Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments

Project Acronym:

EMC²

Grant agreement no: 621429

Deliverable no. and title	**D13.26 Final Standardization Report and Outlook**	
Work package	WP13	Project Management
Task / Use Case	T13.5	Standardization
Lead contractor	Infineon Technologies AG Dr. Werner Weber, werner.weber@infineon.com	
Deliverable responsible	AVL List GmbH Eric Armengaud eric.armengaud@avl.com	
Version number	v1.0	
Date	2017-05-13	
Status	Final	
Dissemination level	Public (PU)	

Authors

Partici-pant no.	Part. short name	Author name	Chapter(s)
02G	AIT	Erwin Schoitsch	Document structure, integration of all contributions, General Parts and ISO resp. IEC standards, new developments in Standardization, Outlook
02A	AVL	Christian El Salloum, Eric Armengaud	Part on IOS (Interoperability Specification)

Document history

Version	Date	Author name	Reason
0.1	2017-04-20	Erwin Schoitsch, Eric Armengaud	Set-up document
0.2	2017-05-02	Erwin Schoitsch	Update of Summary, Introduction, Standardization areas and description of progress in IEC TC65 Ad-Hoc Groups, ISO 26262, IEC 61508 and Railways, AIOTI, Cloud and IOT, Outlook
0.3	2017-05-06	Eric Armengaud, Christian el Salloum	Interoperability Specifications
0.95	2017-05-10	Petr Böhm, Christoph Schmittner	Review
1.0	2017-05-12	Erwin Schoitsch	Final Version
	2017-05-13	Alfred Hoess	Final editing and formatting, deliverable submission

Publishable executive summary

Standardization plays a key role in ARTEMIS (and ECSEL) industry-driven projects, and contribution to standardization is a mandatory part of any proposal, as part of market impact and exploitation of project results. Standardization is a medium to long-term issue compared to the duration of a research project (normally three years). Standardization schedules cover 5 years and more and an immediate uptake requires a "window of opportunity", i.e. the start of a new work item within the time frame addressed by the project or of a maintenance cycle of an existing standard for an update, which also may take five years or more. This means, that a long-term commitment to standardization is necessary to create the full impact. Fortunately, major partners involved in the standardization task of EMC², like AIT, AVL, Thales and many others, are committed to on-going standardization work. This includes the members of the ARTEMIS-IA Standardization Working Group, and CP-SETIS (H2020 project, grant agreement 645149) (most of them EMC² partners), which published just recently (May 2017) an updated Strategic Agenda on Standardization for Cyber-Physical Systems (ISBN 978-90-817213-3-2).

EMC² is quite aware of the importance of standardization. In the current Technical Annex "standardization" is referred to 178 times, most of the references concern contributions of work packages to standardization in their field of interest. Work packages cover technologies (WP1 – WP6) as well as "Living Labs" (containers of industrial use cases) (WP7-12). Since EMC² work packages involve a huge amount of standardization and standards related activities, the subtasks in this task are more complex than in other ARTEMIS or Framework Projects. To provide an overview over the various activities concerning standardization issues and to co-ordinate these activities in the overall frame of EMC² is a major challenge.

The task of WP13.5, standardization, is to harmonize and motivate work packages and tasks to progress towards their standardization goals. The actual work has to be done in the technology and living lab work packages.

This deliverable is the final report on progress in standardization since edition of the three previous deliverables of WP 13.5:

- D13.23 - Standardization survey, collecting active (participation in standardization groups and committees) and passive (monitoring as follower or applying standards) involvement of partners.
- D13.24 – Initial Standardization report and Plan (combined with D.23 in one document)
- D13.25 – Intermediate report about relevant standardization activities of the second year, particularly in the area of
    - Combined approaches to cybersecurity in safety critical systems (IEC, ISO). The work started 2014 and 2015. The topic is important from the "systems-of-systems" view of EMC², which is pertinent in the complex adaptive environments and systems being developed and assessed. Considerable progress was achieved in this respect in IEC and ISO functional safety standardization, with active participation and contribution from EMC² partners, which will continue driven by EMC² partners as delegates and experts from various national mirror committees.
    - Interoperability Specification – part of the efforts undertaken by the ARTEMIS-IA community towards an interoperability standard for tooling (IOS Specification), which in the beginning was based on OSLC and forwarded to an OSLC group within OASIS (CESAR, MBAT and SafeCer, CRYSTAL). Progressing in CRYSTAL, it turned out that IOS cannot be just one standard – it has to be a collection of standards, guidelines and specifications which are adopted to become part of the IOS database through a defined process. To achieve a sustainable structure, an ICF – IOS Coordination Forum - was

initiated by CP-SETIS partners which are partners in several ARTEMIS projects which are devoted to IOS contributions (CRYSTAL, EMC^2 and to a certain degree ARROWHEAD), and members of the ARTEMIS Standardization Working Group. In EMC^2, this is particularly part of WP5, with two deliverables, D5.23 – Interoperability and Standardization, State-of-Art analysis and D5.25 - Report on IOS Standardization work.

- Domain specific standardization activities of the work packages are covered in the annual reports and specific WP-deliverables.

At the end of the document, we provide an outlook on future work and challenges.

Table of contents

List of Figures

1. Introduction

1.1 Objective and scope of the document

The scope of this document is to report on
(1) Progress and additional results on evolving, EMC² standardization activities in IEC and ISO, with focus of the document being on functional safety and the interaction / extension towards cybersecurity & safety interaction and dependencies, but not excluding other related ISO and IEC activities particularly with respect to systems-of-systems issues, and on
(2) Progress with respect to the Interoperability Specification and Standardization.

Related work package deliverables are this time in particular:

Part of (1) was also discussed in WP6, System Qualification and Certification,

- Task 6.1, Certification and Qualification challenges of EMC²-Systems, in D6.8, **Final Requirement Set for WP6 – System Qualification and Certification** and
- Task 6.2, Assurance Methodologies for EMC2 Systems (Safety & Security), D6.9., **Safety & Security co-analysis and co-design (contracts for trust),**

with contributions from authors of this deliverable D13.26.

The Interoperability issue (Part (2)) (particularly of the ARTEMIS High-Reliability project cluster) is discussed in more detail also in WP 5, System Design Platform, Tools, Models and Interoperability, Task T5.5, Interoperability and Standardization, Deliverables D5.23 and D5.25.

1.2 Structure of the document

The document consists of seven parts:

1. Introduction
2. Overview over challenges of the standardization in EMC²
3. Overview over standardization plans and activities of the work packages and tasks
4. Promotion of EMC² activities towards standardization organizations in IEC and ISO towards coordination of safety and security issues in functional safety standardization
5. Interoperability Specifications – the way forward
6. Outlook – what to expect, the way forward.
7. References

2. Overview on Challenges of the Standardization Task in EMC²

Standardization is one of the key elements in exploiting results of research projects, therefore ARTEMIS-IA has founded an active Working Group on standards and Regulations, which has completed a Standardization Support Action "ProSE" (Promoting Standards for Embedded Systems) (lead Thales France, Technical Manager AIT) which resulted in the ARTEMIS Strategic Standardization Agenda. Further on, the Standardization task can build on experiences from many key partners who have been or are active in related projects of the ARTEMIS High-Rel Cluster of projects (iFEST, MBAT, SafeCer, R3-COP, CRYSTAL, RECOMP, Innovation Action CP-SETIS to harmonize the Interoperability Standardization activities across several ARTEMIS projects, etc.) with respect to standardization,

Since EMC² work packages involve a huge amount of standardization and standards related activities, the subtasks in this task are more complex than in other ARTEMIS or Framework Projects and to provide an overview over the various activities concerning standardization issues and to co-ordinate these activities in the overall frame of EMC² is a major challenge. Therefore, the main actual work particularly in domain-specific standardization activities has to be done in the technology WPs WP1 – WP6 and the Use Case oriented Living Labs WP7 – WP11.

Therefore, the main objective is to coordinate and harmonize the various standardization plans and activities addressed in technology WPs and LLs to gain momentum.

In EMC², Standardization is one of the "Expected Innovations", as cited in the Technical Annex:

AWP expected innovation #4: Certification and standardization
Projects are expected to propose an architecture to allow the investigation of the architectural design by the certification authorities as foreseen in the subject development standards of the individual industrial domains (aerospace, automotive, railway, wind-power, smart grid, medical, etc. ...).

All EMC² use cases are strongly bound to certification and standardization. Especially living labs WP7 to WP9 have strong requirements, which need to be fulfilled by any architecture (or application running hereon). Therefore, EMC² directly targets system qualification and certification through its dedicated WP6. The tool environment to be developed within the scope of WP5 as well as application models and design tools of WP2 are aware of these requirements, therefore supporting development with respect to standards and certification compliance.

The activities have to be organized strategically to achieve impact in those fields of interest where the potential and chance to succeed in a reasonable time frame are best. Therefore the so-called survey (assessment, D13.23) was of key importance and aligned with the first year's milestones of the Technology Work Packages (WP1-WP5) and Living Labs (WP7-WP12). This is to be able to include results e.g. from WP5 in a joint deliverable or reference it properly. The next step is to identify "windows of opportunity" provided by the schedules of relevant standards (maintenance phase or new work items).

This **"Window of Opportunity"** is fortunately given at the moment for the two major functional safety standards:

- **IEC 61508,** where **Ed 3.0** has started to be planned and discussed, and
- for the automotive domain, where just now **ISO/DIS 26262: 2018 (which is Ed 2.0)** was just issued, including already the contributions of EMC² partners in the field of **"Safety and Cybersecurity Interfaces" (SCI)** in **Part 2** and **Part 4**.

Additionally, the severe concern of TC65 on the impact of cybersecurity, reliability and related system properties on functional safety, has led to the creation of three IEC TC65 Ad-Hoc Groups (AHG) and was one contributor to starting the development of a new standard item in ISO in cooperation with SAE for cybersecurity engineering in the automotive domain:

- **IEC TC65 AHG1: "Framework towards coordinating safety, security (in industrial automation), now IEC TC65 WG 20, "Framework for functional safety and cybersecurity"**
- **IEC TC65 AHG2: "Reliability of Automation Devices and Systems",**
- **IEC TC65 AHG3: "Smart Manufacturing Framework and System Architecture"** (Kick-off April 2016); this group will address the issues of highly interconnected industrial automation systems for smart manufacturing in a multi-concern manner, covering most of the topics relevant in context of EMC².
- **"Joint ISO/TC 22/SC 32 - SAE WG, Automotive security engineering"**
  During the EMC2 project SAE published the first Guidebook (SAE J3061) aiming at Automotive Cybersecurity and with a focus especially on the safety and security interaction. WP6 and WP7 started immediately with evaluating and applying the Guidance document on the ongoing technical developments aimed at automotive use cases and these experiences, especially also on co-engineering of Automotive Safety and Cybersecurity are one of the influences which are contributed to the development of the new set of Standards. Development started with a first F2F Kick-off meeting (October 2016) in Munich, with participation of EMC2 members.

Another Ad-Hoc Group AHG1 was founded in IEC SC65E (Devices and integration in enterprise systems), called "Smart manufacturing information models". This subcommittee SC65E looks at enterprise management systems from top level down to devices. The main concern in AHG1 is interoperability of models and data exchanged and managed by smart items in enterprise context, so it belongs rather to the "Interoperability Specification" standards group as addressed in chapter 5.

An additional reason for efforts towards standardization is the commitment of EMC² to contribute to the ARTEMIS CRTP, to the ARTEMIS repository and to comply with the ARTEMIS interoperability specification as started with CESAR and continued in MBAT and CRYSTAL. The first implementations of the interoperability specification are making use of OSLC, so the involvement in OSLC and participation in the OASIS group is an important issue, but the further development of the IOS as a set of adopted standards, specifications and guidelines is not restricted to OSLC.

