road vehicles - Cybersecurity engineering & ISO/DPAS 5112: Road vehicles - Guidelines for auditing cybersecurity engineering **YouTube link**: https://youtu.be/J1mzZpVgNkM **LinkedIn text used for promoting the training session**: Cybersecurity is a fundamental area to develop automated system on which we can trust! Get to know more about relevant standards focusing on this area by watching this training session! **Twitter text used for promoting the training session**: Get to know more about relevant standards focusing on this area by watching this training session
01/2022	**Title**: Standardisation Training Session 3 - ISO 26262: Road vehicles - Functional safety & ISO/PAS 21448 Road vehicles - Safety of the intended functionality (Short overview only) **YouTube link**: https://youtu.be/5gZZJgIIvGM **LinkedIn text used for promoting the training session**: Do you want to get to know ISO 26262 and ISO/PAS 21448, two of the more relevant standards focused on safety? Take the opportunity and watch this video, where Christoph Schmittner, from VALU3S partner AIT, gives a very interesting overview about these two standards. **Twitter text used for promoting the training session**: Want to know more about two of more relevant standards focused on functional safety?
02/2022	**Title**: Standardisation Training Session 4 - DO-178C: Software Considerations in Airborne Systems and Equipment Certification & DO-333: Formal Methods Supplement to DO-178C **YouTube link**: https://youtu.be/ZFVK7xZH6fM **LinkedIn text used for promoting the training session**: DO-178C is the de facto document by which the certification authorities all commercial software-based aerospace systems. Get to know more about this standard, and its associated DO-333 supplement by watching this VALU3S training session **Twitter text used for promoting the training session**: Want to know more about certification of commercial software-based aerospace systems and the applicability of formal methods?
03/2022	**Title**: Standardisation Training Session 5 - ANSI/UL 4600: Standard for Safety for the Evaluation of Autonomous Products **YouTube link**: https://youtu.be/4CcOJUX2aGU **LinkedIn text used for promoting the training session**: Autonomous Systems and products are a main player in the process of making our society more and more digital, helping us to overcome societal tasks with high degree of safety. Get to know more about one of the standards that focus on evaluating fully autonomous products requiring no human driver supervision. **Twitter text used for promoting the training session**: Safe autonomous operation of systems and products is key for the digitalization of our society. Get to know more about one of the standards addressing such safety requirements.

Table 3.4 lists the activities that have been carried out between months M24 and M36.

Table 3.4. Training Sessions about Relevant Standards – Year 3

Date	Description of activity
04/2022	**Title**: Standardisation Training Session 6 - ISO/IEC 15408 standard for IT Security Evaluation. **YouTube link:**: https://www.youtube.com/watch?v=-gzLaktxMmQ&list=PLGtGM9euw6A66ceQbywXGjVoTKEhP-Of7&index=19 **LinkedIn text used for promoting the training session**: **Twitter text used for promoting the training session**:
06/2022	**Title**: Standardisation Training Session 7 - Evolution of the IEEE P7009 Standard: Towards Fail-Safe Design of Autonomous Systems Dr Marie Farrell - Senior Post-Doctoral Researcher Department of Computer Science/Hamilton Institute - Maynooth University - Ireland **YouTube link**: https://www.youtube.com/watch?v=ef1Nv5S7DTY&list=PLGtGM9euw6A66ceQbywXGjVoTKEhP-Of7&index=20 **LinkedIn text used for promoting the training session**: **Twitter text used for promoting the training session**:
10/2022	**Title**: Standardisation Training Session 8 - ISO 25119 Tractors and machinery for agriculture and forestry — Safety-related parts of control systems. The training session will be kindly given by Carlo Ferraresi from ESTE. **YouTube link**: https://www.youtube.com/watch?v=E_wkIQr19VY&list=PLGtGM9euw6A66ceQbywXGjVoTKEhP-Of7&index=21 **LinkedIn text used for promoting the training session**: **Twitter text used for promoting the training session**:
11/2022	**Title**: Standardisation Training Session 9 – "ISO_10218-2_2011 Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration". Prof. Dr. Ahmet Yazici R&D Coordinator of Eskisehir Osmangazi University Director of Center for Intelligent Systems Applications Research(CISAR), Department of Computer Engineering - Eskisehir Osmangazi University - Turkey. **YouTube link**: https://www.youtube.com/watch?v=omTXSI7KZ10&list=PLGtGM9euw6A66ceQbywXGjVoTKEhP-Of7&index=22 **LinkedIn text used for promoting the training session**: **Twitter text used for promoting the training session**:

In summary:

- The goal has been to raise awareness and give an overview about standards which can be relevant for VALU3S work.
- All training session have been recorded and afterwards made available on the project's YouTube channel.
- The duration of the trainings range from 30 minutes to 1 hour.

