ECSEL Research and Innovation actions (RIA)

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

Standardization Survey D8.9

Work Package:	WP8 Exploitation, Dissemination and Standardization
Dissemination level:	PU = Public
Status:	Final
Date:	31 March 2017
Responsible partner:	E. Schoitsch, C. Schmittner [AIT]
Contact information:	Erwin.schoitsch@ait.ac.at, Christoph.schmittner@ait.ac.at
Document reference:	AMASS_D8.9_WP8_AIT_V1.0

This deliverable is part of a project that has received funding from the ECSEL JU under grant agreement No 692474. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and from Spain, Czech Republic, Germany, Sweden, Italy, United Kingdom and France.

Contributors

Names	Organization
Erwin Schoitsch, Christoph Schmittner, Petr Böhm, Thomas Gruber, Ma Zhendong	AIT Austrian Institute of Technology GmbH
Jose Luis de la Vara, Jose María Álvarez, Eugenio Parra, Juan Llorens	Universidad Carlos III de Madrid
Luis M. Alonso, Jose M. Fuentes, Borja López	The REUSE Company
Javier Herrero Martín, Elena Alaña Salazar	GMV Aerospace and Defence, S.A.U.
Helmut Martin, Bernard Winkler	Virtual Vehicle (VIF)
Fredrik Warg	RISE Research Institutes of Sweden (SPS)

Reviewers

Names	Organization
Frank Badstuebner (Peer-reviewer)	Infineon
Tomáš Kratochvíla (Peer-reviewer)	Honeywell
Cristina Martínez (Quality Manager)	Tecnalia Research & Innovation
Barbara Gallina, TC-Member review	Maelardalen Hoegskola
Jose Luis de la Vara	Universidad Carlos III de Madrid

TABLE OF CONTENTS

List of Figures

List of Tables

Executive Summary

D8.9 is the first standardization-related deliverable of WP8 (Exploitation, Dissemination and Standardization). With a focus on multi-concern assurance, seamless interoperability, cross and intra domain reuse and compliance, Standardization is an important part of the AMASS work and it is envisioned that AMASS results and approaches will be introduced by AMASS partners into standardization. Although standardization supports the dissemination of project results and the industrial adoption, standardization processes usually take longer than the duration of a research process and results need a certain maturity to be considered for integration in standardization. Therefore, we intend to plan and coordinate the standardization impact, with the expectation that standardization impact will mainly take place after the project and depend on the ongoing involvement of AMASS partner independent of the AMASS project lifecycle.

As a starting point to plan further standardization activities, D8.9 documents the results of a standardization survey in the AMASS consortium. The goal was to get an overview of standards and covered quality attributes which are relevant for the AMASS partners and use cases. Additionally this shows an overview of the State of Standardization in respect to multi-concern assurance, seamless interoperability, cross and intra domain reuse. In addition involvement of AMASS partners in standard developments and committees is documented.

1. Introduction

With a focus on multi-concern assurance, seamless interoperability, and compliance, standardization is an important part of the AMASS work and it is envisioned that AMASS results and approaches will influence standardization. There are two aspects in which AMASS will use, contribute and interact with standards and ongoing standardization activities.

One the one side, safety and security standards (domain independent or domain specific) are of importance to AMASS. All use cases are from domains with strong safety and security requirements, partially codified in standards. In most industrial domains safety standardization is more advanced than security, and the definition of industrial accepted approaches as relevant for security standards is an important contribution in AMASS. Additionally, since safety & security co-assurance and multi-concern assurance in general is still an open issue, AMASS will consider how safety and security interact with each other and with additional system quality attributes to reach a more efficient system engineering methodology and increase the overall dependability of the systems.

The second aspect is interoperability through the complete system lifecycle. The AMASS Reference Tool Architecture is envisioned to build the foundation for the first European-wide open certification/qualification platform, ecosystem and community. While the foundation for such an endeavour can be built in the project, the main challenge is the industrial and scientific acceptance and adoption. AMASS has two work packages, WP7 Industrial impact and community building and WP8 Exploitation and dissemination, which work on different aspects of building an AMASS community and AMASS legacy that will extend beyond the duration of the project. One contributor to the lasting impact is the usage of open standards and seamless interoperability between the different iteration of the AMASS Platform and external tools. This is only possible by using internationally accepted and interoperability standards. AMASS is therefore also cooperating with other ongoing European initiatives, e.g. for tool interoperability standardization like CP-SETIS, a Horizon 2020 Innovation Action of support-action type.

This document starts with an overview of the results of the standardization survey (Section 2), the complete survey is contained in Appendix A Standardization Survey. Section 3 gives an overview of ongoing standard developments in terms of seamless interoperability, cross and intra domain reuse and multi-concern assurance and Section 4 describes domain specific multi-concern standards. Section 5 lists the Involvement of AMASS partner in standardization activities. Finally Section 6 summarizes the current status and gives an outlook of the next steps.

2. Results of standardization survey

In AMASS a survey of standards and quality attributes was elaborated. The goal was to identify which domains are relevant for the AMASS partners, e.g. are there any gaps or weaknesses which may reduce the impact and restrict it to certain domain and identify all quality attributes which are relevant for multi-concern. Multi-concern is only partially defined as relating to the Dependability definition by Avizienis, Laprie, Randell and Landwehr [1]. In the survey the goal was to get a more fine-granular overview of the relevant quality attributes and determine which are relevant to AMASS. The respective table with the complete results is placed in the Appendix A of this document. Future surveys will also include relevant interoperability standards which are of interest or in use by AMASS partner.

We present here two analysis of the survey results. The first focuses on standards per domains and gives an overview about the number of relevant standards for domains for the AMASS partner. This is presented in Section 2.1. In the next Section 2.2 we present the quality attributes which are relevant for AMASS partners and correlate it with relevant domains, to give an overview which attributes are relevant for which domain.

It should be noted that AMASS is working on almost all domains which are summarized in the ECSEL Multiannual Strategic Plan but with differing intensity. Depending on the involved industrial partners there are, as example, multiple use cases related to smart mobility, but only one use case related to smart energy. Nevertheless, AMASS will address all domains addressed in the ECSEL Multiannual Strategic Plan and consider specific challenges and requirements when developing the solutions.

2.1 Relevant Domains for AMASS partners

For the list of domains, we collected not only the information about which domains are relevant but also the number and names of standards related and relevant for each specific domain. Figure 1. Overview of domains and related standards, therefore gives an overview of all domains that are relevant for AMASS partners and the identification of the standard. Since we counted standard per existing standard which should be considered in AMASS, this number can be distorted by the organization of the respective standard. As example, in the automotive domain the relevant safety standard is ISO 26262, which contains 10 parts. Avionics standards have fewer parts, but more stand-alone standards. This increases the number for avionics and decreases the number for automotive.

This explains why in Figure 1 Avionics and Space are the most prominent domains. IEC 62443 or IEC 60601 in the health domain have up to two subpart numbers (e.g. IEC 62443-2-4 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers; IEC 80601-2-77 MEDICAL ELECTRICAL EQUIPMENT – Part 2-77: Particular requirements for the basic safety and essential performance of robotically assisted surgical equipment).

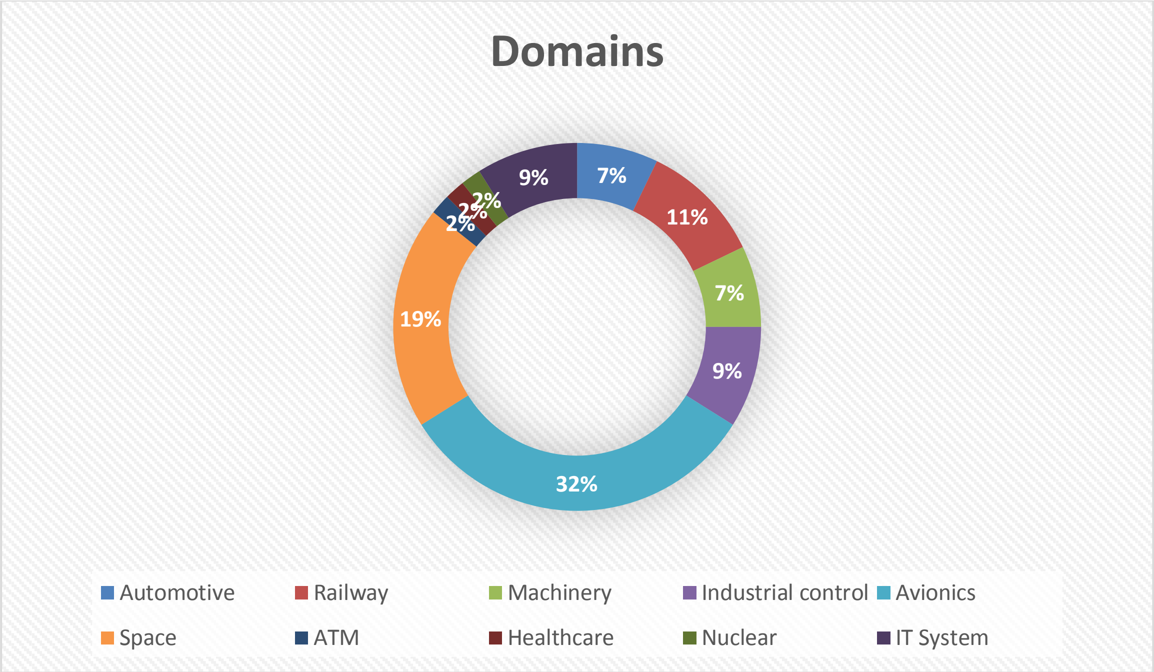

Figure 1. Overview of domains and related standards

2.2 Relevant Quality Attributes

The second overview listed the relevant quality attributes and the number of standards that consider the attributes. Figure 2. Overview of quality attributes, considered in standards gives an overview from all relevant standards which quality attributes are already considered. This list is not yet a complete picture of quality attributes relevant for AMASS; it is the result of a survey that collected the state of the art in the standards. E.g., Safety and Security is considered in the majority of standards, Availability is currently only considered in four standards.