A detailed description of standards to be addressed is to be found in the technology WP descriptions and living lab descriptions (Annexes B-M of the Technical Annex). It should be noted that much of the work for standardization is already included in the WP efforts. An example for standardization work in other areas is partner AICAS with its involvement in **Real-time JAVA** standardization**. AICAS** is engaged in **JSR 282** work. The Realtime and Embedded Specification for Java 2.0 is now complete and will be presented to the Java Community for its final review.

For the standardization task, co-ordination of the activities, organization and management of the approaches to standardization organizations are the primary subtasks in T13.5.

Note: By experience from recent years, time schedules of standardization are by far longer than three years of a research project, not to forget that results of a certain maturity are normally achieved towards the end of the project. Therefore part of the standardization activities will be to identify such "windows of opportunity", where final stages of standards development and of the project match properly. Successful examples in the past from AIT have been introducing Time-Triggered Architectures, Model-based testing and Automated Test Case Generation as results from the FP6 IP DECOS and the FP7 STREP MOGENTES in IEC 61508-3, when the third year of MOGENTES matched the final stage of IEC MT 12 activities). In the second reporting period, several standardization groups on functional safety started officially to consider for the first time or more detailed than before (IEC 61508) the impact of security attacks on safety-related and safety critical systems. This work continued in the current reporting period.

3. Overview over standardization plans and activities of the work packages and tasks

From the WPs, particularly WP5, System design platform, tools, models and interoperability, and WP6, System qualification and certification, with tasks on safety and security assurance methodologies, are contributors to evolving, updating or new standards and users of existing standards. One of the innovations in EMC² is the holistic approach to safety and security assurance and trust case building, and the qualification/certification of mixed-criticality, multi-core systems with resilience requirements, i.e. managing adaptability to changing environments and adaptive maintenance and enhancements during system lifetime under hard real-time run-time conditions in a safe and secure manner. This case is currently not considered in functional safety qualification/certification and needs not only new techniques/measures but also extensions to standards and processes, or new standards and processes. A list of standards to be addressed is to be found in section "References".

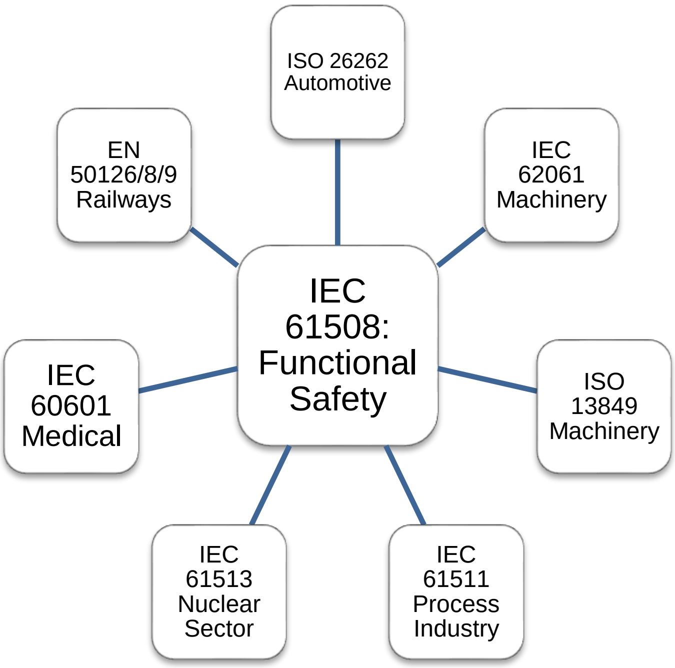


Figure 1: Functional Safety Standards – Security Awareness needed to be included as issue (WP6, WP13.5)

From the other technology WPs and the Living Labs, a short overview delivers:

WP1, SP_SoA – embedded system architecture, expects improvements of standards related to SoA (Service oriented Architecture) protocols and service semantics with focus on the critical applications to be addressed as innovation, through IRTF, IPSO and W3C.

WP2, with focus on application models and design tools for mixed criticality, multi-core embedded systems, works on clear separation of applications, optimized resource usage, code generation and offline analysis tools, with a strong safety concern. This impacts standardization and qualification considerably.

WP3, dynamic run-time environments and services, is involved in inter-core and inter-processor communication standardization and APIs. WP3 will propose results to platforms such as AUTOSAR.

WP4, multi-core hardware architectures and concepts, is interested in processor qualification and verification.

From the Living Labs, WP7 focusses on automotive standards, qualification of automotive software, ETSI standards around LDM automotive-relevant communication standards (ETSI, IEEE).

WP8 focusses on safety standards for airborne systems, e.g. SAEs ARP 4761.

WP9 focusses on aerospace systems (ECSS standards). Details on standardization in Avionics systems for space applications include

- Standardization of the basic functions and the way they interface with each other, in order to allow higher complexity within manageable and affordable limits, justify the increasing of R&D funding through the Space Agency and within all the European Industry Communities. “Avionics Embedded Systems” covers avionics system aspects, which are not adequately covered by a single discipline or technology domain. In fact, it covers areas from On-board Data Systems, to Space Systems Software to Space System Control.
- Within EMC²’s activities the following Areas will be covered:
  - Architectures and interfaces
  - Building Blocks (involving HW and SW)
  - Avionics on-board communications
  - Distributed avionics systems
  - Adaptive, reconfigurable avionics systems (including Fault Tolerant Architecture)
  - Development process and related methods and tools

WP10 (industrial manufacturing and logistics) have to consider, besides the functional safety standards for machinery and protective equipment, EMC standards and security challenges for smart devices integrated in large, complex assemblies (to build a chain of trust on multiple roots of trust).

WP11 includes several use cases based on (mixed criticality) communications of networked EMC² nodes and systems. Many different technologies are applied and assessed – safety and security enhancements are necessary, communication profiles of several communication standards and protocols will be evaluated and the need for extensions or separate profiles for mixed criticality applications evaluated. System qualification and certification in networked environments (trust cases), system architectures and platforms from the WPs are validated. Influence on standardization activities of WPs is expected. Standardization issues are (besides others)

- TTEthernet
- IEEE 1588 group
- ETSI standards (communications, M2M, …)
- Smart Grid related standards (many around these topics in IEC and ISO)
    - smart homes innovations with emphasis on management systems
    - autonomic algorithms and autonomic computing
    - smart home metering
    - smart home energy management

WP12 – cross-domain applications - covers different application domains (control, surveillance and railways). Several standardization groups are affected (security of MPSoCs, resource management, tools, dependability, security, performance of systems, system qualification and certification, etc.). Most standards addressed in WP6 are of relevance. Standards cover, mainly for use, but in a few cases like robust vision, vision based protective devices, medical imaging and railways:

- Surveillance and vision (security, privacy, robustness and reliability)
- Medical imaging (medical safety issues)
- Railways (new issue: security aware safety case evolving)

4. Ongoing promotion of EMC² activities towards standardization organizations in IEC and ISO towards coordination of safety and security issues in functional safety standardization

4.1 Overview with respect to EMC²

As explained before, promotion of research project results towards standardization requires for a rather fast exploitation a "window of opportunity", i.e. a standardization process for a specific topic is in state that allows appropriate input at the right time.

Awareness has risen considerably that in an interconnected world where isolated systems are no longer possible the impact of security attacks on safety has to be taken into account in all life cycle stages of safety related or safety critical systems. That requires some interaction between safety and security measures and cooperation respectively coordination between the two communities which were quite separated in the past (and still are).

EMC² is particularly addressing highly networked adaptive systems, from internally connected multi-cores (quasi-static) to dynamically changing/adaptive closed ones to evolving dynamic open "systems-of-systems" (see Figure **2**).

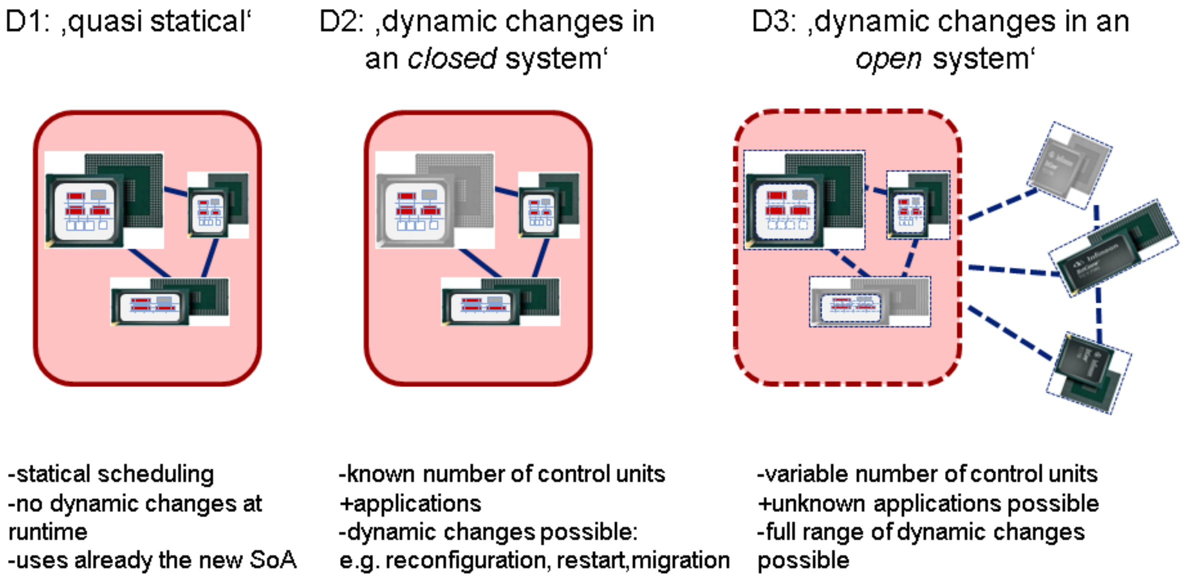

D1: ‚quasi statical'
D2: ‚dynamic changes in an *closed* system'
D3: ‚dynamic changes in an *open* system'
-statical scheduling
-no dynamic changes at runtime
-uses already the new SoA
-known number of control units +applications
-dynamic changes possible: e.g. reconfiguration, restart,migration
-variable number of control units
+unknown applications possible
-full range of dynamic changes possible

Figure 2: EMC² - from closed to open systems

The functional safety standards of the first generation did not tackle the challenges of highly connected "systems-of-systems". Particularly, the arising security issues were not considered at this time in context of safety. Security in an open system has become a new factor in system engineering and safety analysis.

4.2 IEC 61508 Functional Safety of E/E/PE Systems

4.2.1 General overview

IEC 61508 Ed. 2.0 [IEC 04] finished 2010, took as first functional safety standard into account that security may have impact on safety of a system. Therefore it requires consideration in the risk and hazard analysis phase, with accompanying measures to be undertaken in the following phases; particularly security has then to be reflected in the safety manual.

Although security engineering itself is excluded in the description of the scope of the standard, the standard states that it

"*…requires **malevolent and unauthorized actions** to be considered during hazard and risk analysis". The **scope of the analysis includes all relevant safety lifecycle phases."***

The notes definitely address IEC 62443 [IEC 07] and ISO/IEC TR 19791 [ISO 03] (Part 1, 1.2, k). Security is mentioned in multiple requirements for the safety engineering lifecycle. Security threats need to be considered in the Hazard and Risk analysis:

" The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuse and malevolent or unauthorized action). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorized action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out." (IEC 61508, Part 1, 7.4.2.3).

A security threat analysis should be conducted if a security threat is identified as a potential cause for a hazard. For guidance on security risks analysis IEC 61508 refers to the IEC 62443 series (*Industrial communication networks – Network and system security*) and to ISO/IEC/TR 19791. It is explicitly noted that malevolent or unauthorized action includes security threats. If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements (IEC 61508, Part 1, 7.5.2.2).