Figure 3.19 shows the training sessions on relevant standards used in different domains that were carried out.

Figure 3.19. Training Session about Relevant Standards

Chapter 4 Dissemination of Results to SDOs

4.1 Participation of Partners in SDOs

4.1.1 Monitoring of Participation of Partners in SDOs and Gap Analysis of Standards

An Excel file has been set up for monitoring the participation of partners in Standards Development Organizations (SDOs). The excel sheet has made it possible to add, maintain its content, and define specific actions or follow-ups on the activities. Partners have been asked to update the Excel file continuously, every time they participate in SDOs sessions. Table 4.1 shows the type of information requested.

It has been highly encouraged the involvement of VALU3S partners in standardization workgroups to influence the contents, particularly focusing on V&V tools, since there is less focus on tools in recent standards. The works have been done relating the connection between standardisation plan and the VALU3S objectives and Key Performance Indicators (KPI) presented in the Grant Agreement [1].

A database was implemented such that each participation is coupled with a description of what points from VALU3S have been taken to discussion and benefited the initiative, and what topics being addressed in the initiative could be beneficial for VALU3S activities and objectives. However, some concerns have been raised by members in key positions of SDOs, about the sharing of information due to confidentiality issues in the SDO committees. For example, for IEEE standards, the information that is requested in some of the columns is confidential. This is the case for "Summary of Activity", "Suggested follow-up activities", "Topics discussed that may be relevant to VALU3S activities" or "Activities of VALU3S relevant to the topics discussed in the standardization group" which cannot be filled up without breaking the SDO rules. In any case, we believe it is important to show that partners have been active in standardization. Table 4.1 summarizes the participation of partners in SDOs.

Table 4.1. Participation of Partners in SDOs and Gap Analysis of Standards

Date	Description of activity
28.05.2020 - 17.03.2022	**Type of activity:** working group meeting. **Title:** Meetings for ISO PAS 5112 [22], Road vehicles — Guidelines for auditing cybersecurity engineering. **Related Standard:** ISO PAS 5112. **Working Group Active Party/Parties:** ISO/TC 22/SC 32/WG 11 / AIT. **Person involved:** Christoph Schmittner. **Summary of activity:** Developed a Publicly Available Specification (PAS) on how to audit processes and management of automotive cybersecurity with a focus on ISO/SAE 21434 and UN R155. Involved in 16 Working Group Meetings. **Suggested follow-up activities:** Monitor development, involved VALU3S Person was chosen as project lead for development. It is considered to integrate ISO PAS 5112 in next edition of ISO/SAE 21434. **Topics discussed that may be relevant to VALU3S activities:** Audit and Assessment of road vehicle cybersecurity, potential arguments and evidences for achievement and compliance, relation to upcoming regulations. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Cybersecurity analysis, argumentation, V&V and process.
01.05.2020-	**Type of activity:** working group meeting. **Title:** Road vehicles - Cybersecurity Engineering. **Related Standard:** ISO/SAE 21434. **Working GroupActive Party/Parties:** SIS/TK240/AG11 / RISE. **Person involved:** Peter Folkesson, Pierre Kleberger. **Summary of activity:** Participate, reviewed and commented on draft standard. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact.
01.05.2020-	**Type of activity:** working group meeting. **Title:** Road vehicles - Functional Safety. **Related Standard:** ISO 26262. **Working Group Active Party/Parties:** SIS/TK240/AG8 / RISE. **Person involved:** Fredrik Warg. **Summary of activity:** Participated in meetings discussing possible input to next edition. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact.
15.01.2021-	**Type of activity:** working group meeting. **Title:** Road vehicles — Safety for automated driving systems — Design, verification and validation. **Related Standard:** ISO TS 5083. **Working Group/ Active Party/Parties:** SIS/TK240/AG8 / RISE. **Person involved:** Fredrik Warg **Summary of activity:** Participate, reviewed and commented on proposal draft. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact.