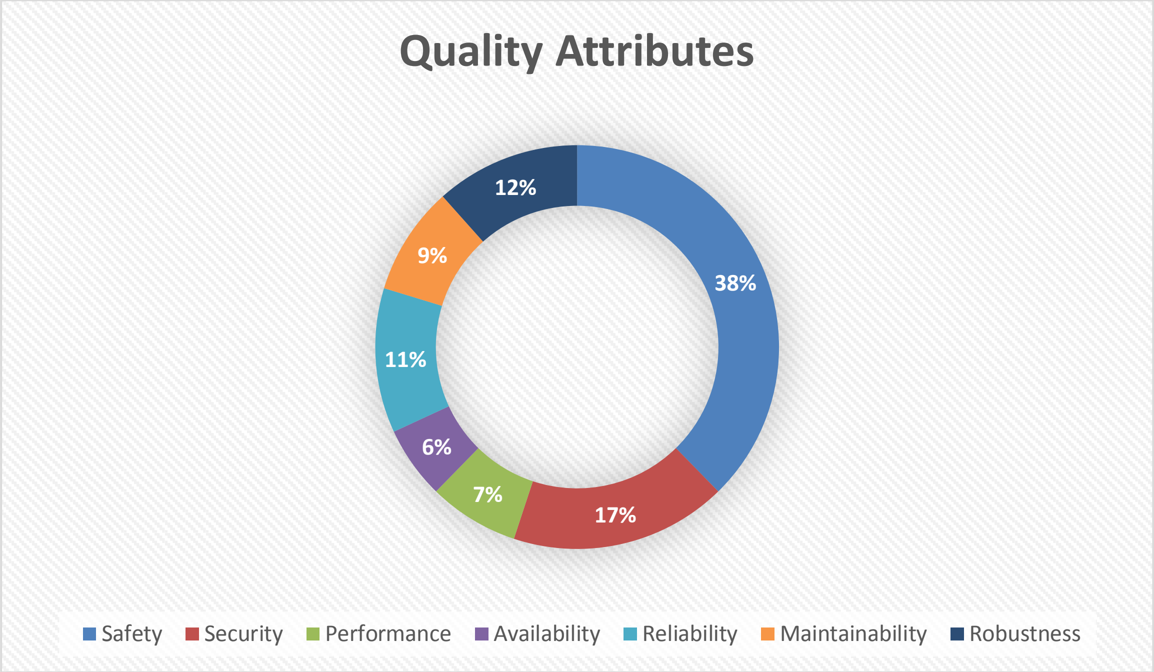

Figure 2. Overview of quality attributes, considered in standards

This is used as a starting point for our work on standards in AMASS, e.g. when we identify a missing concern which is not yet treated by a standard we can identify the gap by using the results of this first survey.

We ordered the overview from Figure 2 also per domains to get an overview which domains already consider multiple concerns. Figure 3. Overview of quality attributes, considered in standards per domain gives this overview. There are a few cross-domain standards which treat multiple concerns and are applicable to all domains, which causes one standard for almost all concerns for a domain.

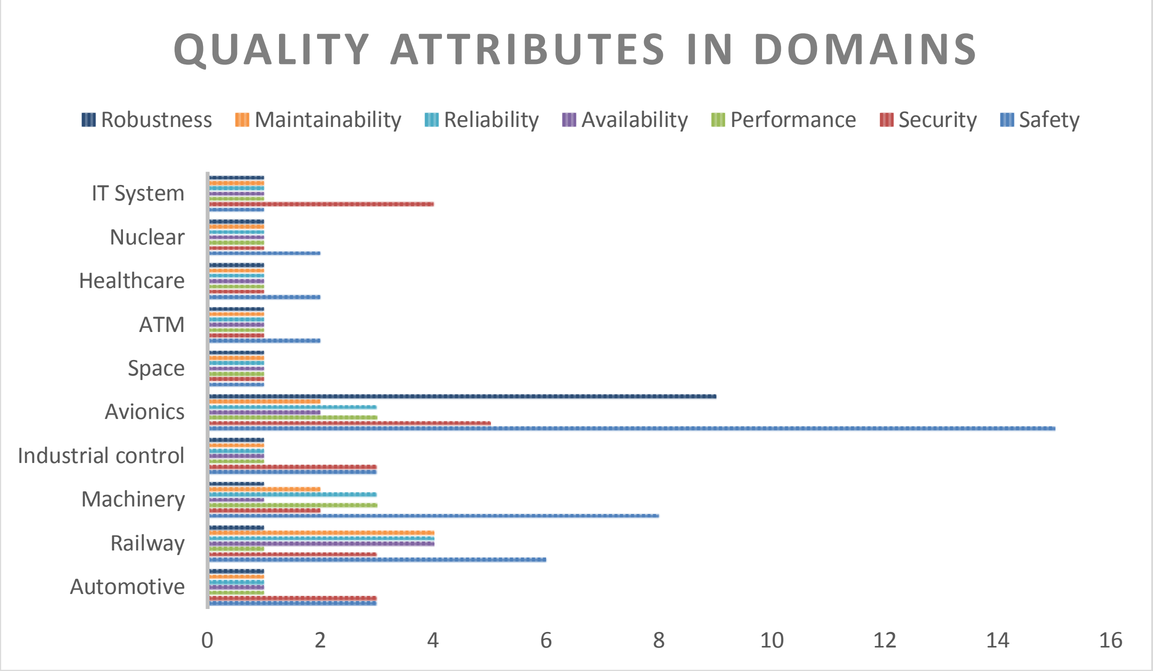

Figure 3. Overview of quality attributes, considered in standards per domain

3. Evolving Standard Landscape and Influence of AMASS

As planned in the proposal and Technical Annex, AMASS is co-operating intensively with the ARTEMIS-IA Standardization WG and the H2020 Project CP-SETIS. A considerable update of the ARTEMIS-IA Strategic Agenda for Standardization is now in progress in CP-SETIS. AMASS partners are already active to introduce first results in safety and security standards for multiple domains.

3.1 AMASS relevant developments in the Object Management Group

OMG (Object Management Group) is an international, open membership, not-for-profit organization that develops technology standards. OMG standards are driven by vendors, end-users, academic institutions, and government agencies. OMG Task Forces develop enterprise integration standards for a wide range of technologies. OMG's modelling standards, such as UML and SysML, enable powerful visual design, execution, and maintenance of software and other processes.

Several standards and initiatives at OMG are related to and can be the target of AMASS standardization activities. Among them, SysA (System Assurance Task Force) aims to:

- Adapt and extend OMG technologies that apply across domains to enhance system assurance (e.g. reliability, safety, security, and compliance);
- Establish a common framework for analysis and exchange of information related to system assurance and trustworthiness, and;
- Promote system, software and information assurance in OMG product interoperability mechanisms.

The work in SysA includes the development and maintenance of SACM (Structured Assurance Case Metamodel). This standard is arguably one of the closest ones to the CACM. SACM includes an argumentation metamodel and an artefact (evidence) metamodel, and also deals with other aspects such as the terminology used in an assurance and the support to the specification of argument modules and patterns.

The current version of SACM (2.0, beta) is a major version release over previous versions. Among other objectives, it has aimed at:

- Improving the understandability of an assurance case to a 3rd Party
- Improving rigor of assurance case modelling
- Allowing for re-examination of assumptions, argument structuring, and evidence appropriateness
- Better supporting the reuse of argument and evidence constructs
- Providing for more suitable exchange of assurance cases

This version is further based on many results from and insights gained in the OPENCOSS project [2], which is one of the main base EU projects for AMASS.

There is currently a close interaction between AMASS and the team developing SACM. Jose Luis de la Vara (UC3) is part of this teams and provides input for SACM revision based on the work performed in AMASS.

3.2 Inclusion of the CP-SETIS Findings concerning IOS (Tool Interoperability Specifications) Framework

The CP-SETIS project aims at two targets (besides the goal to update the ARTEMIS-IA Strategic Agenda for Standardization in general, covering all CPS areas):

- Coherent setting of standards and specifications for Tool Interoperability, covering the full set of requirements identified, sustainable maintenance process and evolution process, resulting in a "Multi-Standard Concept" to meet different tool interface concerns.
- Finding a way to identify and implement a hosting and maintenance structure (ICF–Interoperability Coordination Forum) so that the work done in several ARTEMIS projects like IFEST [3], MBAT [4], SafeCer [5], ARROWHEAD [6], EMC^2 [7] and particularly CRYSTAL is harmonized and maintained in a sustainable manner.

The Multi-standard approach is depicted in the following manner:

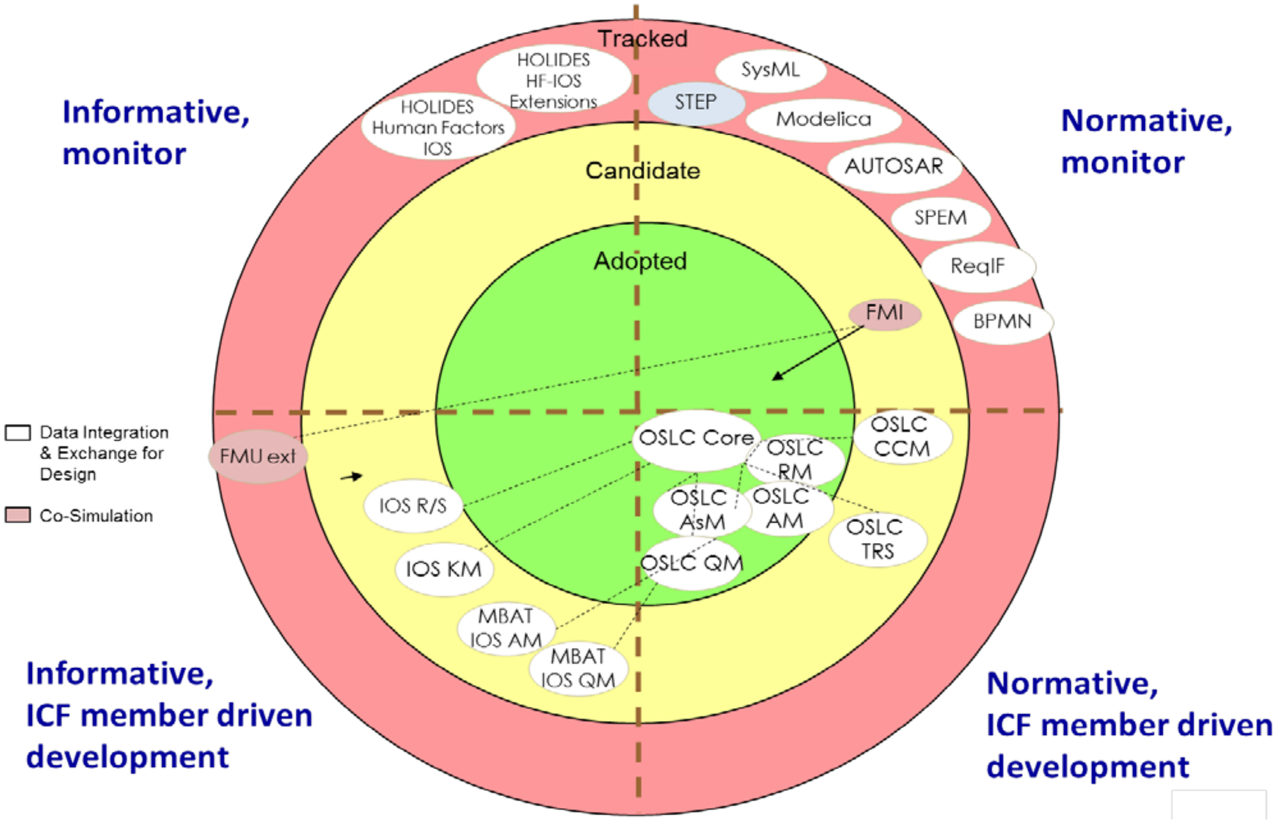

Figure 4. Visualization of the IOS example database, showing some standards on different levels of integration (maturity, adoption)

The IOS consists of different types of parts, which are similar to those arising in multi-concern standardization issues:

a) IOS parts that are based on an existing standard, do not necessarily include all specifications of this particular standard, but only those parts that are relevant for the respective Engineering Concern.

b) IOS also includes specifications that are not yet part of an existing standard. These are either extensions of existing standards (if the standard does not yet completely cover the Engineering Concern), or as an independent specification (if there is no existing standard yet covering this particular Engineering Concern).

c) IOS also includes so called Bridges, which describe the relations between the different Engineering Concerns and the corresponding interoperability specifications and standards. These bridges are essential to make IOS indeed cover the whole development process, yet they are specifications that by definition do not belong to a single (extension of an) existing standard.

For a Multi-Standard like IOS, two different selection – or 'standardization' – processes have to be accomplished:

1. Selection of new specifications **for inclusion and adoption into the Multi-Standard**. In the case of IOS, these specifications are new IOS parts, i.e. specifications covering a specific Engineering Concern, which are (a) based on existing standards including extensions of these, or (b) not based on an existing standard (usually because there is no existing standard for this particular Engineering Concern), or (c) bridges between other parts of the IOS (c.f. 3.1.).
2. **Formal Standardization** of parts of the Multi-Standard. In the case of IOS, this includes (a) for those parts of the IOS that are based on existing standards, inclusion of the IOS specific extensions into these standards, (b) for those parts, which are not based on an existing standard yet, the creation and development of an appropriate formal standard and (c) for bridges the same as for (b).

At any time, each part of the Multi-Standard is in one of four states with regard to its maturity level (or adoption status):

- **Proposed**. A specification that has been proposed by a (group of) stakeholder(s) to become part of the Multi-Standard.
- **Tracked**. A specification that has been deemed appropriate for inclusion into the Multi-Standard. The development, evaluation and application of this specification is tracked by the organization handling the multi-standard.
- **Candidate**. A specification that has successfully been applied to and evaluated with appropriate use-cases.
- **Adopted**. A specification that is adopted as a part of the Multi-Standard.

The stakeholders group (ICF, as mentioned above) guides this process.

In principle, each part of a Multi-Standard can be standardized – i.e., become a formal standard managed by a standardization body – independently of any other part. For each part, this standardization would basically follow the same process as for a single standard, that is, stakeholders would decide which parts to formally standardize, would select an appropriate standardization body and work towards setting up a corresponding formal standard within this standardization body. Here, we will only describe the characteristic differences between formal standardization of a single-standard vs. that of a part of a Multi-Standard.

For a Multi-Standard, note that stakeholders may decide for some parts not to formally standardize specific parts at all. Especially for bridges, but also for small or 'less important' specifications, it might be sufficient to be an adopted part of the Multi-Standard and a formal standard might either not be required, not worth the effort, or even infeasible.

For Multi-Standards like the IOS, where some parts already build upon existing standards and extend them, there is obviously no need to decide whether this part should become a formal standard or which standardization body to choose. Here, the process would comprise activities to modify/update the existing standard within the standardization body to include the new extensions.

The multi-standard approach can be a model for the multi-concern standardization issues to be managed for many domains and standardization areas/bodies in a coherent manner, in cooperation of AMASS with other related projects and initiatives – we may have just a look on the landscape of functional safety and security standards in IEC, ISO, Aerospace and other areas (see Figure 5).

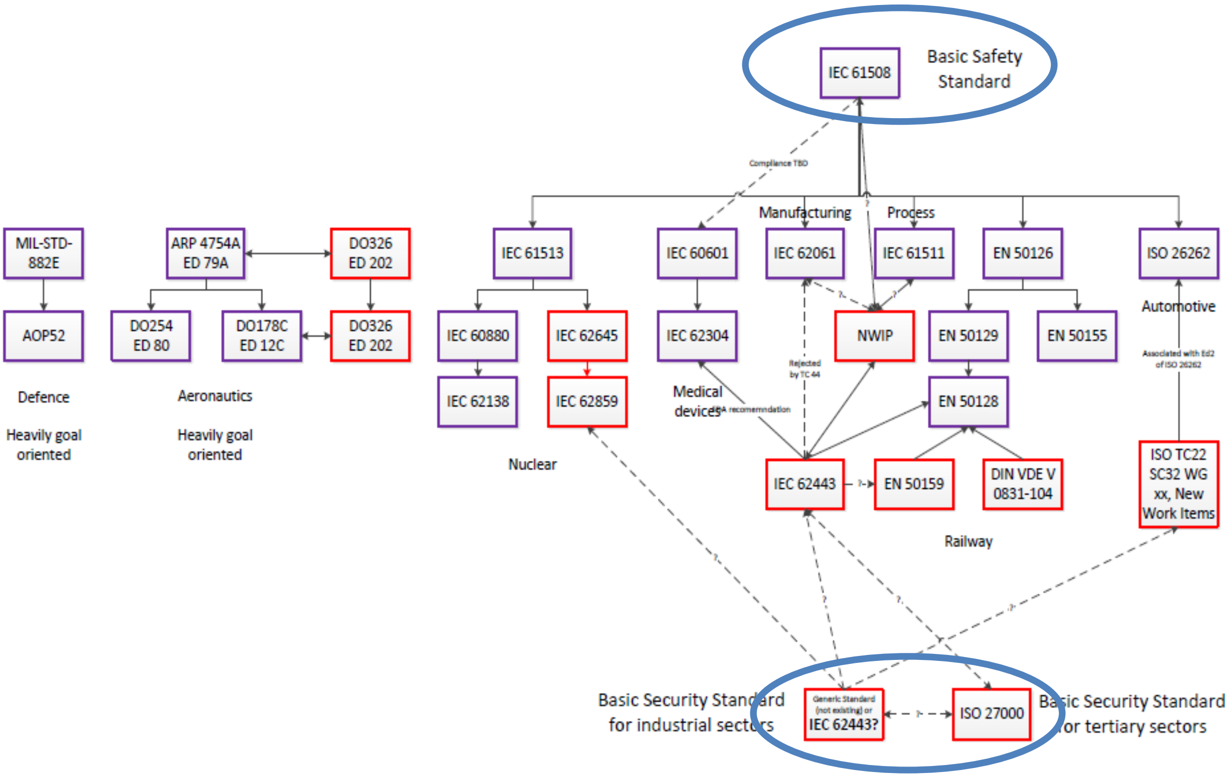

Figure 5. A view of the International Standardization Framework of Safety & Security (Bertrand Rique, 2015)

3.3 Tool integration via OSLC

In the context of software and system interoperability and integration, the Open Services for Lifecycle Collaboration (OSLC) initiative [8] is a joint effort between academia and industry to boost data sharing and interoperability among applications by applying the Linked Data principles [9]: "*1) Use URIs as names for things. 2) Use HTTP URIs so that people can look up those names. 3) When someone looks up a URI, provide useful information, using the standards (RDF*, SPARQL) and 4) Include links to other URIs, so that they can discover more things*". Led by the OASIS OSLC working group[1], OSLC is based on a set of specifications that take advantage of web-based standards such as the Resource Description Framework (RDF) [10] and the Hypertext Transfer Protocol (HTTP) to share, integrate and exchange data under a common data model (RDF) and protocol (HTTP). Every OSLC specification defines a *shape* for a particular type of resource. For instance, requirements, changes, test cases, models (the OSLC-MBSE specification Model-Based Systems Engineering by the Object Management Group) or estimation and measurement metrics, to name a few, have already a defined shape (also called OSLC Resource Shape).

Thus, tools for supporting Application Life-cycle Management (ALM) or Product Life-cycle Management (PLM) have now an agreement on what data must be shared, and how. In terms of knowledge management as a driver for integration, the *Assets Management* and the *Tracked Resource Set* are the most convenient specifications for the purpose of managing artefacts. However, there are many artefacts generated during the development lifecycle, which may not fit to existing shapes or standard vocabularies. Simulation models, business rules or physical circuits are examples of potential artefacts whose OSLC resource shape is not yet defined. Furthermore, some common and useful services such as indexing, naming, retrieval, quality assessment, visualization or traceability must be provided by all tool vendors, creating a tangled environment of query languages, interfaces, formats and protocols.