Finally, Part 3 requires that all details about security should be included in the safety manual: *"The following shall be included in the safety manual: (...) Details of any security measures that may have been implemented against listed threats and vulnerabilities."* (Part 3, Annex D 2.4).

Similar concepts are now evolving in IEC 61511, Ed. 2, and ISA TR 840009. Just recently, work on defining harmonized IT security requirements for railway automation was started [Brab 01], with the goal to build on the well-known safety certification processes of EN 50129, EN 50159 and integrate security requirements based on IEC 62443.

The initial concept to relate the rigor of security evaluation levels (EALs of Common Criteria) to the potential impact on safety (SIL level) did not find the necessary consensus. Now SLs (Security Levels 1 – 4) of IEC 62443 seem to be more accepted by industry than the Common Criteria EALs. Nevertheless, there is now some work in the automotive domain on using EAL levels and especially the approach to define an Protection Profile (implementation independent set of requirements) across manufactures as guidance document for automotive Ethernet and mixed criticality communication was developed by an EMC2 partner and will be presented in ongoing standardizations.

In the preparation phase of IEC 61508-3 Ed. 3.0 (Software part), which started Nov. 20-21, 2014 in Frankfurt, and was continued in Toulouse March 17/18, 2015, it was decided to look at the ongoing activities in ISO and IEC with respect to "security-aware safety" and to provide more mandatory and informative guidance on a coordinated approach to security in context of functional safety.

4.2.2 Progress in IEC 61508-3:

At the **IEC 61508-3 meeting in Tokyo, April 5-7, 2016**, an extensive proposal was tabled, guided by EMC² work in this respect, to provide more guidance and adapt the existing mandatory and non-mandatory requirements, examples and notes.

The document states:

> *The intention is not to define requirements for the development, implementation, maintenance and/or operation of security but to give guidance on how to integrate security engineering in software safety lifecycle and when to consider security.*

(Changed/added) Mandatory Requirements (marked yellow) addressed are:

(this list is insofar not complete, as "should" requirements and other notes are not summarized here; this is just to demonstrate the main ideas of the proposal)

> ***7.1.2.5*** *Any customisation of the software safety lifecycle shall be justified on the basis of functional safety.*
>
> *NOTE Increased system safety by consideration and integration of cybersecurity related activities in the software safety lifecycle is such a justification*
>
> ***7.1.2.6*** *Quality, and safety assurance procedures shall be integrated into safety lifecycle activities*
>
> *NOTE Quality includes, if applicable, security*
>
> ***7.2.2.10*** *The software safety requirements specification shall express the required safety properties of the product, but not of the project as this is covered by safety planning (see Clause 6 of 61508-1). With reference to 7.2.2.1 to 7.2.2.9, the following shall be specified as appropriate*
>
> *b3) safety related (cyber)security requirements*
>
> ***7.2.2.12*** *Where data defines the interface between software and external systems, the following performance characteristics shall be considered in addition to 7.4.11 of IEC 61508-2*
>
> *NOTE Security threats can cause a violation of performance characteristics*
>
> ***7.4.2.14*** *This Subclause 7.4.2 shall, in so far as it is appropriate, apply to data and data generation languages.*
>
> *….. configuration data, to ensure that the configuration data correctly states the application logic and to protect the configuration data against unauthorized changes.*
>
> ***7.4.3.2*** *The software architecture design shall be established by the software supplier and/or developer, and shall be detailed. The software architecture design shall*
>
> *g) consider safety related (cyber)security aspects*
>
> ***7.7.2.7*** *The validation of safety-related software aspects of system safety shall meet the following requirements:*
>
> *a) testing shall be the main validation method for software; analysis, animation and modelling may be used to supplement the validation activities;*

b) *the software shall be exercised by simulation of:*

1) *input signals present during normal operation;*
2) *anticipated occurrences;*
3) *undesired conditions requiring system action, including, if applicable unauthorized and malicious input;*

7.8.2.6 *The safety planning for the modification of safety-related software shall meet the requirements given in Clause 6 of IEC 61508-1.*

NOTE Depending on the nature of the application, trustworthiness of staff and involvement of domain and security experts may be important.

> *Details of any identified vulnerabilities, implemented security measures and potential implications and constraints on performance (including response time), effectiveness, reliability or operation of functions important to safety.*
>
> *The possibility that a failure or vulnerability in one element (such as an overflow, or divide by zero exception, or an incorrect pointer calculation) may cause or enable a consequent failure in other elements.*

4.3 Progress in Ad-Hoc Groups of IEC TC65:

4.3.1 IEC TC65 AHG1 – Framework towards coordinating safety, security

In IEC TC65 (Industrial-process measurement, control and automation) considerable concerns arose with respect to the safety impact of security issues in industrial automation systems, since many complex systems of that kind are becoming connected "systems of systems", particularly by interaction based on wireless connectivity from sensors/actuators to complete plants, grids etc., in maintenance and operations. An Ad-hoc Group (AHG1- "Framework towards coordination of safety and security") was founded to look into the issue and provide recommendations how to handle the co-ordination of security issues in functional safety standards. The kick-off took place Oct. 28/29 2014 at VDE in Frankfurt. In the first meeting overviews were provided by several participants from Europe, Japan, China, US and Australia on ongoing activities and some research projects. E. Schoitsch from AIT provided an overview on several domains and the ARTEMIS projects ARROWHEAD, EMC² and SESAMO which had in-depth work provided in the field of security-aware (security-informed) safety. The domains were not restricted to IEC standards areas but included also conceptual ideas from railways (EN 50126/28/29 and EN 50159), Airworthiness standards, Nuclear, Off-shore Platforms and Automotive (including pre-information from safety & security workshops e.g. at Fraunhofer IESE, ISSE WS at SAFECOMP 2014 Florence, ICCVE 2014 Vienna, ISSC Boston 2013 etc.).

The overall question to be discussed and recommendations to be given are: *„How to manage safety and security - in cooperation, integrated, separately? How to certify critical industrial systems taking industrial Cyber-security into account?"*

A short overview on standards' approaches discussed is provided here:

- Railways (DIN/VDE just updating EN 50129: Pre-standard DIN V 0831-104) – integrative approach (with IEC 62443, SL 1)
- Airworthiness Standards: 3 security standards (DO 326A (E 202A) Airworthiness Security Process Specification; DO 355 (ED 204) Information Security Guidance for Continuing Airworthiness; evolving DO YY3 Airworthiness Security Methods and Considerations) – far reaching separation
- IEC 62859: Nuclear power plants – fundamental principles defined how to include cybersecurity without impacting safety

- IEC 61511/ISA TR 840009 (draft) proposes the Cyber Security Life Cycle to be integrated with Process Safety Management
- TC44, Safety of Machinery, electro-technical aspects: separation of safety and security already at requirements level, OEM (integrator) should be the only responsible, not the machinery manufacturer - not appreciated e.g. by ISA or most of the experts.
- Example from an off shore facility: different safety and security levels at different parts of the facility assessed jointly, to be considered in allocation phase.
- IEC 62443 (security levels SL 1-4) vs. Common Criteria (ISO 15408, Evaluation Assurance Levels EAL 1-7): IEC 62443 the preferred standard for industrial automation.

EMC² was presented as an example for a well-founded approach to design, assess, manage and later on be able to qualify/certify such systems at several meetings of IEC TC65 AHG1, ISO TC22 SC 32 WG08 and IEC 61508-3 preparation for Ed. 3.0.

AHG1 finished its work 2015 by presenting a report to the Plenary of IEC TC65 on Oct. 30, 2015, in Dalian, China: "**AHG1 – FRAMEWORK TOWARD COORDINATING SAFETY, SECURITY**".

The report was accepted, the recommendation was a NWIP (New Work Item Proposal). This NWIP was proposed by the Japanese Committee, because Koji Demachi, the chairperson of AHG1, is an expert sent by the Japanese Committee and is voted 2016 (deadline 2016-05-06).

The proposal was to develop a **TS (Technical Specification) "Industrial-process measure-ment, control and automation - Framework to bridge the requirements for safety and security"**

The scope is "The project will develop a technical specification (TS) to facilitate the application of safety and cyber security standards by bridging the relevant technical areas, in the area of industrial-process measurement, control and automation. The scope includes, but is not limited to, aspects of the cyber security of safety-related systems."

During the follow-up meetings, it was recently decided to change the title of the WG20 to "Framework for functional safety and cybersecurity", and to start with a TR (Technical Report), which is easier to agree) rather than with a TS. The concept of a fuzzy understanding of "interference" was extended to more concrete "interaction points" between functional safety and cybersecurity teams, as shown in the following figure (Figure 3):

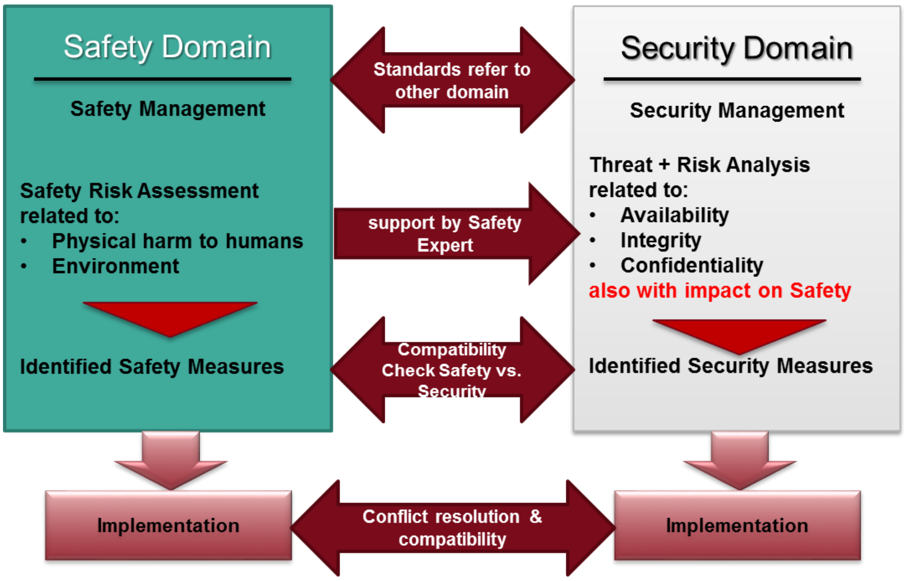

Safety Domain
Safety Management
Safety Risk Assessment related to:
• Physical harm to humans
• Environment
Identified Safety Measures
Standards refer to other domain
support by Safety Expert
Compatibility Check Safety vs. Security
Security Domain
Security Management
Threat + Risk Analysis related to:
• Availability
• Integrity
• Confidentiality
also with impact on Safety
Identified Security Measures
Implementation
Conflict resolution & compatibility
Implementation

Figure 3: Safety & Security Co-Engineering, WG 20, current proposal

4.3.2 IEC TC65 AHG2: “Reliability of Automation Devices and Systems”

IEC TC65 has defined the majority of functional safety standards (generic: IEC 61508, and most domains except road vehicles: ISO 26262) (see Figure 1). TC65 as main safety-standardization group, is looking primarily on the system (safety, security are system properties and rather holistic). On the contrary, IEC TC56 is standardizing reliability evaluation and calculation methods.

But TC65 identified gaps in the TC56 approach with respect to the requirements for automation devices and systems. Therefore TC65 created the Ad-Hoc Group AHG2, “Reliability of Automation Devices and Systems”, which looks at the demand of reliability design, test, verification and operational life of (safety related) automation devices and systems as handled by IEC TC65. This will be based on the analysis of the applicability of relevant standards in automation devices and systems and define the standardization frame of reliability for automation devices and systems.