Date	Description of activity
01.05.2020-	**Type of activity:** working group meeting. **Title:** Road vehicles - Software Update Engineering. **Related Standard:** ISO 24089. **Working Group /Active Party/Parties:** SIS/TK240/AG11 / RISE. **Person involved:** Peter Folkesson, Pierre Kleberger. **Summary of activity:** Participate, reviewed and commented on draft standard. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact.
01.05.2020-	**Type of activity:** working group meeting. **Title:** Meetings for the SACM (Structured Assurance Case Metamodel) standard by OMG. **Related Standard:** SACM. **Working Group / Active Party/Parties:** OMG's System Assurance Task Force / UCLM. **Person involved:** Jose Luis de la Vara. **Summary of activity:** Provision of input and feedback for the revision of SACM. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S. **Topics discussed that may be relevant to VALU3S activities:** Updates on the metamodels for argumentation and for assurance evidence management. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Assurance and certification.
01.05.2020-	**Type of activity:** working group meeting. **Title:** Meetings for requirements specification guidelines. **Related Standard:** INCOSE Guide for Writing Requirements. **Working Group/ Active Party/Parties:** INCOSE Requirements Working Group / TRC. **Person involved:** Luis Alonso, Jose Fuentes. **Summary of activity:** Input and feedback for requirements specification guidelines. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S. **Topics discussed that may be relevant to VALU3S activities:** Revision and definition requirements quality criteria. **Activities of VALU3S relevant to the topics discussed in the standardization group:** System artefact quality analysis.
01.05.2020-	**Type of activity:** working group meeting. **Title:** Meetings for work on knowledge management by INCOSE. **Related Standard:** INCOSE Knowledge Management & Ontology for Systems Engineering. **Working Group/ Active Party/Parties:** INCOSE Working Group on Knowledge Management / TRC. **Person involved:** Luis Alonso, Jose Fuentes. **Summary of activity:** Contribution to INCOSE's knowledge management approach, covering system V&V. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S. **Topics discussed that may be relevant to VALU3S activities:** Definition of an approach for knowledge management in the scope of systems engineering. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Knowledge-centric system artefact quality analysis, Knowledge-centric traceability management.

Date	Description of activity
Since 2022	**Type of activity:** working group meeting. **Title:** Participation in meetings and work on propagation of VALU3S inputs. **Related Standard:** ISO PWI 8477 Road vehicles — Cybersecurity verification and validation. **Working Group Active Party/Parties:** ISO/TC 22/SC 32/WG 11 / AIT. **Person involved:** Christoph Schmittner. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact.
Since 2018	**Type of activity:** working group meeting. **Title:** Meeting for work on FMI based co-simulation analysis and Digital Twins for aerospace use-cases. **Related Standard:** FMI standard. **Working Group Active Party/Parties:** INTO-CPS association committee and inputs to FMI committee Collins. **Person involved:** (UTRC) Stylianos Basagiannis. **Summary of activity:** Member of the board. Inputs to the future versions of the FMI standard. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S. **Topics discussed that may be relevant to VALU3S activities:** Explore FMI -based co-simulations for aerospace safety critical systems. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Relevant standardization activities that the VALU3S activities and technology has been disseminated internally. Every PoC listed in the excel has been reached out from Collins (UTRC) the past 2 and half years, exploiting directly and indirectly impact of the technology to relevant standardization activities INTO-CPS Association for the FMI standard, DO178C, EUROCAE WG 114 and 115, and ASTM F3269-17.
Since 2021	**Type of activity:** working group meeting. **Title**: Supporting Collins Aerospace with DO-178C Enterprise Tool Qualification. **Related Standard:** DO178C. **Working Group Active Party/Parties:** RTCA DO178C - EUROCAE ED-12C Collins (UTRC) - through Collins US and Collins Italy. **Person involved:** Kyle Ford. **Summary of activity:** TSO Certification Representative. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact. **Topics discussed that may be relevant to VALU3S activities:** WCET tools.
Since 2021	**Type of activity:** working group meeting. **Title:** Industry standards in support of ATM/UTM/C-UAS integration. **Related Standard:** EUROCAE WG-115. **Working Group Active Party/Parties:** EUROCAE WG-115 Collins (UTRC) - through Collins France. **Person involved:** Elias Bitar. **Summary of activity:** Company representative. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S. **Topics discussed that may be relevant to VALU3S activities:** WG-115 is established to develop standards to support the safe and harmonised implementation of Counter-UAS Systems into airport and ANSP systems.