Therefore, one of the current trends in software and systems development lies in boosting interoperability and collaboration through the sharing of existing artefacts under common data models, formats and

[1] http://www.oasis-oslc.org/

protocols. In this context, OSLC is becoming a collaborative software ecosystem [11] for software product lines [12] through the definition of data shapes that serve as a contract to get access to information resources through HTTP-based services.

In particular, the Representational State Transfer (REST) software architecture style is used to manage information resources that are publicly represented and exchanged in RDF. Obviously, OSLC represents a big step towards the integration and interoperability between the agents involved in the development lifecycle.

Taking into account that systems and software integration is continuously being explored and new technologies and techniques arise to tackle the problems of storage, representation and retrieval, it seems that semantic approaches can ease these tasks. In this light, the Semantic Web, coined by Tim Berners-Lee in 2001 [13], has experienced during last years a growing commitment from both academia and industrial areas with the objective of elevating the abstraction level of web information resources.

The Resource Description Framework (RDF), based on a graph model, and the Web Ontology Language (OWL), designed to formalize, model and share domain knowledge, are the two main ingredients to reuse information and data in a knowledge-based realm. Thus, data, information and knowledge can be easily represented, shared, exchanged and linked to other knowledge bases through the use of Uniform Resource Identifiers (URIs), more specifically HTTP-URIs. As a practical view of the Semantic Web, the Linked Data initiative [14] emerges to create a large and distributed database on the Web by reusing existing and standard protocols. In order to reach this major objective the publication of information and data under a common data model (RDF) with a specific formal query language (SPARQL) provides the required building blocks to turn the Web of Documents into a real database or Web of Data. In this context, a large body of work can be found in different domains such as Geography, Bibliography, e-Government, e-Tourism or e-Health, all of them having common needs, such as interoperability among tools, different schemes or data models, or cross-cutting services (index and search).

On the other hand, in recent times we have seen the deployment of service oriented computing [15] as a new environment to enable the integration of software in organizations. In general, a service oriented architecture comprises an infrastructure (e.g. Enterprise Service Bus) in which services (e.g. software as web services) are deployed under a certain set of policies. A composite application is then implemented by means of a coordinated collection of invocations (e.g. Business Process Execution Language). In this context, Enterprise Integration Patterns (EAI) [16] have played a key role to ease the collaboration among services. Furthermore, existing W3C recommendations such as the Web Services Description Language (WSDL) or the Simple Object Access Protocol (SOAP) have improved interoperability through a clear definition of the input/output interface of a service and communication protocol.

In order to improve the capabilities of this type of web services, semantics was applied to ease some tasks such as discovery, selection, composition, orchestration, grounding and automatic invocation of web services. The Web Services Modelling Ontology (WSMO) [17] represented the main effort to define and to implement semantic web services using formal ontologies. OWL-S (Semantic Markup for Web Services), SA-WSDL (Semantic Annotations for WSDL) or WSDL-S (Web Service Semantics) were other approaches to annotate web services, by merging ontologies and standardizing data models in the web services realm.

However, these semantics-based efforts did not reach the expected outcome of automatically enabling enterprise services collaboration. Formal ontologies were used to model data and logical restrictions that were validated by formal reasoning methods implemented in semantic web reasoners. Although this approach was theoretically very promising, since it included consistency checking or type inference, the reality proved that the supreme effort to create formal ontologies in different domains, to make them interoperable at a semantic level, and to provide functionalities such as data validation, was not efficient. More specifically, it was demonstrated [18] that, in most of cases, data validation, data lifting and data lowering processes were enough to provide an interoperable environment.

That is why the approach based on the W3C recommendations, WSDL+SOAP, fulfilled most of these requirements with a huge industrial and technological support. However, the lack of agreement on the schemas to be shared (any service provider offered their own schema) and the use of a restricted data model such as XML was still present with the result of preventing a paradigm shift.

Taking advantage of the Linked Data principles and Web standards and protocols, the OSLC effort emerges to create a family of web-based specifications for products, services and tools that support all the phases of the software lifecycle.

Similar to OSLC, Agosense Symphony[2] offers an integration platform for application and product lifecycle management, covering all stages and processes in a development lifecycle. It represents a service-based solution with a huge implantation in the industry due to the possibility of connecting existing tools. WSO2[3] is another middleware platform for service-oriented computing based on standards for business process modelling and management. However, it does not offer standard input/output interfaces based on lightweight data models and software architectures such as RDF and REST. Other industry platforms such as PTC Integrity[4], Siemens Team Center[5], IBM Jazz Platform[6] or HP PLM[7] are now offering OSLC interfaces for different types of artefacts.

In conclusion, it is clear that software and systems interoperability and integration is an active research area that evolves according to the current trends in development lifecycles. It may have the potential of leveraging new technologies such as the web environment, service-oriented computing, semantics and Linked Data. That is why current efforts are focused on providing integration via software as a service while interoperability is being reached through the agreement on flexible data schemes. Both data schemes and data are being shared using a Linked Data approach (REST services + RDF) with the aim of exchanging any piece of information in a standard environment.

However, data exchange does not necessarily imply integration. From service providers to data items, an integration strategy is required to really represent, store, search and coordinate collaboration between software artefacts metadata and contents. In this light, the OSLC initiative is currently following this approach, having impact on the main players of software and systems industry. Nevertheless, it only covers a restricted type of artefacts and some crosscutting and basic services for reuse, such as indexing or retrieval, must be provided by all third-parties.

[2] http://www.agosense.com/english/products/agosensesymphony/agosensesymphony

[3] http://wso2.com/

[4] http://www.ptc.com/application-lifecycle-management/integrity

[5] http://www.plm.automation.siemens.com/en_us/products/teamcenter/

[6] https://jazz.net/

[7] http://www8.hp.com/us/en/business-services/it-services.html?compURI=1830395

4. Overview on maintained standards, on new standardization areas, evolving technologies, and of new standardization groups tackling CPS and SoS (Systems of Systems)

4.1 Space Standards

4.1.1 ECSS standards

The European Cooperation for Space Standardization (ECSS) represents a cooperative effort of the European Space Agency (ESA), national space agencies and European industry associations for the development of a coherent, single set of consistent space standards for use by the entire European Space Community. The objective of creating this organization was to produce standards to be used throughout the European space business. Therefore, the European Space Agency (ESA) contractors have to adhere to the standards created by this organization.

The result of this effort is the ECSS series of Standards (ST), Handbooks (HB) and Technical Memoranda (TM) organized in four branches as depicted in Figure 6:

- M: Management Standards
- Q: Product Assurance Standards
- E: Engineering Standards
- U: Usability Standards

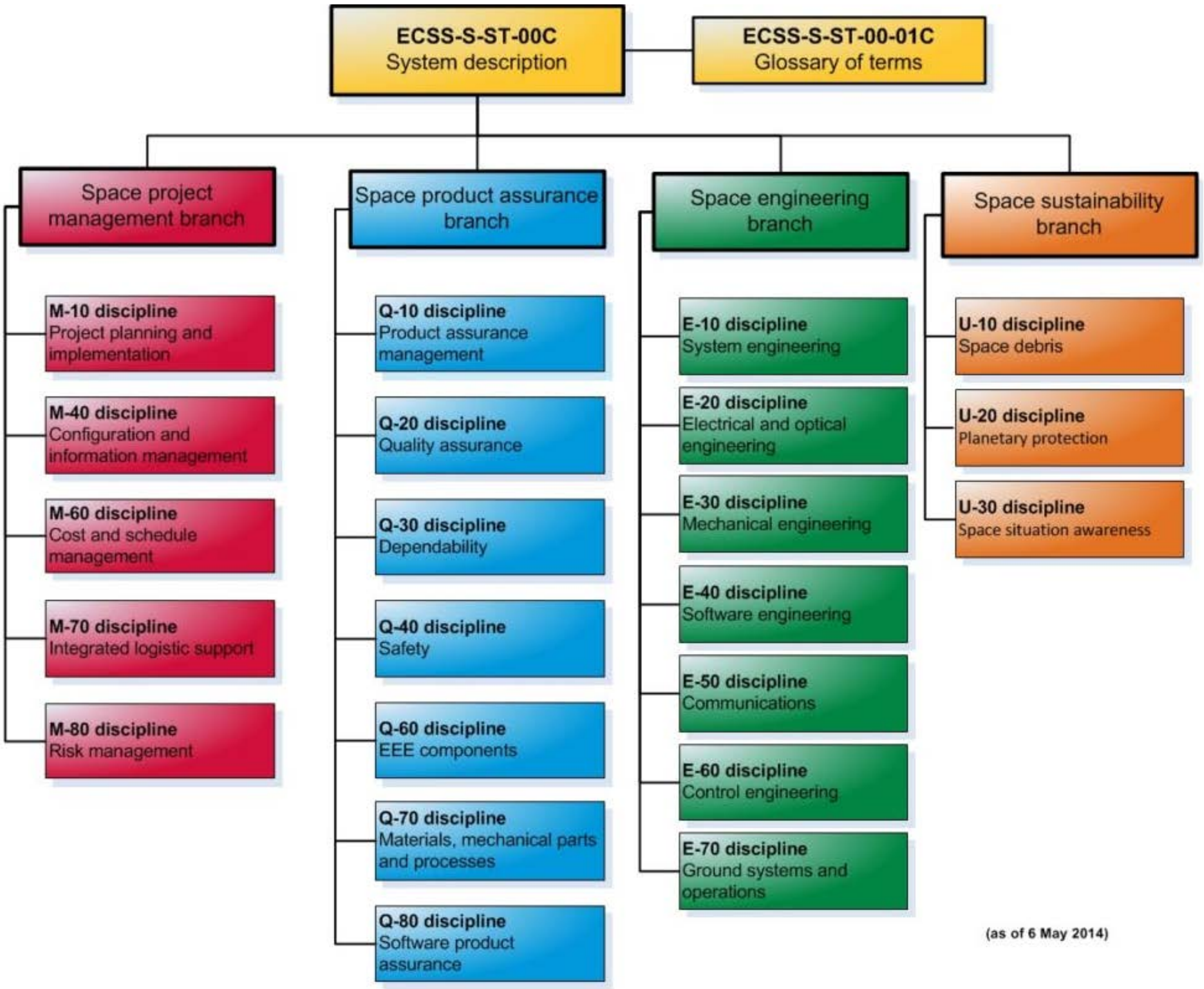

Figure 6. ECSS standards organization [19]

The most relevant standards for the AMASS project are detailed below.