Here, systems means low-level systems, like control loops, control modules, other than plants, except any programming for controller (covered already by IEC 61131).

The group started in Oct. 30, 2015, in Dalian, China, and continues its work via telephone conferences and internet/emails. The next Face-to-Face meeting took place in Vienna at AIT, June 1-3, 2016. The idea to look primarily at the integration aspect and the device/component requirements needed to achieve the system/systems of systems view of reliability and the interaction with safety and security, and not to compete with IEC TC56 (“Dependability”), which cover quite well the reliability methods, models and mathematics of (hardware) components, has still to be fought for.

4.3.3 IEC TC65 AHG3 - Smart Manufacturing Framework and System Architecture

This group will address the issues of smart manufacturing in a multi-concern manner, covering most of the issues relevant in context of EMC². The Kick-off is in April 4 – 6, 2016, Paris.
The scope and motivation is given as:

> *The general goal of the ad-hoc group is to contribute to clarify the relationships between the concepts coming from these different bodies:*
> - *terminology,*
> - *system models (description of structure),*
> - *dictionaries, semantics (classes and properties of electronic catalogues),*
> - *device profiles,*
> - *transaction models,*
> - *resources and asset descriptions.*
>
> *The ad-hoc group shall take into account different axis:*
> - *value stream (supply chain, key performance indicators ...),*
> - *life cycle,*
> - *enterprise levels,*
>
> *The task of the ad-hoc group is to:*
> - *draw a picture of the existing standards and projects;*
> - *recognize the acknowledged references,*
> - *identify gaps between the models and the needs of the industry.*

This is relevant not only for top-level considerations in EMC². This is even more relevant for related ARTEMIS projects, e.g. ARROWHEAD, SemI40, or, in future, Productive4.0. AIT took part in this AHG3 group meetings, the Kick-off was in Paris, April 4 – 6, 2016. This group is very well aware about the importance of safety & cybersecurity co-engineering, and has taken up several use cases to demonstrate the relevant aspects for the final report, which may lead to another WG in IEC. One of the use cases is provided by EMC² partners derived from the ECSEL project SemI40, on safety & security of device/enterprise systems. Anyway, work done in EMC² provided considerable initial input and motivation.

It should be noted, that there has been founded now a joint working group JWG21 "Smart Manufacturing Reference Models" of IEC TC65 and ISO TC 184 ("Automation and Integration"). In IEC SC65E ("Devices and integration in enterprise systems") a complementary activity was started ("Smart manufacturing information models").

4.4 ISO 26262: 2018 (Ed. 2.0):

A proposal from Austria (AIT) to ISO TC22 SC32 WG 08 (road vehicles – functional safety) presented at the ISO 26262 meeting at VDA in Berlin, Jan. 29/30, 2015, was set up by AIT after the AHG1 kick-off meeting, taking up ideas as well as some concerns pro and con from AHG1 members and WP6 of EMC².

The proposal left open, of course, the details, which approach should be taken, although the proposer (AIT, Austria) preferred a more integrated approach. The proposal looked like

- Cyber-security should be included as an risk factor to be considered during hazard and risk analysis
- If necessary appropriate security measures should be implemented, e.g. include recommendations for fitting security standards into ISO 26262 Ed. 2.0
- Include a requirement consolidation phase to resolve potential conflicts and coordinate safety and security requirements
- Validation of safety concept should <include>/<consider> security concept
- Security has to be considered throughout the whole (safety) life cycle – recommendations to be included where appropriate

It was decided to re-evaluate the issue in a small task group, which has started to work already, with input from industry and AIT, based on WP6 intentions. In automotive this is of great interest because of the developments towards the "connected car" (V2V, V2I, highly automated or even autonomous driving) – all trends that make security an important vulnerability and risk factor for safety [Sch01].

Progress 2016 in ISO 26262:2018 (Ed. 2.0):

In this respect there was already considerable progress. The Cybersecurity & Safety Task Group started work shortly after the January 2015 presentation at VDA in Berlin, mainly via email and telephone conferences. The output were

- One mandatory requirement for Part 2, Management of functional safety:

  5.4.2.3 *The organization shall institute and maintain effective communication channels between functional safety and other disciplines that are related to functional safety.*
  EXAMPLE 1 Communication channels between functional safety and cybersecurity in order to exchange relevant information e.g. the hazard analysis and risk assessment (see ISO 26262-3:2018, Clause 7), threat analysis and vulnerability analysis, safety goals (see ISO 26262-3:2018, Clause 7), cyber security countermeasures and functional safety measures. See also Annex F.

- Many additions and notes in Part 2,Part 4 and Part 6 (Product development at the system level / software level) referring to the additional impact and necessary treatment of cybersecurity in context of functional safety, as taking into account threats and system vulnerabilities similar to safety hazards and risks and especially ensuring compatibility between safety and security.
- In Part 2, an Annex F (informative) “Guidance on potential information exchanges between functional safety and cybersecurity” (directed at team cooperation and activities, identifying interface resp. communication points during the life cycle); this part exceeds what was already achieved 2010 in IEC 61508 to consider security when impacting functional safety. Figure 4: Overview of ANNEX F in ISO 26262-2 DIS Stage of Edition 2, gives an overview of the current content of Annex F. The Guidance is on two levels, on the company level there is guidance how cybersecurity and safety should interact and cooperate between projects, as example information about used tools (like compiler versions) that should be exchanged in order to ensure that no vulnerabilities or faults are introduced by tools with insufficient tool qualification. In addition, there is project specific guidance on the interaction for concept, product development and production and operation phase regarding information exchange and cooperation. It should be remarked that Annex F was developed and finalized before the development in the "Joint ISO/TC 22/SC 32 - SAE WG, Automotive security engineering" started and therefore the references are more specific on the safety lifecycle part. The goal was to ensure that the Annex is compatible with developments for automotive security engineering and does not restrict them.

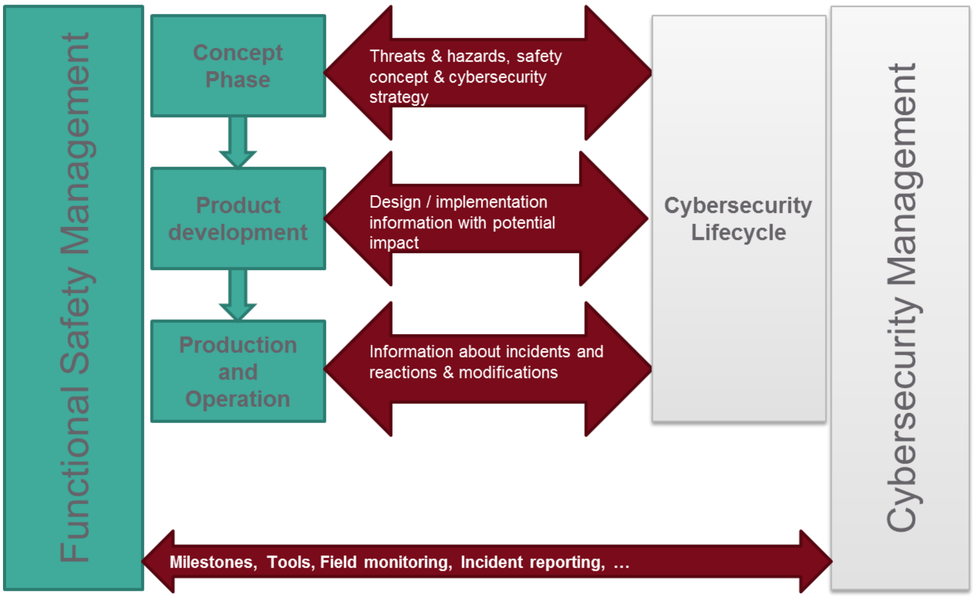

Functional Safety Management
Concept Phase
Product development
Production and Operation
Threats & hazards, safety concept & cybersecurity strategy
Design / implementation information with potential impact
Information about incidents and reactions & modifications
Cybersecurity Lifecycle
Cybersecurity Management
Milestones, Tools, Field monitoring, Incident reporting, …

Figure 4: Overview of ANNEX F in ISO 26262-2 DIS Stage of Edition 2

These changes are already part of ISO/CD 26262 – 2018; the CD was commented upon until February 2016 and the comments were discussed in Salzburg, April 6 – 8, 2016.

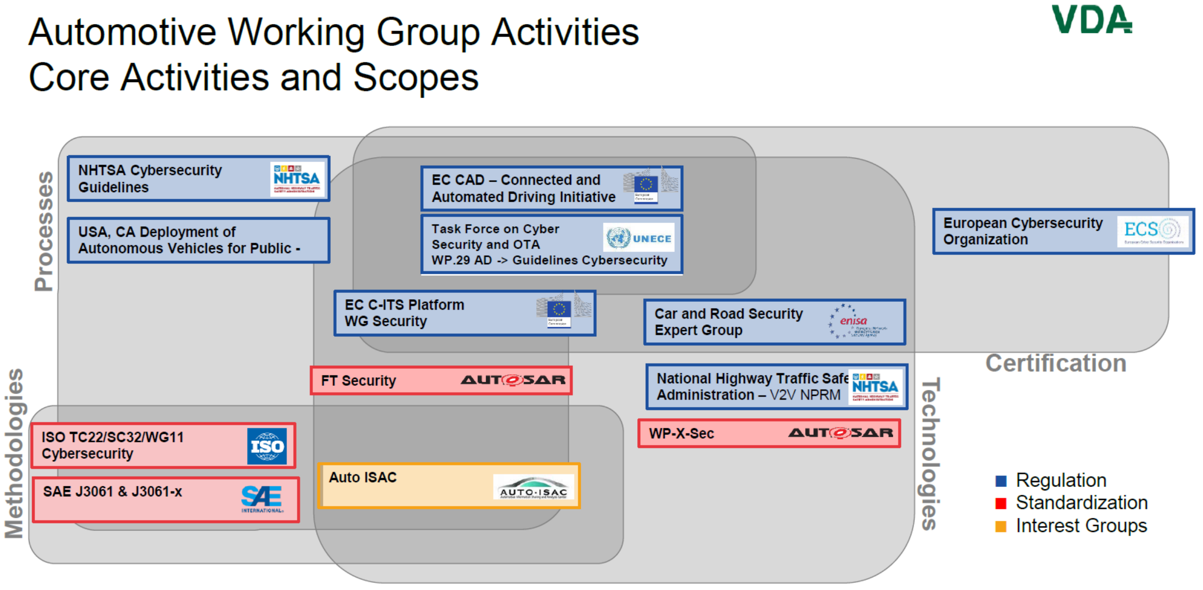
The work progressed further successfully and put forward extended proposals primarily for additions to Part 2 and Part 4. At the last meeting of ISO TC 22 SC 32 in JeJu in South Korea February 6 – 10, 2017, we successfully achieved, that the cybersecurity impact from the safety point of view has to be taken in to account throughout the life cycle. There are requirements and guidance now in Part 2 (Safety Management), Part 4 (Product Development) and Part 6 (Software Development). An Annex in Part 2 provides some guidance on the interaction between safety and cybersecurity teams in the process of a holistic approach to system engineering, which is now part of the DIS and will hopefully in autumn 2017 lead to the FDIS, the last phase before being voted and published as an IS (International Standards).