Date	Description of activity
Since 2021	**Type of activity:** working group meeting. **Title:** Artificial Intelligence in Aviation. **Related Standard:** SAE G34 / EUROCAE WG-114. **Working Group Active Party/Parties:** SAE G34 / EUROCAE WG-114 : Collins (UTRC) - through Collins US and Collins Italy. **Person involved:** Darren Cofer, Giacome Gentile. **Summary of activity:** Contribution to EUROCAE White paper for Assured AI. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact. **Topics discussed that may be relevant to VALU3S activities:** Employ formal methods for NN assurance - Methods and approaches.
Since 2022	**Type of activity:** working group meeting. **Title:** Standard Practice For Methods To Safely Bound Flight Behaviour Of Unmanned Aircraft Systems Containing Complex Functions. **Related Standard:** ASTM F3269-17. **Working Group Active Party/Parties:** ASTM F3269-17 Collins (UTRC) - through Collins US. **Person involved:** Daren Coffer. **Summary of activity:** Contribution to NASA-cross discipline standard for UAS. **Suggested follow-up activities:** Monitor standard development for potential impact on and benefit from VALU3S.
2022	**Type of activity:** working group meeting. **Title:** Creation of the national technical committee on biometrics. **Related Standard:** IPQ/CT 226. **Working Group:** Biometrics. **Active Party/Parties:** Biometria / CardioID. **Person involved:** Andr, Louren. **Summary of activity:** Participate in regular meetings. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact. **Topics discussed that may be relevant to VALU3S activities:** Revision and definition requirements quality criteria. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Assurance and certification.
2023	**Type of activity:** working group meeting. **Title:** Joined SC 37 Biometrics ISO/IEC CD 19795-10. **Related Standard:** ISO/IEC JTC 1/SC 37. **Working Group:** Biometrics. **Active Party/Parties:** Biometria / CardioID. **Person involved:** Andr, Louren. **Summary of activity:** Review and comment draft. **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact. **Topics discussed that may be relevant to VALU3S activities:** Revision and definition requirements quality criteria. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Assurance and certification.

Date	Description of activity
2023	**Type of activity:** working group meeting. **Title:** Joined SC 37 Biometrics ISO/IEC CD 29794-4. **Related Standard:** ISO/IEC JTC 1/SC 37 **Working Group:** Biometrics**.** **Active Party/Parties:** Biometria / CardioID. **Person involved:** Andr, Louren. **Summary of activity:** Review and comment draft**.** **Suggested follow-up activities:** Monitor standard development for potential VALU3S impact. **Topics discussed that may be relevant to VALU3S activities:** Revision and definition requirements quality criteria. **Activities of VALU3S relevant to the topics discussed in the standardization group:** Assurance and certification.
since 2021	**Type of activity:** working group meeting. **Title:** Fail-Safe Design of Autonomous and Semi-Autonomous Systems. **Related Standard:** ISO/IEC JTC 1/SC 37 **Working Group:** IEEE P7009**.** **Active Party/Parties:** IEEE P7009 Fail-Safe Design of Autonomous and Semi-Autonomous Systems NUIM. **Person involved:** Marie Farrell, Matt Luckcuck. **Summary of activity:** Participate in regular meetings and directly contribute to the draft standard which will go to ballot (expected in 2023).

Chapter 5 Conclusions

The purpose of this deliverable has been to finalize the work documented in deliverables D6.5 [2], D6.9 [3], D6.10 [4] and D6.17 [5]. This deliverable is presented at the end of the project. The main focus has been to describe the actions carried out during the project and how we believe they have helped us in achieving VALU3S objectives and KPIs, in order to influence the standardization organizations. The results obtained by implementing the final plan given in D6.17 are reported in this deliverable.

The works presented in this deliverable are in line with the objectives set up at the beginning of the project. Objective 7 states "To revisit and identify the weaknesses of relevant safety and security standards and develop a concrete strategy to influence the development of new standards. To influence the development of different standards targeting SCP of systems within the domains of the project through an active participation in related standardisation groups. This is complemented by identification of gaps in different Standards with regards to V&V methodology to conduct safety, cybersecurity, and privacy- related V&V of automated systems."

The final plan presented in D6.17 made possible the achievement of KPI10 "VALU3S aims to conduct a comprehensive gap analysis on SCP V&V methods, tools and concepts detailing strengths and weaknesses of the existing standards through active participation in at least 14 standardisation initiatives which are also used as platforms to disseminate the results of VALU3S."