4.1.1.1 ECSS-E-ST-40 Space engineering Software

The software developed for space systems has a high level of criticality since failures can cause loss of the entire mission. Unlike other kind of systems (avionics, automotive, etc.), the software in space systems has to work correctly once the space system is released from the launcher. In the space systems, the limitations of power and mass forces the use of processors with small processing power and limited memory. In addition, the proportion of missions implemented with software is increasing.

In this scenario, the ECSS-E-40 standard for space projects was created. It replaced the PSS-05 standard and tailors the ISO12207 standard. The ECSS-E-40 standard focuses on space software engineering processes requirements and their expected outputs, putting a special emphasis on the system-software relationship and on the verification and validation of software items.

In the space systems, software is found at all levels, ranging from system functions down to firmware, including safety and mission critical functions. The ECSS-E-40 standard reflects the specific methods used in space systems developments providing a coherent and complete framework for software engineering in a space project.

The standard shall be tailored for the specific characteristics and constraints of each project. [20] [21]

4.1.1.2 ECSS-Q-ST-80 SOFTWARE PRODUCT ASSURANCE

The ECSS-Q-ST-80 standard defines a set of software product assurance requirements to be used for the development and maintenance of software for space systems.

The objective of software product assurance is to provide adequate confidence to the customer and to the supplier that a software (developed or reused) satisfies its requirements throughout the system lifetime. In particular, that the software performs properly and safely in its operational environment and meeting the quality objectives agreed for the project.

The requirements defined in the ECSS-Q-ST-80 standard deal with quality management, process definition and quality characteristics of software products during the whole project life cycle.

This standard may be tailored for the specific characteristics and constrains of a space project [22] .

4.1.1.3 Dependability and Safety standards

The Q-30 and Q-40 branches are in charge of the dependability and safety issues of the space systems. Here are detailed some of the standards:

- ECSS-Q-ST-30 Space product assurance (dependability) defines the requirements for a dependability assurance programme in space projects. This standard calls for the use of dependability analysis techniques, tailored to match the generic requirements in each project, to address the hardware, software and human functions composing the system.
- ECSS-Q-ST-40 Space product assurance (safety) defines the safety programme and the technical safety requirements for space projects.

4.1.2 SAVOIR initiative

The European Space Agency recognized the need of improving the way space systems are being developed and delivered. This challenge can be met through a harmonization process based on the generation and application of standards across multiple operational projects. Namely, definition of reference architectures at both avionics and software levels with standard interfaces and definition of reference specifications, which could be adopted in future missions.

To this end, the ESA created SAVOIR (Space Avionics Open Interface Architecture) initiative [23], which responds to the need for improving competiveness of European industry by minimizing costs and risks whereas the efficiency and schedule are improved. This process is based on the definition of a reference and harmonized architecture.

SAVOIR represents an initiative between European Space Agencies (European Space Agency, the National Space Agencies of France and Germany) and Space Industry at prime and supplier level, working in cooperation with the following working groups:

- The European Cooperation for Space Standardization (ECSS) (see section 4.1.1).
- The Consultative Committee for Space Data Systems (CCSDS) [24]. CCSDS is a multinational forum for the development of communications and data systems standards for spaceflight. Several CCSDS standards are currently being assessed by SAVOIR, such as those related to the architecture and communication (e.g., SOIS services), protocols (e.g., File Delivery Protocol CFDP) or spacecraft monitoring and control (e.g., Mission Operations).

Several sub-groups have been created to focus on specific areas: General group for Avionics Architecture and specific subgroups for OBCs, Flight Software, MMUs, and IMA architecture.

The main outputs of this working group are:

- An avionics reference architecture.
- A functional reference architecture

- A set of hardware generic specification and interface

4.2 Automotive Standards

In the automotive domain three major standardization activities are currently ongoing (see Figure 7. Automotive domain standards):

- Functional Safety: The first version of ISO 26262 was published in 2011. While the standard was a huge success and adapted by the automotive industry, technological developments like the increased usage of assistant functions, increased connectivity and the rising importance of software required a revision and update of the standard. This process is almost finalized and ISO 26262 Ed. 2 is planned for publication in 2018.
- Safety of The Intended Functionality – SOTIF: For automated or autonomous vehicles safety is not only endangered by failures in the classical understanding, e.g. a hardware element is failing or a software has a design error, but also by misinterpretations of sensor signals or lacking combination of sensor data and processing. SOTIF is a newly developed standard (ISO PAS 21448 – Public Available Specification) which addresses such issues.
- Automotive Cybersecurity: Due to the increasing connectivity, V2X communication and the shift of functionality towards software and more complexity that increases the need for Over the Air Updates (OTA), cybersecurity is increasingly important for dependable automotive systems. Recently demonstrated hacker attacks on automotive control systems via maintenance or entertainment channels have shown the necessity as well. Therefore SAE, who created already SAE J3061 as Guideline for Automotive cybersecurity Engineering, and ISO have joined forces towards an Automotive Cybersecurity Standard (ISO/SAE JWG1, ISO TC22 SC32 WG 11, for ISO 21434).
- Besides these well-known standards in the safety & security community, ISO TC 31, Road vehicles – Extended vehicle methodology, has started work on ISO 20077-1 (General information) and 20077-2 (Methodology for designing the extended vehicle), keeping in mind particularly the connected vehicle aspects (V2V, V2I, or general V2X), which are now already in the DIS-stadium.

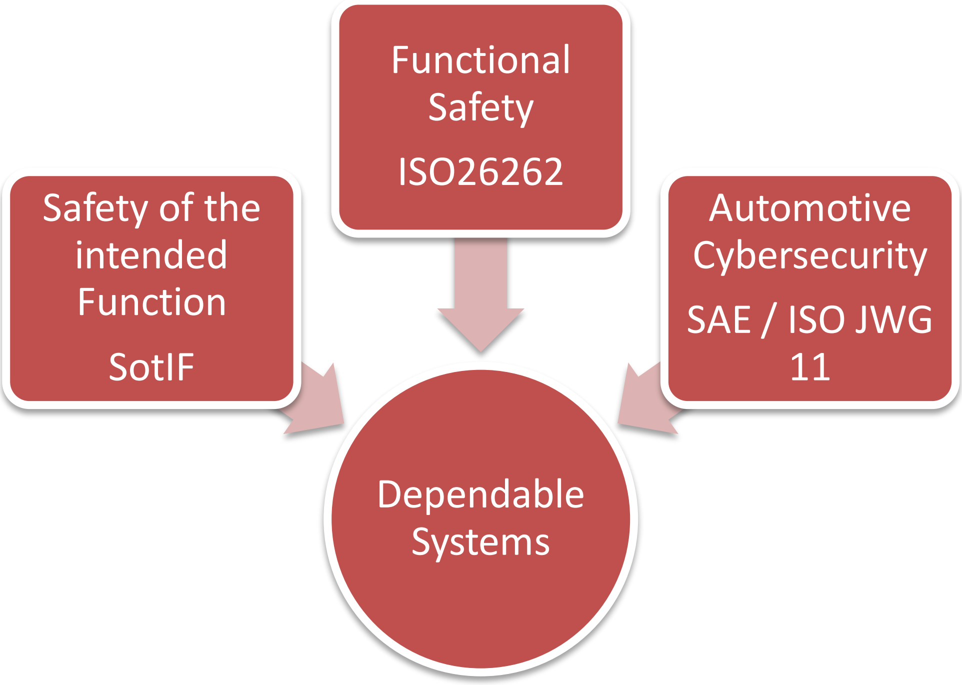

Figure 7. Automotive domain standards

4.2.1 Functional Safety according to ISO 26262

ISO 26262 which was published in 2011 and covers the overall engineering lifecycle of safety critical E/E systems, is divided in 10 parts (see Figure 8).