4.5 SotiF – Safety of the intended Functionality

Unfortunately, an important part of the planned ISO 26262:2018 edition on “SotiF – Safety of the intended Functionality” could not be included in the current Ed. 2.0 (2018) version, but will be continued as a PAS 21448 (Publicly Available Specification) to be later integrated into ISO 26262 (Ed. 3.0?) or become a separate standard (not decided at the moment). This part could be most important for self-driving autonomous vehicles because without failure of a component or constituent in the sense of ISO 26262 Ed. 1.0, a system may fail in its intended functionality e.g. by wrong interpretation of sensor input, unexpected environmental conditions and wrong perception of a situation. However, a majority of national mirror committees considered it not to be sufficiently mature for inclusion in ISO 26262:2018 within the schedule of this standard. Nevertheless, the SotiF issue will play an important role in many application areas of highly automated systems of all kinds as well in highly automated M2M systems.

4.6 Joint ISO/TC22/SC32 - SAE WG, Automotive cybersecurity engineering

Since both sides, SAE and DIN/DVA, proposed cybersecurity automotive engineering standardization work items, a PSDO agreement (Partnership Standards Development Organization) recently signed between ISO and SAE came into force by founding a joint working group ISO/SAE JWG1, which should develop an agreed standard, now called ISO 21434. “Road vehicles – Cybersecurity engineering” (in ISO: ISO TC22 SC32 WG11). This type of cooperation between two groups organized in such totally different ways, with different voting and decision mechanisms, is absolutely new. The kick-off meeting was in Munich, 19.-21.10.2016. Our goal was, as mentioned above, to keep developments in line with other cybersecurity/safety standards and co-engineering. The first ideas collected in brainstorming groups at the kick-off meeting look quite promising for a holistic solution which would conform somehow with the results of EMC² and ARROWHEAD (and related ARTEMIS/ECSEL projects). ARTEMIS-IA partners like AVL and AIT were active at this meeting. This is another good example that overarching topics have to be addressed jointly (the landscape around this is shown in Figure 5:



Automotive Working Group Activities
Core Activities and Scopes

VDA
Processes
Methodologies
Technologies
Certification
NHTSA Cybersecurity Guidelines
USA, CA Deployment of Autonomous Vehicles for Public -
EC CAD – Connected and Automated Driving Initiative
Task Force on Cyber Security and OTA WP.29 AD -> Guidelines Cybersecurity
UNECE
European Cybersecurity Organization
ECS
EC C-ITS Platform WG Security
Car and Road Security Expert Group
enisa
FT Security
AUTOSAR
National Highway Traffic Safe Administration – V2V NPRM
NHTSA
WP-X-Sec
AUTOSAR
ISO TC22/SC32/WG11 Cybersecurity
ISO
SAE J3061 & J3061-x
SAE INTERNATIONAL
Auto ISAC
AUTO-ISAC
■ Regulation
■ Standardization
■ Interest Groups

Figure 5: Automotive Cybersecurity: Core Activities and Groups

4.7 Railways

In railways, the solution as it is planned by VDE in Germany is a more integrated one and was presented at the first Safety & Security Workshop at Fraunhofer IESE last year in September, with presentations from AIT and VDE as well.

In the railway domain, safety engineering is guided primarily by a set of four standards:

- EN 50126 Railway Applications – the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS):
  - Part 1 – Basic Requirements and generic process (CENELEC 1999, Corr. 2010)
  - Part 2: - Guide to the application of EN 50126-1 for safety (informative) (2007)
- EN 50128 Railway Application – Communication, signaling and processing systems – Software for railway control and protection systems (IEC June 2011)
- EN 50129 Railway Applications - Communication, signaling and processing systems – Safety related electronic systems for signaling (IEC 2003, corrigenda 2010).
- EN 50159 Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems.

The current version of EN 50126-1 does not address security issues and unauthorized access issues. It states

"…this standard does not specify requirements for ensuring system security".

Nevertheless, similar as was defined the relation of security to safety in IEC 61508 Ed. 2 (2010), we find:

- Under "4.3 Elements of Railway RAMS" it states (4.3.4) *"Security as an element that characterizes the resilience of a railway system to vandalism and unreasonable human behavior, can be considered as a further component of RAMS. However, consideration of security is outside the scope of this standard".*
- Under "6.2 System definition and application conditions" *"security hazards"* are listed in the scope of the system hazard analysis.

The current version of EN 50128 (2011), although published after IEC 61508 (2010) does not refer to security at all. But in the mean-time, as railway communication systems are no longer isolated and use partially public or wireless networks even to transmit critical information and data, and wireless communication is used as well for control and signaling (GSM-R, ETCS Level 2). The cybersecurity issue effects EN 50159 (Railway applications - Communication, signaling and processing systems - Safety-related communication in transmission systems) as well.

EN 50129 does not address security as well. However, chapter B.4.6 "Protection against unauthorized access" (normative Annex B, operation with external influences, to be described in Section 4 of the Technical Safety Report of the Safety Case) takes into account different access levels guarding against unauthorized access. This focuses primarily on personal access (related to ISO 27001), but requires to define how protection is achieved against accidental and intentional unauthorized access in general. Security is one of the protection means of "external conditions". These requirements allow to be extended to cybersecurity threats as well.

Therefore awareness has raised in the community that security issues have to be considered as potential cause of safety critical failures. An approach has started particularly in Germany (DKE) to include security requirements in EN 50129 by taking into account IEC 62443, the international group of standards for communication and network security for industrial networks. It was identified that the 41 requirements for security level 1 (SL 1) of IEC 62443 ("Protection against casual or co-incidental violation") are mostly covered already explicitly by requirements of EN 50129 or usually fulfilled, a few are not in the scope of safety. It is recommended to include the missing SL1 requirements in the safety system's requirements and add them in future to EN 50129. DKE in Germany plans a guideline based on IEC 62443 to address some issues, particularly of higher SLs having safety impact, in more detail. An integration of industrial "Cybersecurity for Safety" should be proposed, which allows separation of issues as far as possible, but without missing the context of a joint overall system certification including safety relevant security issues as part of the safety certification. This was discussed e.g. at the 1st Safety & Security Workshop at Fraunhofer IESE in Kaiserslautern on Sept. 15, 2014 (Jens Braband, Hans-Hermann Bock) and the Conference "Safety meets Security" at IESE, Kaiserslautern, on March 2, 2016. A discussion document (internally, not public) **DIN VDE V 0831-104, Electric signalling systems for railways – Part 104: IT Security Guideline based on IEC 62443,** does exist already.

In the meantime, the relevant standardization group in CENELEC, TC9X, SC9XA, took over the work, which is responsible for maintaining EN 50129, the basic railway safety standard, which defines the "Railway Safety Case", and other railway standards.

An advisory group SC9XA SGA16 was asked

"to prepare a report for the next meeting of SC9XA, setting out the proposed scope of a future standard on IT security and recommending whether it should be a EN/TS/TR."

SGA16 recommended

- to create an EN related to IT Security for Signalling
- a scope for a NWI proposal
- to embed this EN into an overall framework at TC9X

The overall framework of CENELEC TC9X is depicted as in Figure 6:

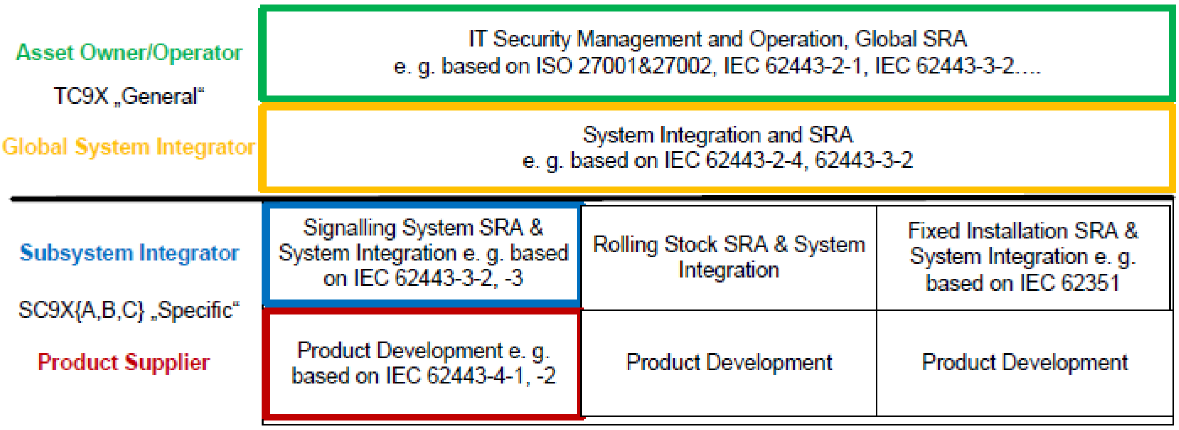

Asset Owner/Operator
TC9X „General"
Global System Integrator
IT Security Management and Operation, Global SRA
e. g. based on ISO 27001&27002, IEC 62443-2-1, IEC 62443-3-2….
System Integration and SRA
e. g. based on IEC 62443-2-4, 62443-3-2
Subsystem Integrator
SC9X{A,B,C} „Specific"
Product Supplier
Signalling System SRA & System Integration e. g. based on IEC 62443-3-2, -3
Rolling Stock SRA & System Integration
Fixed Installation SRA & System Integration e. g. based on IEC 62351
Product Development e. g. based on IEC 62443-4-1, -2
Product Development
Product Development

Figure 6: Overall CENELEC TC9X Framework (Railways Safety and Security)

5. Interoperability Specifications

A second important activity is related to interoperability specifications. This work started in the ARTEMIS project CESAR[1], then was handed over to further European projects such as MBAT[5], nSafeCer[4] and CRYSTAL[6]. In order to set up a sustainable organizational structure as a platform joining all stakeholders and to coordinate all IOS-related activities, especially the formal standardization and further extensions of the IOS, several partners submitted together with stakeholders from other projects a proposal for an innovation action in the H2020-ICT-2014-1 call, called **CP-SETIS**[7] *(Towards Cyber-Physical Systems Engineering Tools Interoperability Standards***)**. SafeTrans coordinates the CP-SETIS project (H2020 Innovation Action, grant agreement 645149), and the initiative has been driven by EMC², nSafeCer, MBAT and CRYSTAL partners. This chapter gives an overview of the proposed Innovation Action. The CP-SETIS project was accepted for funding and successfully started in March 2015, finishing May 2017 [CP-SETIS 01]

5.1 Background & Motivation

Past and on-going EU research projects have initiated a momentum around a common vision for the Establishment of Recognized International Open Standards of Lifecycle Tool & Data Integration Platforms for CPS Engineering.

Related EU research projects include:

- **CESAR[1] (59 partners)** - Cost-efficient methods and processes for safety relevant embedded systems, an Artemis project,
- **iFEST[2] (21 partners)** - industrial Framework for Embedded Systems Tools, an Artemis project,
- **Sprint[3]** – Simplifying the Design of Complex Engineering Systems, an FP7 ICT project
- **p/nSafeCer[4] (29 partners)** - Safety Certification of Software-Intensive Systems with Reusable Components, an ARTEMIS project, tool integration in a CTF (Certification Tool Framework)
- **MBAT[5] (39 partners)** – Combined Model-based Analysis and Testing of Embedded Systems, an Artemis project
- **CRYSTAL[6] (71 partners)** - CRitical sYSTem engineering AcceLeration, an Artemis project

However, the current situation with respect to IOS (pre-) standardization is characterized by a wide variety of activities, which are only partly coordinated:

- There is a wide variety of projects running, which build upon and extend the IOS (, EMC2, DANSE, D3COS, HOLIDES). These projects are run by different consortia and have different objectives. Many of them are already doing or at least aiming at pre-standardization activities for the IOS. Although there are some initiatives from these projects, to establish bilateral harmonization of IOS pre-standardization activities in areas of overlap, these initiatives only cover part of the IOS and only few projects.