The plan has been structured in five steps:

1. Carry out a close surveyance of standardization activities by the "Communication team" in monthly communication meetings dealing with this and other important WP6 issues.
2. Set up an Excel file for partners for monitoring the participation of partners in Standards Development Organizations (SDOs).
3. Make a series of training sessions on relevant standards on the different domains.
4. Description of standardization landscape for each domain.
5. Collection of surveys on standards related issues.

References

[1] VALU3S consortium, «VALU3S Grant Agreement,» 2021.

[2] AIT et al., «Deliverable D6.5 - Initial report on the results of the standardization survey (methods, tools, concepts suggested by the standards),» VALU3S Consortium, 2021.

[3] RGB et al., "Deliverable D6.9 - Initial plan on dissemination of VALU3S results to different Standardization groups," VALU3S Consortium, 2021.

[4] AIT et al., «Deliverable D6.10 - Final report on the results of the standardization survey (methods, tools, concepts suggested by the standards),» VALU3S Consortium, 2021.

[5] VALU3S Consortium, «Deliverable 6.17 - Final plan on dissemination of VALU3S results to different Standardisation groups,» April 29, 2022.

[6] SAE International, «SAE J3061. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,» 2021-12.

[7] International Organization for Standardization (ISO), «ISO 26262-10. Road vehicles — Functional safety — Part 10: Guidelines on ISO 26262,» 2018.

[8] International Organization for Standardization (ISO) and SAE International, «ISO/SAE 21434. Road vehicles — Cybersecurity engineering,» 2021.

[9] COIMBRA et al., «VALU3S web-based repository,» VALU3S Consortium, 11 2022. [En línea]. Available: https://repo.valu3s.eu/. [Último acceso: 25 04 2023].

[10] International Organization for Standardization (ISO), «ISO/PAS 21448. Road vehicles — Safety of the intended functionality,» 2019.

[11] International Electrotechnical Commission (IEC), «IEC TR 61508-0. Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 0: Functional safety and IEC 61508,» 2005.

[12] International Society of Automation (ISA), «Quick Start Guide: An Overview of ISA/IEC 62443 Standards,» 2020.

[13] CENELEC - European Committee for Electrotechnical Standardization, «CLC/TS 50701. Railway applications - Cybersecurity,» 2021-07-09.

[14] International Organization for Standardization (ISO), «ISO 10218-1. Robots and robotic devices — Safety requirements for industrial robots — Part 1: Robots,» 2011.

[15] International Organization for Standardization (ISO), «ISO 10218-2. Robots and robotic devices — Safety requirements for industrial robots — Part 2: Robot systems and integration,» 2011.

[16] International Organization for Standardization (ISO), «ISO 14971. Medical devices — Application of risk management to medical devices,» 2019.

[17] Underwriters Laboratories (UL), «ANSI/UL 4600. Standard for Safety for the Evaluation of Autonomous Products,» 2022.

[18] Radio Technical Commission for Aeronautics (RTCA), «DO-178C, Software Considerations in Airborne Systems and Equipment Certification,» 2011.

[19] International Organization for Standardization (ISO), «ISO/IEC JTC 1/SC 42. Artificial intelligence».

[20] International Organization for Standardization (ISO), «ISO/AWI PAS 8800. Road Vehicles — Safety and artificial intelligence».

[21] International Organization for Standardization (ISO), «ISO 24089. Road vehicles — Software update engineering,» 2023.

[22] International Organization for Standardization (ISO), «ISO/PAS 5112. Road vehicles — Guidelines for auditing cybersecurity engineering,» 2022.

[23] International Organization for Standardization (ISO), «ISO/AWI TS 5083. Road vehicles — Safety for automated driving systems — Design, verification and validation».

[24] International Organization for Standardization (ISO), «ISO/TC 22/SC 31. Data communication».

[25] International Organization for Standardization (ISO), «ISO 20078-1. Road vehicles — Extended vehicle (ExVe) web services — Part 1: Content,» 2019.

[26] International Organization for Standardization (ISO), «ISO 23132. Road vehicles — Extended Vehicle (ExVe) time critical applications — General requirements, definitions and classification methodology of time-constrained situations related to Road and ExVe Safety (RExVeS),» 2020.

[27] International Organization for Standardization (ISO), «ISO/DTR 4609. Road vehicles — Report on standardization prospective for automated vehicles (RoSPAV)».

[28] United Nations, «UN Regulation No. 155 - Cyber security and cyber security management system,» 2021-03-04.

[29] International Organization for Standardization (ISO), «ISO/IEC AWI 5888. nformation security, cybersecurity and privacy protection — Security requirements and evaluation activities for connected vehicle devices».