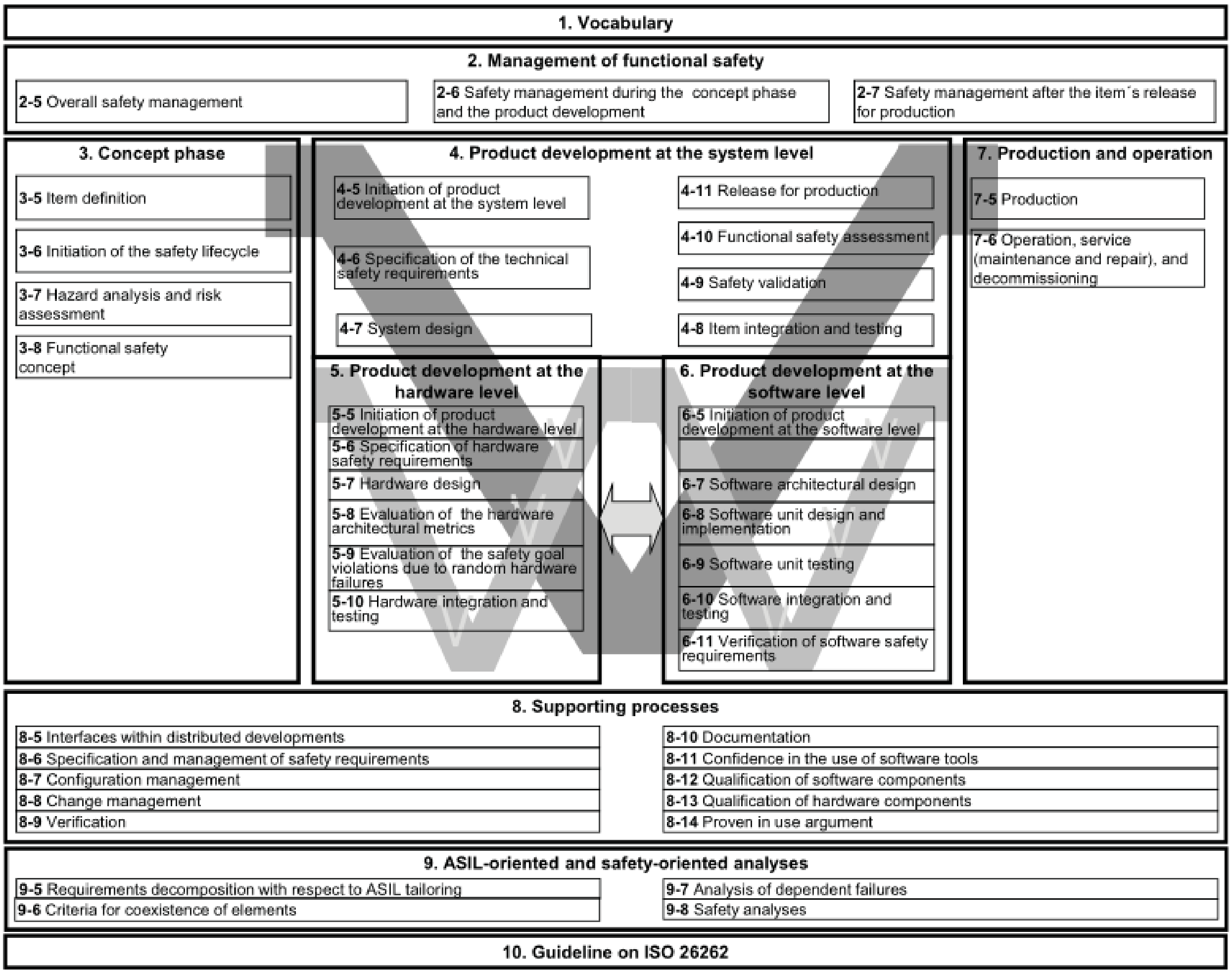
1. Vocabulary
2. Management of functional safety
2-5 Overall safety management
2-6 Safety management during the concept phase and the product development
2-7 Safety management after the item´s release for production
3. Concept phase
3-5 Item definition
3-6 Initiation of the safety lifecycle
3-7 Hazard analysis and risk assessment
3-8 Functional safety concept
4. Product development at the system level
4-5 Initiation of product development at the system level
4-6 Specification of the technical safety requirements
4-7 System design
4-11 Release for production
4-10 Functional safety assessment
4-9 Safety validation
4-8 Item integration and testing
7. Production and operation
7-5 Production
7-6 Operation, service (maintenance and repair), and decommissioning
5. Product development at the hardware level
5-5 Initiation of product 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 the safety goal violations due to random hardware failures
5-10 Hardware integration and testing
6. Product development at the software level
6-5 Initiation of product development at the software level
6-7 Software architectural design
6-8 Software unit design and implementation
6-9 Software unit testing
6-10 Software integration and testing
6-11 Verification of software safety requirements
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 use of software tools
8-12 Qualification of software components
8-13 Qualification of hardware components
8-14 Proven in use argument
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 analyses
10. Guideline on ISO 26262

Figure 8. Structure of ISO 26262

At the moment the ISO 26262 standard is currently in the process of rework and Edition 2 of ISO 26262 is intended for publication in mid of 2018. The major goals of the rework are:

1. Increase consistency between parts
2. Adapt standard to evolving technologies and industrial developments
3. Ease adaption and application of standard
4. Extension of the standard for other road vehicles like motorcycles, trucks and busses

As a sub goal for the second edition, it will contain some guidance on how to harmonize automotive system engineering with safety and security engineering.

4.2.2 Safety of the Intended Functionality - SOTIF

ISO 26262 addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems, including interaction of these systems. The ISO 26262 does not address the nominal performance of E/E systems, but the development of safety-related functions needs rules.

New automated functionalities are planned to be introduced in automotive vehicles and such kind of systems rely on information data from the environment provided by different kind of sensor technologies.

Such sensors could provide wrong interpretation-data of the environment that could lead to safety violations, even by fault free systems (e.g. wrong operation of processing algorithm on environment sensor inputs).

The ISO/TC22/SC32/WG8 is working on a standard under development called SOTIF, which is planned to be released by Mid of 2018 (in parallel to ISO 26262 2nd Ed.) as ISO PAS 21448, SOTIF-Safety Of The Intended Functionality“, which should provide guidance to avoid such kind of violations.

4.2.3 Automotive Cybersecurity

After the publication of SAE J3061, SAE and ISO started joint working group 11, which has the goal to develop an automotive cybersecurity standard. Currently a first task group structure (Risk management; Process overview / Interdependencies; Product development; Operations, Maintenance, other processes) was defined.

4.3 Railway Standards

The basic safety-related standards for railways are EN 50126, EN 50128, EN 50129 and EN 50159.

- EN 50126 – Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic Requirements and generic process.
- EN 50128 - Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems.
- EN 50129 - Railway applications – Communications, signalling and processing systems – Safety related electronic systems for signalling.
- EN 50159 - Railway applications. Communication, signalling and processing systems. Safety-related communication in transmission systems.

In all these standards “security” is not mentioned besides physical access, based on the traditional isolation of railway signalling and communication systems from regular public systems. With increased use of public facilities and wireless communication and control systems, e.g. the European Train Control System, the “security-aware safety” considerations in standardization are now starting also in the railway sector. DKE in Germany, is integrating requirements from IEC 62443 in the railway standards (proposal, addressing EN 50129 and EN 50159 issues) by DIN VDE V 0831-104 “Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443”.

4.4 Industrial Automation and Machinery Standards

IEC TC65 [6], Industrial-process measurement, Control and Automation, had started an ad-hoc group AHG1 to investigate the issue of coordination of safety, security, and was looking at a broad variety of domains and standardization groups starting to think about including (cyber-)security aware safety considerations. This was achieved already partially in IEC 61508, Ed. 2, by a group with members from ARTEMIS-IA.

IEC TC44 (Safety of machinery – electro-technical aspects) has started a new work item as well, somehow triggered by the general IEC concerns on cybersecurity impact on safety: “Security aspects related to functional safety of safety-related control systems”. IEC 62061 from TC44, Safety of Machinery, is a domain-specific standard implementing IEC 61508 for machinery. It is listed in the Official EU Journal since 31.12.2005 as a standard with presumption of conformity with EC Machinery Directive 2006/42/EC. A guideline for using IEC 62601/82601 and ISO 13849-1 (general machinery safety standard) was jointly developed and published by IEC TC 44 and ISO/TC 199 (safety of machinery) (IEC/TR 62061-1 and ISO/TR 23849).

Robotics is standardized mainly in ISO context (one exception are medical robotics, where some parts are mainly handled by IEC TC 62D) and these groups have now become an independent TC 299 (formerly part of ISO TC 184, machinery, as SC2).

In the meantime, AHG1 has completed its work with a report recommending preparation of an IEC TS on the topic "Framework to bridge the requirements for Safety and Security" and started a new working group IEC TC65 WG 20 under this title. There have been already a few Face-to-Face meetings (one in Vienna at AIT) and work is done via web and telephone conferences (almost monthly). Our goal is to keep our ARTEMIS - triggered intention to foster safety & security co-engineering and remain on a level to produce a basic safety & cybersecurity standard bridging IEC 61508 and IEC 62443 for industrial automation. This does not only impact production facilities and manufacturing industries, but also related industries in the transport, logistics, machinery and energy sector. A further concern is to keep this notion in line with the developments in other e.g. domain specific standards where ARTEMIS-IA members are active (e.g. automotive cybersecurity engineering, as explained later).

The "Human factors and functional safety" group IEC TC65 WG17 successfully restarted with a new convenor, Mr. Schaub, IABG, in Munich (Ottobrunn) from 4.-5.10.2016. The intention is now to write a TR (Technical Report) instead of a TS (Technical Specification) because this is easier to accomplish and finalize. This report should be fed into the IEC 61508 update cycle for Ed. 3.0 (or later), so it made sense for ARTEMIS project partners who are involved in IEC 61508 Ed. 3.0 to take part.

The maintenance cycle for IEC 61508-3 (Software) started in a "preparatory mode" already two years ago because so many software paradigms arose in the meantime which are already used in safety-critical systems' development but not covered by existing standards (or even quasi "forbidden"). The Hardware- und systems' people were not so eager to start (Part 1 and 2), but are impacted by some of the proposed changes in IEC 61508-3 as well (because in many cases the system aspect is most important, not just software or hardware). Some concepts developed and explored in ARTEMIS projects, like contract-based development, run-time certification and guidelines or mandatory requirements to achieve security-aware safety have already been brought into the maintenance cycle as topics.

In the recently established new ad-hoc working groups of IEC TC65 (Industrial process measurement, control and automation), AHG2 (Reliability of Automation Devices and Systems, meeting 1.-3.6.2016, Vienna, AT) and AHG3 (Smart Manufacturing – Framework and System Architecture, kick off meeting 4.4.-6.4.2016, Frankfurt, DE, and a follow-up meeting again in Frankfurt from 11.-14.10.2016) the upcoming topics are also related to multi-concern issues, complementing the other AHG1, now WG 20, mentioned before. AHG3 wants to identify frameworks for smart manufacturing on a higher level. This is another opportunity to find a path to standardization which needs multi-concern considerations to take into account, based on the Industry 4.0 RAMI 4.0 reference model. Complementary, IEC SC65E (Devices and integration in enterprise systems) started with an ad-hoc group AHG1 (Smart Manufacturing Information Models), covering the aspects of information models for exchange in context of enterprise systems, which has some impact on the work in IEC TC65A AHG3 and on interoperability.

Since Standardization in the field of machinery (except the electro-technical aspects) is done in ISO TC 184 and ISO TC 199, just now is the voting for a new work item in a joint working group ISO/IEC JWG21 "Smart Manufacturing – Reference Models" between IEC TC 65 and ISO TC 184, which is supported by several countries of ARTEMIS members and project partners, some of them already active in this process.