[1] http://www.cesarproject.eu/
[2] http://www.artemis-ifest.eu/
[3] http://www.sprint-iot.eu/
[4] http://www.safecer.eu
[5] http://www.mbat-artemis.eu
[6] http://www.crystal-artemis.eu/
[7] https://cp-setis.eu/

- New projects emerge that aim at interoperability solutions for development tools, where the consortia are not always aware of the existing IOS and its applicability for their project objectives.
- First attempts of formally standardizing parts of the IOS (for Lifecycle Interoperability, OSLC based) within OASIS have been started, but cover only part of the IOS.
- The commitment of major stakeholders to IOS activities is strong at project level, but not always on an inter-project or even company-wide level.
- Different groups, organizations, clusters and networks (like for example the ARTEMIS Working Groups on Standardization and on Tool Platforms, the ARTEMIS Center of Innovation Excellence EICOSE) have a high interest in and support both, activities for Interoperability of Development Tools as well as Standardization Activities, but still more commitment is required from all key stakeholders involved in IOS Activities.

On an inter-project level, this lack of coordination leads to ungovernable structures, un-coordinated and therefore potentially diverging activities, thus jeopardizing the huge investment in and the innovation potential of the IOS by endangering the chance of establishing a major standard in Cyber-Physical Systems engineering.

5.2 Challenges, Goals and Objectives

The two main challenges to be addressed by the CP-SETIS Innovation Action can be summarized as follows:

- Challenge 1 (Organizational & Strategical): A common vision and mission, shared by all major stakeholders, for supporting lifecycle data and tool interoperability for CPS Engineering has to be established urgently and acted upon, aligning the as yet only partially coordinated European IOS-related activities and paving the way for establishing the IOS as a major standard in CPS Engineering.
- Challenge 2 (Technical): A clear bridge has to be defined between the on-going definition of the IOS and other wide spread Interoperability and Engineering Standards commonly used by European developing organizations (e.g., ASAM[7], FMI[8], AUTOSAR[9], STEP[10], OMG ReqIF[11], etc.) for supporting CPS Engineering activities.

In order to tackle these issues, CP-SETIS is articulated by the following goals and objectives:

- Goal 1: The alignment of all IOS-related forces within Europe to support a common IOS Standardization Strategy, aiming at a formal standardization process of the IOS.
- Goal 2: The definition and implementation of sustainable IOS Standardization Activities supporting both, formal standardization of ‘stable’ IOS versions as well as extensions of IOS, if possible within existing structures that survive the lifespan of single projects.

[7] Association for Standardisation of Automation and Measuring Systems, http://asam.net
[8] Functional Mockup Interface for model exchange and tool coupling, https://www.fmi-standard.org
[9] AUTomotive Open System Architecture, http://autosar.org
[10] STEP – standing for "Standard for the Exchange of Product model data" is the informal name used for the ISO 10303 standard for the computer-interpretable representation and exchange of product manufacturing information.
[11] Requirements Interchange Format, http://www.omg.org/spec/ReqIF/

From these goals, the following objectives were derived:

- Objective 1: To build-up a consensus across key stakeholders (i.e., end-users organizations, tool providers, research organizations) and projects on a common IOS Standardization Strategy.
- Objective 2: To define a concrete model for sustainable IOS Standardization Activities (activities, processes, roles, responsibilities, interactions with projects, end-users, tool providers and relevant standardization bodies).
- Objective 3: To support implementation of sustainable IOS Standardization Activities within sustainable structures having a far longer lifespan than a single project (for example: existing ARTEMIS-IA structures10, i.e., the Tool Platform Working Group, the Standardization Working Group, the EICOSE Center of Innovation Excellence, etc.).
- Objective 4: To get commitment from key stakeholders for supporting common IOS Standardization Strategy and its implementation (firstly from key end-users and projects, ARTEMIS-IA, secondly from key tool & technology providers).
- Objective 5: To generalize findings of IOS Standardization Activities to update then ARTEMIS/PROSE Strategic Agenda for Standardization and to support further Standardization Activities within ARTEMIS/ECSEL.

5.3 Standardization Activities for a Multi-Standard

In CRYSTAL, it turned out very soon, that it is not possible to create just one single IOS standard, it has to be a set of standards, specifications, processes and guidelines. For such 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, including the IOS specific extensions into these standards, (b) for those parts that 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).

5.3.1 Adoption of new parts into the Multi-Standard

With respect to process 1 above, i.e., the selection of new specifications for inclusion and adoption into the Multi-Standard, a stepwise approach depicted in Figure 7 is appropriate.

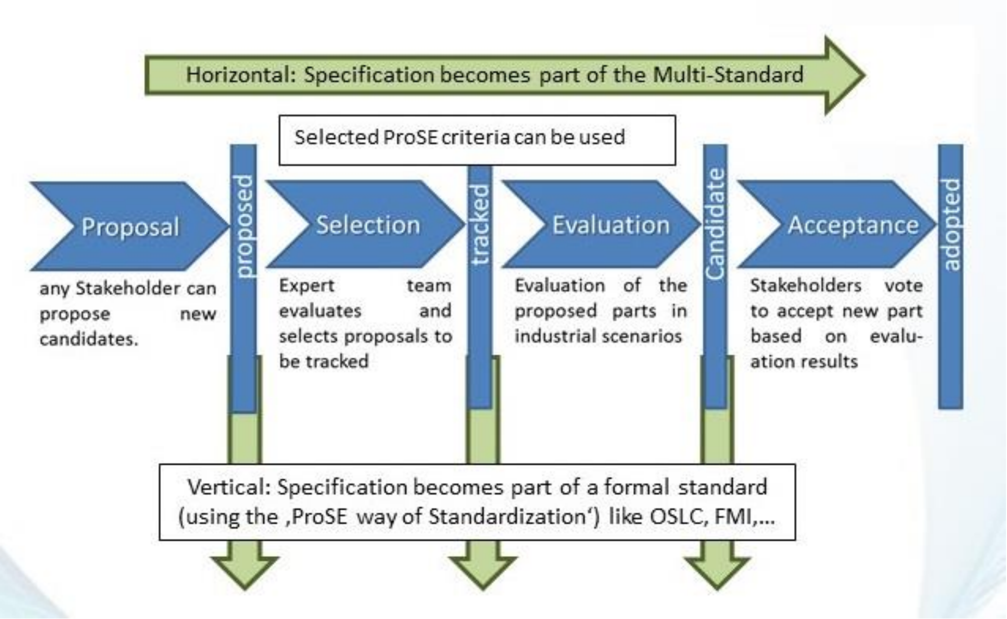

Horizontal: Specification becomes part of the Multi-Standard
Selected ProSE criteria can be used
Proposal
proposed
Selection
tracked
Evaluation
Candidate
Acceptance
adopted
any Stakeholder can propose new candidates.
Expert team evaluates and selects proposals to be tracked
Evaluation of the proposed parts in industrial scenarios
Stakeholders vote to accept new part based on evaluation results
Vertical: Specification becomes part of a formal standard (using the ‚ProSE way of Standardization') like OSLC, FMI,...

Figure 7: Multi-Standard Approach: Horizontal and Vertical Maturity-Level Advancement Process

This approach assumes that there is a structure/organization whose members decide about inclusion and maturity advancement of new parts and new specifications within the Multi-Standard, much like a standardization body would do for a single standard. In the case of the Interoperability Specification, this organization is the IOS Coordination Forum (ICF, c.f. 3.2.). We will give a high level description of this process, which we think is appropriate for any Multi-Standard. A more detailed description of the process as implemented specifically for the IOS can be found in the Deliverables of the CP-SETIS project.
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.

Each part of the Multi-Standard undergoes maturity level advancement according to the following process. Any stakeholder can **propose** a specification for inclusion into the Multi-Standard. At this point in time, there need not even be all the information about the new part available, probably not even the full specification. The minimum information to be supplied depends on the specific Multi-Standard in question. In the case of IOS, this minimum information includes

(a) The name of the specification,

(b) Which Engineering Concern is (or will be) covered by this specification,

(c) Which, if any, existing standard does this specification build on (and possibly extend), and

(d) The names of the promoters of this specification, i.e., the stakeholders that plan to develop this specification. For other Multi-Standards, the required information may differ, but in any case not too much information is needed at this early stage.

A quick check by a – probably small – team of experts will determine whether a proposed specification becomes **tracked**. Typical evaluation criteria will be the fit with the scope of the Multi-Standard, check for minimal or even no overlap with existing parts of the Multi-Standard, and perhaps size and impact of the promoter group. Note that these criteria are a subset of the criteria used for selection of a single-standard (c.f. Table 4 in Section 4.1.).

While in tracked state, additional information about the part must be supplied by the promoters. Obviously, the specification itself is needed for further evaluation. Use cases to show the applicability and usefulness of the specification should be provided as well as reference (prototype) implementations (where appropriate) and any further information needed to assess the new part. In the case of IOS, both the development of the specification as well as its application to use cases and the set-up of reference implementations were done for most IOS parts in publicly funded projects. Depending on the specific Multi-Standard in question, this might or might not be an appropriate model, especially considering the long run-time of these projects and the corresponding time these parts stay in tracked state. The tracked state is concluded with an evaluation by an expert team in cooperation with the promoters. Again, a subset of the criteria for a single-standard depicted in Table 4 is used here together with criteria about technical maturity, especially the appropriateness of the use case selected, the applicability and 'success' of applying the specification to the use case and its incorporation in the reference implementation. A successful evaluation leads to the part becoming a **candidate**. In the candidate state, the stakeholders vote upon for adoption into the Multi-Standard. The evaluation results from the candidate stage are the basis for this vote and a positive vote leads to the state **adopted**, i.e., the specification is now a full member part of the Multi-Standard. If stakeholders deem it necessary to modify/extend this specification in the future, a new version of this part will be **proposed** and the process starts again (depending upon the concrete criteria used for state tracked in this specific Multi-Standard, the process for those updates and modifications could start in the state **tracked**).

At least two aspects are noteworthy within this process:

First, the existence of a managing organization is absolutely necessary for this process to work. Handling all the book-keeping (which part of the Multi-Standard is in which state, which information about this part is available where, which promoters/stakeholders are associated with each state, and much more) is only one part of the work that this organization has to perform. Other activities are mandatory for the success of a Multi-Standard:

- keeping the process running,
- supplying experts for evaluation and
- being able to supply up-to-date information about all parts of the Multi-Standard to the multitude of other processes that are running in parallel, like evaluation and maturity level advancements of different parts, formal standardization activities of different parts, implementations or application activities of different parts, etc.

The second aspect concerns the similarities of this process with the standardization for single standards:

- groups of promoter organizations to propose, develop (i.e. specify) and evaluate a candidate for a standard, which then becomes a formal standard through a defined process managed by the rules of a support organization (similar to the standardization body hosting a single standard), where this process involves all stakeholders/promoters of this specification.
- Although these processes differ in detail – especially for Multi-Standards where the maturity level advancement of each part requires considerably more knowledge about other parts of the Multi-Standard than what is typically the case for a single standard – the processes are similar enough to use experiences and methods known from standardization of single standards. This observation applies, for example, to the various criteria for selecting standards originally

collected in the PROSE project, which also apply to the various steps of maturity level advancement for parts of a Multi-Standard.

5.3.2 Formal Standardization of parts of a Multi-Standard

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 (c.f. 4.1.), that is, stakeholders would decide which parts to formally standardize, 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 against 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 not be required, not be worth the effort or even be 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.

For any Multi-Standard, one has to decide which maturity level a specific part needs to reach before it can become a formal standard. Obviously, adopted parts of the Multi-Standard are candidates for standardization, but there are probably many cases in which it is beneficial to even start standardization at lower maturity levels. As an example, the IOS standardization of parts based on OSLC started while these parts were in the tracked state. As for the question of the minimum maturity level requirement for formal standardization, this specifically depends upon the Multi-Standard in question, and might even depend upon the specific part considered for standardization. Therefore, it is advisable not to define this minimum level in advance, but leave the stakeholders to decide on a case-by-case basis.