[30] International Organization for Standardization (ISO), «ISO/IEC Standard 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security,» 2005.

[31] International Organization for Standardization (ISO), «ISO/SAE AWI PAS 8475. Road vehicles — Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF),» Under development.

[32] Regulation of the European Parliament and of the Council, «Regulation (EU) 2017/745. Medical Devices Regulation,» 2017.

[33] Regulation of the European Parlament and of the Council, «Regulation (EU) 2023/607 amending Regulations (EU) 2017/745 and (EU) 2017/746 as regards the transitional provisions for,» 2023..

[34] Regulation of the European Parliament and of the Council, «Regulation (EU) 2017/746. In Vitro Diagnostic Medical Devices,» 2017.

[35] Council of the European Union, «EPSCO meeting. Employment, Social Policy, Health and Consumer Affairs Council,» [En línea]. Available: https://video.consilium.europa.eu/event/en/26650.

[36] Medical Device Coordination Group EU, «MDCG 2019-16. Guidance on Cybersecurity for medical devices,» 2019.

[37] International Electrotechnical Commission (IEC), «IEC 60601-1. Medical electrical equipment - Part 1: General requirements for basic safety and essential performance,» 2005.

[38] International Electrotechnical Commission (IEC), «IEC 62304. Medical device software – Software life cycle processes,» 2006.

[39] International Electrotechnical Commission (IEC), «IEC 62366-1. Medical devices - Part 1: Application of usability engineering to medical devices,» 2015.

[40] Regulation of the European Parliament and of the Council, «Regulation (EU) 2016/679. General Data Protection Regulation (GDPR),» 2016.

[41] European Commission, «The EU Cybersecurity Act,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act.

[42] International Organization for Standardization (ISO), «ISO 27799. Health informatics — Information security management in health using ISO/IEC 2700,» 2016-07.

[43] Regulation of the European Parliament and of the Council, «Directive (EU) 2022/2555 (NIS2). Measures for a high common level of cybersecurity across the Union,» 2022.

[44] European Comission, «The Cybersecurity Act strengthens Europe's cybersecurity,» [En línea]. Available: https://digital-strategy.ec.europa.eu/en/news/cybersecurity-act-strengthens-europes-cybersecurity.

[45] European Comission, «Questions and Answers - EU Cybersecurity,» [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369.

[46] Food and Drug Administration (FDA), «Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions,» 2022.

[47] International Medical Device Regulators Forum (IMDRF), «IMDRF/CYBER WG/N60. Principles and Practices for Medical Device Cybersecurity,» 2020.

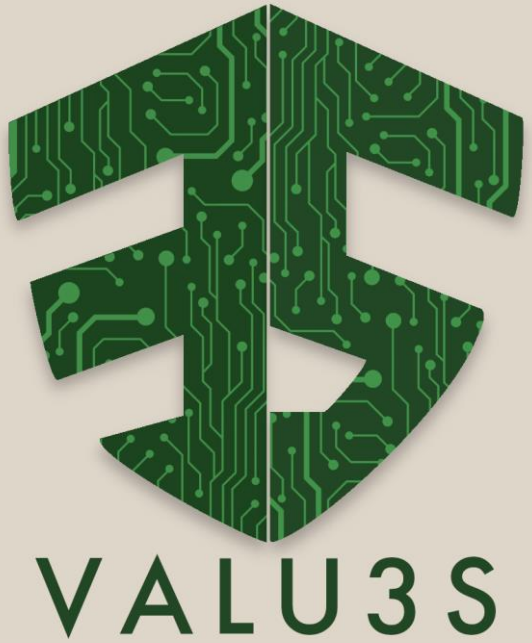
[48] International Organization for Standardization (ISO), «ISO 13482. Robots and robotic devices — Safety requirements for personal care robots,» 2014-02.

[49] International Electrotechnical Commission (IEC), «IEC 61496. Series of standards for Electro-sensitive protective equipment».

[50] International Electrotechnical Commission (IEC), «IEC TS 62998. Series of standards for Safety-related sensors used for the protection of persons,» 2019-05-02.

[51] International Organization for Standardization (ISO), «ISO 12100. Safety of machinery — General principles for design — Risk assessment and risk reduction,» 2010.

[52] International Organization for Standardization (ISO), «ISO 25119. Tractors and machinery for agriculture and forestry — Safety-related parts of control systems,» 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.