5. Active Involvement of AMASS partners

AIT and other partners are involved particularly in the IEC TC65 AHG-groups, IEC 61508-3 and the automotive standards covering multi-concern issues as part of the updates. Some successes were achieved with respect to cybersecurity and safety joint issues: in ISO 26262 DIS, in ISO 21434 starting at the kick-off with inputs from the holistic view pointed by us to take into account the interdependencies safety & security & maybe other dependability properties, consider related standards (safety, dependability),etc.

VIF is participating in the Austrian standardization committee regarding road vehicles "Komitee 038 – Straßenfahrzeuge" of Austian Standards. In this committee VIF is active member in the international ISO/TC022/SC32/WG08 for Functional safety. The following standards are under development by VIF participation:

- ISO 26262 – "Road vehicles -- Functional safety - 2nd Edition" (Planned Release: 2018)
- ISO PAS 21448 – "SOTIF-Safety Of The Intended Functionality" (Planned Release: 2018)

RISE (SPS) participates in the Swedish committees for several functional safety and cybersecurity standards, mainly in the industrial control, machinery and automotive domains: IEC 62061 (Swedish committee TK44), ISO 13849 (TK282), IEC 61508 (TK65), ISO 26262 (AG8), and the proposed ISO 21434 "Cybersecurity" (WG11). This includes taking part in development of new versions of these standards.

CEA and others OMG members are involved in the drafting of an OMG Request for Proposal (RFP). The RFP aims at soliciting proposals for a profile and/or model library for the OMG Unified Modelling Language (UML®) that works with the OMG Systems Modelling Language (SysML®) to allow the integration of safety and reliability information directly in a system model, where it can be modelled and processed directly with other system information. This RFP will be submitted February 20th, 2017.

CEA was also involved in the specification of the ISO/IEC 19514 standard (SysML 1.4) issued for publication last November 2016 by OMG.

HON is active in many standardisation activities. Main participation and contribution from the AMASS point of view is in European Aviation Safety Agency (EASA), Federal Aviation Administration (FAA), The European Organisation for Civil Aviation Equipment (EUROCAE). HON contributes to most important industrial guidance document from ARP, RTCA and SAE.

HON is also very active in the Airlines Electronic Engineering Committee (AEEC) and participate in more than 80 AEEC Project Initiation/Modifications. One of the activity is in AEEC Systems Architecture and Interfaces Subcommittee. The SAI NextGen and SESAR WG is revising ARINC 660B, which specifies the aircraft avionics functions necessary for operation in the evolving CNS/ATM environment expected for the FAA NextGen program and Single European Sky ATM Research (SESAR) program.

TEC together with **UC3** are members of the OMG group and both organizations take part in the discussions about the evolution of the SACM standard, whose 2.0 release is in beta version currently. TEC is focused on the argumentation part, which aims to formalize the assurance case creation, while UC3 is focused on the evidence-related topics. Both approaches are complementary and in parallel will work in the inclusion of AMASS related-aspects such as multi-concern assurance, variability, and evolution in the standard.

TEC in the past has been involved in discussion working groups related to the application of the ISO 26262 in self-adaptation systems, and the use of model-based techniques for the design and early validation & verification of critical functions.

UC3 is involved in the specification of standard tool integration mechanisms via the OSLC working groups[8]. The University participates in the discussion about certain specifications, e.g. the one for requirements management, and is starting the work on specifications for exchange of knowledge management data.

TRC and **UC3** collaborate in some INCOSE working groups[9]. These groups aim to provide standards and recommendations for industrial practices on systems engineering. More concretely, TRC and UC3 are active members of the Requirements Management Working Group and contribute to aspects related to V&V-based assurance, e.g. for correct requirements specifications. They are also involved in the group on Ontologies, which is chaired by Juan Llorens (UC3). For AMASS, the work of this working group mostly relates to assurance reuse, i.e. how to specify assurance information with ontologies and semantic technologies to enable effective and efficient information reuse across projects, products, and application domains.

GMV. Most of the projects in the space domain performed in GMV use the ECSS (European Cooperation for Space Standardization) and CCSDS (Consultative Committee for Space Data Systems) standards.

Additionally, SAVOIR (Space AVionics Open Interface aRchitecture) is an initiative to federate the space avionics community and to work together in order to improve the way that the European Space community builds avionics sub-systems. GMV is an active member in some of the SAVOIR working groups:

- SAVOIR-FAIRE: working group in charge of defining a Software reference architecture
- SAVOIR-IMA: working group in charge of defining a Software reference architecture for integrated modular avionics
- SAVOIR-SAFI: working group in charge of defining a Sensor/Actuator Functional Interface

GMV is also member of the ARINC 653 subcommittee, invited by Airbus.

GMV has been extensively involved in Eurospace DASIA events with the presentation of papers and studies related to modelling and tools, the on-board software reference architecture, Modular Avionics and Embedded systems.

[8] https://open-services.net/

[9] http://www.incose.org/ChaptersGroups/WorkingGroups

6. Conclusions

There is currently a window of opportunity in many domains and standards regarding multi-concern considerations. The interplay between dependability attributes is increasingly accepted by all involved shareholders and discussions on how to react to this development in standardization is ongoing. Safety and Security standards in multiple domains are currently in revision or (especially security standards) for the first time in development. For IoT and the increasingly open and dynamic systems, it will be necessary to regulate and consider multiple dependability attributes. Due to the ongoing involvement of AMASS partners in standardization activities, AMASS will influence standardization. It is still difficult to address such issues in a cross-domain way. Different domains have established safety standards, and security standards are partially designed to interact and extend existing standards. Therefore, we do not expect much overlap between the domains in standardization. A positive counterexample is the acceptance of IEC 62443 as template for future cybersecurity standards for additional domains like railways.

Besides multi-concern standardization, tool interoperability will also play an important role in the success of the AMASS platform. While AMASS will develop a core of assurance tools, there will always be external tools. Only accepted and well-specified interoperability standards will allow the seamless interoperability between AMASS internal and external tools and support the automation of engineering processes.

D8.9, as first standardization deliverable, has collected mainly the start of standardization and involvement of AMASS partners and has focused on multiconcern assurance, especially safety & security and interoperability. In the future we will also consider architecture-driven assurance and extend from interoperability towards reuse of assurance artefacts. An additional focus will be on the issue of compliance with standards, and maturity and process assessment models like SPICE and CMMI.

Abreviations and Definitions

AEEC	Airlines Electronic Engineering Committee
AHG	Ad-Hoc Group
ALM	Application Life-cycle Management
AMASS	Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems
ARINC	Aeronautical Radio Inc.
ARP	Aerospace Recommended Practice
ARTEMIS-IA	ARTEMIS Industry Association
CACM	Common Assurance and Certification Metamodel
CCSDS	Consultative Committee for Space Data Systems
CFDP	CCSDS File Delivery Protocol
CMMI	Capability Maturity Model Integration
CNS/ATM	Communication Navigation Surveillance / Air Traffic Management
CP-SETIS	Towards Cyber-Physical Systems Engineering Tools Interoperability Standardarisation
DASIA	Data Systems In Aerospace
E/E	Electrotechnical/Electronic
EAI	Enterprise Integration Patterns
EASA	European Aviation Safety Agency
ECSEL	Electronic Components and Systems for European Leadership
ECSS	European Cooperation for Space Standardization
EN	European Standard
ESA	European Space Agency
EUROCAE	The European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
HB	Handbooks
HTTP	Hypertext Transfer Protocol
IACS	International Automation Control System
IEC	International Electrotechnical Commission
IMA	Integrated Modular Avionics
IOS	Interoperability Specifications
IoT	Internet of Things
MBSE	Model-Based Systems Engineering
MMU	Memory Management Unit
OASIS	Organization for the Advancement of Structured Information Standards
OBC	On-Board Computer Unit
OMG	Object Management Group
OPENCOSS	Open Platform for EvolutioNary Certification Of Safety-critical Systems
OSLC	Open Services for Lifecycle Collaboration
OTA	Over the Air Updates
OWL	Web Ontology Language
PAS	Public Available Specification
PLM	Product Life-cycle Management
PSS	Procedures, Specifications and Standards
RAMI	Reference Architectural Model for Industry 4.0
REST	Representational State Transfer
RDF	Resource Description Framework
RFP	Request for Proposal
RTCA	Radio Technical Commission for Aeronautics

SA-WSDL	Semantic Annotations for WSDL
SACM	Structured Assurance Case Metamodel
SAE	Society of Automotive Engineers
SAVIOR	Space AVionics Open Interface aRchitecture
SESAR	Single European Sky ATM Research
SOAP	Simple Object Access Protocol
SOIS	Spacecraft Onboard Interface Services
SOTIF	Safety of The Intended Functionality
SoS	Systems of Systems
SPARQL	SPARQL Protocol and RDF Query Language
SPICE	Simulation Program with Integrated Circuit Emphasis
ST	Series of Standards
SysA	System Assurance Task Force
SysML	System Modelling Language
TM	Technical Memoranda
TS	Technical Specification
UML	Unified Modeling Language
URI	Uniform Resource Identifiers
V&V	Verification & Validation
XML	eXtensible Markup Language
W3C	World Wide Web Consortium
WG	Working Group
WP	Work Package
WSDL	Web Services Description Language
WSMO	Web Services Modelling Ontology

Bibliography

[1] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, Carl Landwehr, “Basic Concepts and Taxonomy of Dependable and Secure,” 2007.

[2] “OPENCOSS,” [Online]. Available: http://www.opencoss-project.eu/.

[3] “industrial Framework for Embedded Systems Tools,” [Online]. Available: http://www.artemis-ifest.eu/.

[4] “Combined Model-based Analysis and Testing of Embedded Systems,” [Online]. Available: http://www.mbat-artemis.eu/home/.

[5] “Safety Certification of Software-Intensive Systems with Reusable Components,” [Online]. Available: http://www.safecer.eu/.

[6] “ARROWHEAD | AHEAD of the future,” [Online]. Available: http://www.arrowhead.eu/.

[7] “Embedded Multi-Core systems for Mixed Criticality applications in dynamic and changeable real-time environments,” [Online]. Available: http://www.artemis-emc2.eu/.