5.4 Implementation of the IOS Multi-Standards Approach

For a Multi-Standard, it is therefore essential that a stakeholders establish some kind of organizational structure that

- Collects, maintains and makes accessible all information about the Multi-Standard, especially the current specifications of each part, their maturity level, links – if any – to standardization bodies, etc.
- Serves as a communication forum, i.e., as a place where stakeholders can meet (physically or virtually) to coordinate their activities, plan extensions of the specification and formal standardization of its parts, and which generally supports all of these activities.

In the specific case of the IOS (as the only known instance of a Multi-Standard now), the CP-SETIS project, funded from the Horizon 2020 ICT-1 call, set out to derive and implement such an organization structure for the Multi-Standard IOS.

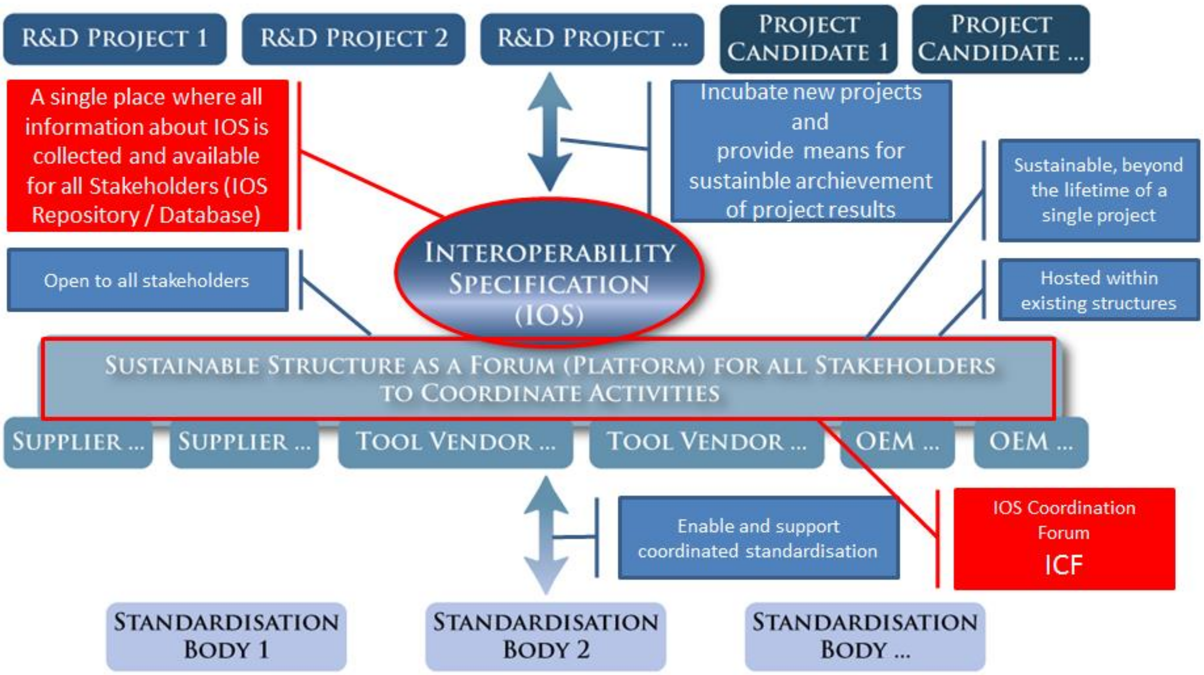

R&D Project 1
R&D Project 2
R&D Project ...
Project Candidate 1
Project Candidate ...
A single place where all information about IOS is collected and available for all Stakeholders (IOS Repository / Database)
Incubate new projects and provide means for sustainble archievement of project results
Sustainable, beyond the lifetime of a single project
Open to all stakeholders
Interoperability Specification (IOS)
Hosted within existing structures
Sustainable Structure as a Forum (Platform) for all Stakeholders to Coordinate Activities
Supplier ...
Supplier ...
Tool Vendor ...
Tool Vendor ...
OEM ...
OEM ...
Enable and support coordinated standardisation
IOS Coordination Forum ICF
Standardisation Body 1
Standardisation Body 2
Standardisation Body ...

Figure 8: IOS Standardization - goals

Figure 8 depicts the corresponding goals of the project: to implement an organizational structure that serves as a coordination and harmonization forum for all IOS related activities of the stakeholders – here called the IOS coordination forum (ICF) – and that at the same time sets up and maintains the IOS Database, a place where all IOS related information is stored. (see 5.2.).

As has been explained above, the existence of a coordination forum like the ICF is essential to handle Multi-Standards. To fully exploit the benefits of these kinds of forums even beyond the essential needs, one has to carefully exploit and weigh up implementation alternatives against each other:

- Obviously, the coordination forum needs to be sustainable, i.e. it has to have a lifetime that goes beyond the lifetime of typical projects. Defining the financing and organizational structure is therefore very important.
- The coordination forum needs to be independent and neutral to ensure openness of the specification as well as openness and equal participation rights for all stakeholders.
- The coordination forum needs to be, or at least to be supported by, a legal body, to be able to act as a legal entity (e.g. hire personnel, buy infrastructure, etc.). On the other hand, stakeholders often dislike creating 'yet another legal body'. Ideally, one would be able to establish this structure within an existing legal structure. Care has to be taken to choose this 'hosting structure', which needs to be neutral and sustainable as well as trusted by stakeholders to fit this purpose.

When these implementation alternatives are met, stakeholders can take full advantage of the benefits that such a coordination forum. They can

- use ICF as an independent, neutral forum, to meet other stakeholders at eye level
- find allies
    - i.e., for standardization activities and project incubation
- find experts for the Multi-Standard to help them adopt it
- shape the Multi-Standard according to own needs regarding
    - extensions
    - further developments/concretization of existing parts
    - drive efficient, formal standardization

- be able to guarantee sustainability and accessibility for their Multi-Standard related project results
    - by bringing them into ICF and into the Database, where they are stored and publicly available
    - by advertising them
- be the first to know
    - current baseline or version of each part of the Multi-Standard
        - including maturity level of each part, thereby also allowing fast take-up
    - new extensions
    - standardization activities
- be able to focus on those parts of the specification that are actually of interest to them, while at the same time being aware of all Multi-Standard related activities

6. Outlook – What to Expect, the Way Forward

Recent developments in international standardization are very promising. ARTEMIS members are involved in many of them driving in the right direction as indicated by the ARTEMIS SRA priorities and research challenges addressed.

In terms of international standardization, awareness is rising particularly for the topic of Smart Manufacturing, Safety, Reliability and Cybersecurity in industrial automation and control, transportation, smart cities, buildings and associated targets, in Cloud Computing including particularly Cloud Security, and IoT as a complex, but moreover the overarching topic of standardization.

6.1 Machine – to –Machine Communication

ETSI is one of the European Standardization Organizations (ESOs) officially mandated by the European Commission to take care of M2M Communication Standards and Compliance Testing in this area. Important industries and research organizations worldwide (not just from Europe) are members of ETSI (in total 819, including industry, SMEs, operators, RTOs and Universities), working on communication standards, also in (cyber-) security and some industrial sectors. Many ARTEMIS partners are ETSI members, and a few persons are directly involved in ETSI. ETSI is fully financed by its members and projects (e.g. EC mandates), so all standards can be downloaded from the ETSI websites free of charge.

Machine-to-Machine Communication is a key issue today – it is of interest for ARTEMIS members not only to use existing standards but also to try to influence emerging standards.

In the case of M2M, ETSI is a key member of oneM2M, an alliance to develop global standards in the M2M and IoT field.

Formed in 2012 by eight of the world’s leading information and communications technology (ICT) standards development organizations, with more than 200 member companies, oneM2M provides a necessary framework for interoperability between the many M2M and IoT technologies being introduced. oneM2M is developing globally agreed, access-independent, end-to-end specifications for an M2M and IoT communications and management system that can be easily embedded within various hardware and software. oneM2M is experiencing major growth and progress towards connecting billions of devices in the field with the worldwide M2M application servers that power the IoT.
There are already many fragmented standardization activities around (I)IoT, (Industrial) Internet of Things, because IoT is not just one technology but a huge variety of technologies and technology areas, so IEC and ISO list a huge number of “related standards”.

Therefore there are many competing standardization activities in (I)IoT, such as (but not an exhaustive list)

- ISO/IEC JTC1, WG 10, Internet of Things; SWG 5
- ISO/IEC JTC1, WG 7, Sensor networks
- ISO, IEC: Many IoT relevant related standards in the communication area
- IEEE: many IoT related standards and standards projects: IEEE has an ongoing IoT Ecosystem study and the IEEE P2413 draft standard for an Architectural Framework for the Internet of Things
- ITU working group SG20 on “IoT and its applications, including smart cities and communities”,
- IPSO alliance where Internet technology IETF standards like 6LoWPAN and CoAP are developed and supported
- Particular protocols, e.g. the open AllJoyn protocol, now supported by the AllSeen Alliance (Qualcomm, Cisco, Linux, MicroSoft, …)
- Open Interconnect Consortium (Intel, Atmel, Dell, Samsung, WindRiver, …)

- Thread protocol (Google)
- Particular protocols for e.g. home devices etc.

6.2 Internet of Things

Without claiming being exhaustive, a list of IoT-related ISO Standards comprises:

- ISO/IEC CD 20924 - Information technology -- Internet of Things (IoT) -- Definition and vocabulary
- ISO/IEC WD 30141 Internet of Things Reference Architecture (IoT RA)
- ISO/IEC FDIS 29341-30-2 Information technology -- UPnP Device Architecture -- Part 30-2: IoT management and control device control protocol -- IoT management and control device
- ISO/IEC FDIS 29341-30-1 Information technology -- UPnP Device Architecture -- Part 30-1: IoT management and control device control protocol -- IoT management and control architecture overview
- ISO/IEC FDIS 29341-30-10: IoT management and control device control protocol -- Data store service
- ISO/IEC FDIS 29341-30-11: IoT management and control device control protocol -- IoT management and control data model service
- ISO/IEC FDIS 29341-30-12: IoT management and control device control protocol -- IoT management and control transport generic service
- ISO/IEC 29161 Information technology -- Data structure -- Unique identification for the Internet of Things
- ISO/IEC AWI 18574 – 18577: Internet of Things (IoT) in the supply chain

It is of interest that the ISO/IEC JTC1 (Joint Technical Committee 1) has just now decided to propose the foundation of a new Subcommittee ISO/IEC JTC1 SC41 “Internet of Things and related Technologies”. These efforts are being undertaken to avoid duplicating standards, overlapping standards and unclear, diverse terminology – the overall (international) standardization landscape is already very fragmented and diverse, so every attempt at cooperation is supported by research and company members. These activities to align standardization with the new technology and market developments (emerging and disruptive) can be only be judged positively, and hopefully will be successful in simplifying and aligning the diverse issues arising, particularly in disruptive cross-domain areas like IoT, Cloud Computing, Smart Anything, where there are always many existing but not holistic standards.

IoT is becoming a more and more intriguing issue. The recently founded AIOTI has worked in 11 Working Groups on Recommendations for an IoT Research Programme for the European Commission, who issued the first IoT Calls in 2016 (Large Scale Pilots). WG 3 on “Standardization” has issued three documents:

1. IoT LSP Standard Framework Concepts (LSP means “Large Scale Pilots”, an EC Large Projects’ Initiative)
2. IoT High Level Architecture
3. Semantic Interoperability

Particularly in 3.), tools are addressed, and more precisely the need for appropriate tools and semantic interoperability. In the IoT environment, the landscape is even more fragmented than it was 10 years ago in the embedded system environment, so there may be another option here for the application of the IOS – ICF ideas in this fast evolving field.