[8] A. G. Ryman, A. L. Hors, and S. Speicher, “OSLC Resource Shape: A language for defining constraints on Linked Data,” in *LDOW*, 2013.

[9] C. Bizer, T. Heath, and T. Berner-Lee, “Linked Data - The Story so Far,” *Int. J. Semantic Web inf. Syst.,* vol. 5, no. 3, pp. 1-22, 2009.

[10] P. Hayes, RDF Semantics, World Wide Web Consortium, 2004.

[11] K. Manikas and K.M. Hansen, “Software ecosystems - A systematic literature review,” *J. Syst. Softw.,* vol. 86, no. 5, pp. 1294 - 1306, 2013.

[12] T. Thüm, S. Apel, C. Kästner, I. Schaefer, and G. Saake, “A Classification and Survey of Analysis Strategies for Software Product Lines,” *ACM Comput. Surv.,* vol. 47, no. 1, pp. 1 - 45, 2014.

[13] T. Berners-Lee, J. Hendler, and O. Lassila, “The semantic Web,” *Sci. Am.,* vol. 284, no. 5, pp. 34 -43, 2001.

[14] T. Berner-Lee, Linked Data, 2006.

[15] D. Krafzig, K. Banke, and D. Slama, Enterprise SOA: A service-oriented architecture best practice, Prentice Hall Professional, 2005.

[16] G. Hohpe and B. Woolf, Enterprise Integration patterns: designing, building, and deploying messaging solutions, Boston: Addison-Wesley, 2004.

[17] D. Roman et al., “Web service modeling ontology,” *Appl. Ontol.,* vol. 1, no. 1, pp. 77 - 106, 2005.

[18] M. G. Rodriguez, J. M. Alvaez-Rodriguez, D. B. Munoz, L. P. Paredes, J. E. L. Gayo, and P. O. de Pablos, “Towards a Practiacl Solution for Data Grounding in a Semantic Web Services Environment,” *J UCS JUCS,* vol. 18, no. 11, pp. 1576 - 1597, 2012.

[19] “ECSS Website,” [Online]. Available: http://ecss.nl.

[20] M. Jones et al, “Introducing ECSS Software-Engineering Standards within ESA,” ESA Bulletin.

[21] ECSS-E-ST, E. S. A, 40C Space Engineering-Software, Noordwijk: ESA-ESTEC Requirements & Standards Division, 2009.

[22] ECSS-Q-ST E. C. S. S. , 80C–Space product assurance-Software product assurance., European Cooperation for Space Standardization (ECSS) , 2009.

[23] “SAVOIR Website,” [Online]. Available: http://savoir.estec.esa.int.

[24] “CCSDS Website,” [Online]. Available: https://public.ccsds.org/default.aspx.

[25] “CRYSTAL - CRITICAL SYSTEM ENGINEERING ACCELERATION,” [Online]. Available: http://www.crystal-

artemis.eu/.

Appendix A. Standardization Survey

Table 1. Appendix A - Applicable standards and their domain

Item No	Standard No	Standard title	in force	Applicability for domains										Comment on domain / content / applicability	Quality attributes treated						
				Automotive	Railway	Machinery	Industrial control	Avionics	Space	ATM	Healthcare	Nuclear	IT System		Safety	Security	Performance	Availability	Reliability	Maintainability	Robustness
1	IEC 61508	Functional Safety	yes	X	X	X	X	x	x	x	X	X		Generic standard, Cyber security impact to strengthen NOW	X	.					
2	ISO 26262	Road vehicles – Functional safety	yes	x										Automotive, functional safety, Cyber security impact to include NOW	X	.					
3	EN 50126	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	yes		X									System level	X	.		X	X	X	
4	EN 50128	Railway applications - Communication, signalling and processing systems	yes		X									Software level, Cyber security impact to include NOW	X			X	X	X	
5	EN 50129	Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling	yes		X									RAMS guidance, Q24	X			X	X	X	
6	RTCA DO-278A	Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems	yes					X							X						
7	RTCA DO-178B/C	Software Considerations in Airborne Systems and Equipment Certification	yes					X							x						x
8	RTCA DO- 326A	Cyber-Security and Safety for Aircraft and Aircraft Systems	yes					X							X	X					x
9	RTCA DO-355	Information Security Guidance for Continuing Airworthiness	yes					X							x	x					
10	RTCA DO-356	Airworthiness Security Methods and Considerations	yes					X							x	x					x
11	RTCA DO-357	User Guide: Supplement to DO-160G	yes					X													
12	RTCA DO-160G	Environmental Conditions and Test Procedures for Airborne Equipment (Change 1)	yes					X						Testing of system performance under physical stress (temperature, vibrations, …)							

13	RTCA DO-248C	Supporting Information for DO-178C and DO-278A	yes					X													

Legend: "X"= high relevance, "x"= medium relevance, "." = minor relevance

Item No	Standard No	Standard title	in force	Applicability for domains										Comment on domain / content / applicability	Quality attributes treated						
				Automotive	Railway	Machinery	Industrial control	Avionics	Space	ATM	Healthcare	Nuclear	IT System		Safety	Security	Performance	Availability	Reliability	Maintainability	Robustness
14	RTCA DO-297	Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations	yes					X							x	x	x	x	x	x	x
15	RTCA DO-307	Aircraft Design and Certification for Portable Electronic Device (PED) Tolerance	yes					X						Aircraft design and certification recommendations to mitigate risks of using portable electronic devices on board							
16	RTCA DO-330	Software Tool Qualification Considerations	yes					X							x						x
17	RTCA DO-331	Model-Based Development and Verification Supplement to DO-178C and DO-278A	yes					X							x						x
18	RTCA DO-332	Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A	yes					X							x						x
19	RTCA DO-333	Formal Methods Supplement to DO-178C and DO-278A	yes					X							x						x
20	SAE-ARP 4754/4754A	Guidelines for development of civil aircraft and systems	yes					X													
21	RTCA DO-254	Design assurance guidance for airborne electronic hardware	yes					X							x		x		x		
22	ARP 4761	Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment	yes					X							x						
23	ISO/TS 15066:2016	Safety requirements for collaborative industrial robot systems and the work environment	yes				x								x						
24	SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems	yes	X									.	Automotive Cybersecurity		x					
25	SAE J3101	Requirements for Hardware-Protected Security for Ground Vehicle Applications		x									x	Automotive security		x					
26	IEC TC44	IEC 60204, ISO/IEC 17305, IEC 62046, IEC 614	yes			x								Safety of machinery, protective devices, separation of safety and security already at requirements level, Cyber security impact to include NOW	x	x	x		x		

Legend: "X"= high relevance, "x"= medium relevance, "." = minor relevance

Item No	Standard No	Standard title	in force	Applicability for domains										Comment on domain / content / applicability	Quality attributes treated						
				Automotive	Railway	Machinery	Industrial control	Avionics	Space	ATM	Healthcare	Nuclear	IT System		Safety	Security	Performance	Availability	Reliability	Maintainability	Robustness
27	ECSS-M-ST-40C	Configuration and information management	yes						x												
28	ECSS-M-ST-10C	Project planning and implementation	yes						x												
29	ECSS-M-ST-80C	Risk management	yes						x												
30	ECSS-M-ST-60C	Cost and schedule management	yes						x												
31	ECSS-Q-ST-10C	Product assurance management	yes						x												
32	ECSS-Q-ST-80C	Software product assurance	yes						x												
33	ECSS-E-70-41A	Telemetry and telecommand packet utilization	yes						x												
34	ECSS-E-ST-10C	System engineering general requirements	yes						x												
35	ECSS-E-ST-40C	Software	yes						x												
36	ECSS-E-ST-60-30C	Satellite attitude and orbit control system (AOCS) requirements	yes						x												
37	ISO 13849-1:2016	Safety of machinery -- Safety-related parts of control systems	yes			x									x						
38	ISO 10218-1:2011	Robots and robotic devices -- Safety requirements for industrial robots	yes				x							Industrial robots	x						
39	IEC/TR 62061-1	Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery	yes											Machinery safety guideline, IEC	X		x		x	x	

Legend: "X"= high relevance, "x"= medium relevance, "." = minor relevance

Item No	Standard No	Standard title	in force	Applicability for domains										Comment on domain / content / applicability	Quality attributes treated						
				Automotive	Railway	Machinery	Industrial control	Avionics	Space	ATM	Healthcare	Nuclear	IT System		Safety	Security	Performance	Availability	Reliability	Maintainability	Robustness
40	ISO/TR 23849	Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery	yes			X								Machinery safety guideline, ISO	X		x		x	x	
41	IEC 62061:2012	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems	yes			x								Machines with moving parts and machine directive harmonized	X						
42	IEC 61511	Functional safety - Safety instrumented systems for the process industry sector	yes												X						
43	ISO 2700x	Information security management systems	yes										x	Security aspects		X					
44	ISO 15408	Information technology -- Security techniques -- Evaluation criteria for IT security	yes										x	Common criteria, security aspects		x					
45	IEC 62589	Railway applications - Fixed installations - Harmonisation of the rated values for converter groups and tests on converter groups	yes		x																
46	IEC 62443	Industrial communication networks -Security for industrial automation and control systems	yes		.		x						x	Cybersecurity / Industrial automation and control systems security/ Network and system security for industrial process measurement and control. Basis of security for safety.		x					
47	IEEE 1686	Standard for Intelligent Electronic Devices Cyber Security Capabilities	yes				x							Cyber security		x					
48	EN 50159	Railways, Safety related communications	yes		x									Cyber security impact to include NOW	X	.					
49	IEC 62351	Power systems management and associated information exchange - Data and communications security	yes										x	Cyber security		x					
50	ISO 15026	Systems and software engineering — Systems and software assurance	yes	.	.	.	.	.	.	.	.	.	.	Generic standard for assurance of any quality attribute. Covers vocabulary, assurance cases, integrity levels, and assurance in the lifecycle.	x	x	x	x	x	x	x

Legend: "X"= high relevance, "x"= medium relevance, "." = minor relevance