It should be mentioned that the European IoT Community in Research founded AIOTI (Alliance for Internet of Things Innovation) which this year became an Association as a first step towards a cPPP (contractual Public-Private Partnership) to be able to influence future European Research Programmes in IoT. AIOTI currently has 13 Working Groups.

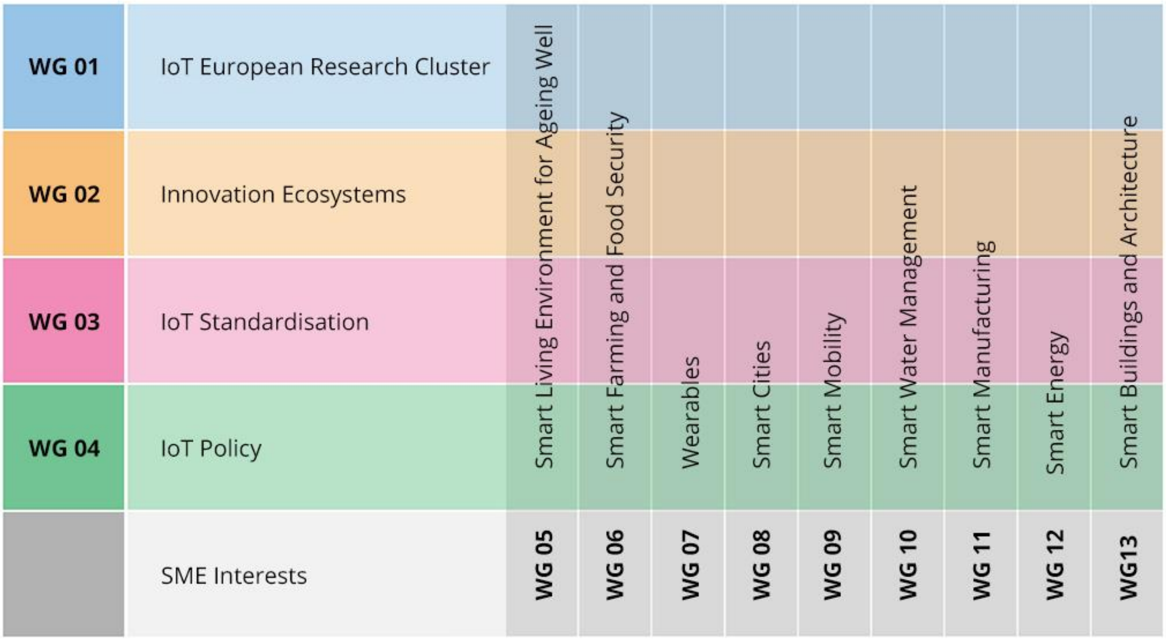


Figure 9: Structure of AIOTI Working Groups

As can be seen in Figure 9, most domain-related Working Groups are of interest for ARTEMIS. Therefore, ARTEMIS-IA has become member of AIOTI whose members already include several ARTEMIS-IA members. The goal is to join forces, since IoT is a major challenge for CPS in research and development, as outlined in the ARTEMIS SRA 2016. ARTEMIS-IA has expressed its intention to become member of WG3, standardization, which provides a very good fit with the overall strategy and the ARTEMIS Strategic Agenda for Standardization. AIOTI itself is not a standardization organization but it has close cooperation with international standardization organizations, including ETSI, ITU-T, CEN/ISO, CENELEC/IEC, IETF, IEEE, W3C, OASIS, oneM2M and OGC (Open Geospatial Consortium).

6.3 Standards in the Cloud

To facilitate Cloud Computing and Communication in a secure and reliable manner, also in the case of safety-relevant, safety-critical or highly availability-driven applications (e.g. smart energy, smart mobility, smart cities, smart health, etc.), a Joint Working Group of ISO and IEC was already created some time ago. The Joint Technical Committee of ISO and IEC, JTC1, Subcommittee 30 (“Distributed Application Platforms and Services”) started foundational work on the Cloud Computing Standards:

- ISO IEC 17788 – Cloud computing – overview and vocabulary
- ISO/IEC 17789 - Cloud computing - Reference architecture,

These standards are recommended and supported by ITU-T, the International Telecommunication Union. In the meantime, related standards like ISO/IEC 19831:2015 have been published (“Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based protocol”).

New standardization projects are another window of opportunity for ARTEMIS/ECSEL project partners, particularly when not just file services but more complex digital industrial services should be addressed in future:

- Service level agreements,
- Interoperability and portability,
- Data and their flow across devices and cloud services,

- Security issues

This covers the main topics of interest of the work done in ARTEMIS/ECSEL for the Platform and Framework activities. Involvement in these groups is encouraged, but this is a mid-term goal because it takes several years and needs consensus in sometimes diverse groups and group interests.

Besides ISO/IEC, a number of standards and specifications from IETF, W3C and OASIS are relevant in the area of Cloud and Web Services. For addressing many common security requirements standardized protocols and specifications can be used, like SSL/TLS (RFC 5246), IPsec (RFC 4301), XML Signature and XML Encryption, SAML, XACML and others (see [2], Chapter 10 of ARROWHEAD Book). The IPSO Alliance and IETF are examples of ARROWHEAD solutions finding their way into standards. Standardization as an ARTEMIS SRA Priority has already been successful in many cases, and only a few recent examples have been mentioned here.

6.4 Tool Interoperability - IOS

In the final phase of EMC² and CP-SETIS, the most important achievement towards a sustainable future development and maintenance of IOS was the agreement with ARTEMIS-IA to host and support the IOS Database management and maintenance for the first three years. ARTEMIS-IA and the ARTEMIS-IA Standardization Working Group as an existing structure of ARTEMIS-IA will host the ICF (IOS Coordination Forum) as WG-subgroup, and basic funding for the initial phase is agreed. The plan is to establish a contract with a small professional company which is knowledgeable in this area, and to set up a scientific and technical manager.The joint work with the other projects was very fruitful and the IOS Coordination Forum is implemented and was officially kicked-off in May, 2017 (collocated with the Digital Innovation Forum 2017, in Amsterdam). The ICF Forum is open to all interested stakeholder (e.g. the ECLIPSE group showed interest at DIF 2017). The initial members will be from CP-SETIS, EMC² and the other projects involved in the development of the IOS concept. Thus, successful further development and maintenance work can start just now!

6.5 IEC 61508 Maintenance Cycle – starting for all parts 2017

IEC MT 61508-3, Software part of the generic functional safety standard, has started preliminary work already two years ago, because the large number of new software paradigms and issues applied already partially in industry, without appropriate guidance in the standard. This was already explained in chapter 4.2. During this work, it became very clear that many of the issues started to consider or reconsider concern the system and hardware parts IEC 61508-1 and -2 as well. The last meeting of MT 61508-3 had a meeting with the convenor of MT 61508-1-2, which had not officially started maintenance activities until now. The following issues were presented by members of MT 61508-3 and in the end agreed to be brought forward to MT 61508-1-2 in the next meeting of this group June 13 – 14, 2017, at BSI in London (in liaison of both groups):

- Proven in Use
- (Cyber) security and safety*
- Tool Qualification (including tool chain issues and interoperability)*
- SW/HW Interface
- Systematic Capability
- Vulnerabilities from Concurrent and Multi-core Architecture*
- Regression testing
- Architecture

- Diagnostics*
- Safety Cases/Arguments*
- Basing requirements on Consequence only
- Independence of Assessment and Properties
- Formal Methods
- Terminology
- Cross references (standards and compliance between them)*

Those items marked * are of particular interest and input triggered by EMC². This list shows that there is now a long way to go and a lot of standardization involvement of some partners required to successfully implement results of EMC² in this generic functional safety standard, Ed. 3.0.

6.6 Concluding Statement

This is a unique “Window of Opportunity” of the EMC² project to achieve sustainable results in standardization. This concerns IEC MT 61508, ISO/SAE JWG1 “Road vehicles – Cybersecurity Engineering” and ISO TC22 SC32 WG8, SotiF, Safety of the intended Functionality. Additionally, the Austrian National Mirror Committee sent a proposal as comment to ISO TC299, Robotics, in the voting process on reviewing ISO 10218 to start maintenance of ISO 10218, Safety requirements of industrial robots, under particular consideration of cybersecurity aspects, as in the other standardization groups mentioned before. Although this is still not decided yet, a first step is undertaken in the standardization process towards future developments in the direction as indicated by EMC² results!

7. References

[AS-NZS] AS/NZS (Australian/New Zealand Standard) 4360:2004 Risk Management

[Brab 01]J. Braband, “Towards an IT Security Framework for Railway Automation,” presented at the Embedded Real Time Software and Systems, Toulouse, 2014.

[CP-SETIS 01] E. Schoitsch, J. Niehaus, “Strategic Agenda on Standardization for Cyber-Physical Systems”, CP-SETIS/ARTEMIS-IA, 2017, ISBN 978-90-817213-3-2, funded by the EC,H2020 Innovation Action, grant agreement 645149.

[ECSS 01] ECSS-E-ST-40 ECSS Space Engineering Standard, Software Engineering

[ECSS 02] ECSS-Q-ST-80 ECSS Product Assurance Standard, Software Product Assurance

[IEC 01] IEC 31010: Risk management — Risk assessment techniques, 2009.

[IEC 02] IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), IEC, 2006.

[IEC 03] IEC 61025: Fault Tree Analysis, 2007.

[IEC 04] IEC 61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, Ed. 2.0, 2010

[IEC 05] IEC 61882: Hazard and operability studies (HAZOP studies), IEC, 2001.

[IEC 06] IEC Smart Grid Standardization Roadmap, 2010.

[IEC 07] IEC 62443, Industrial communication networks - Network and system security - Security for industrial automation and control systems.

[IEEE 01] IEEE Std 1012 - Standard for System and Software Verification and Validation, 2004

[IEEE 02] IEEE Standard Glossary of Software Engineering Terminology, 1990.

[ISO 01] ISO, 26262 Road Vehicles - Functional Safety, 2011.

[ISO 02] ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation

[ISO 03] ISO/IEC TR 19791: Information technology -- Security techniques -- Security assessment of operational systems, 2010

[IT-BLP] IT Baseline Protection Manual (German: IT Grundschutz-Handbuch), German Federal Office for Security in Information Technology (BSI), since 2005 “Baseline Protection Catalogues”

[MSDL] Microsoft Security Development Lifecycle http://www.microsoft.com/security/

[RTCA 01] DO-178C/EUROCAE ED-12C Software Consideration in Airborne Systems and Equipment Certification, 2012.

[RTCA 02] DO 178C Technology Supplements:

- DO-330 "Software Tool Qualification Considerations" - clarifying software tools and avionics tool qualification
- DO-331 "Model-Based Development and Verification Supplement to DO-178C and DO-278" - addressing Model-Based Development (MBD) and verification and the ability to use modeling techniques to improve development and verification while avoiding pitfalls inherent in some modeling methods
- DO-332 "Object-Oriented Technology and Related Techniques Supplement to DO-178C and DO-278A" - addressing object-oriented software and the conditions under which it can be used

- DO-333 "Formal Methods Supplement to DO-178C and DO-278A" - addressing formal methods to complement (but not replace) testing

[RTCA 03] DO-254/ EUROCAE ED-80 “Design Assurance Guidance for Airborne Electronic Hardware”.

[RTCA 04] DO-278 / EUROCAE ED-109 “Guidelines for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance”, is the ground based complement to the DO-178B airborne standard.

[RTCA 05] DO-178B / EUROCAE ED-12B “Software Considerations in Airborne Systems and Equipment Certification. Requirements and Technical Concepts for Aviation”

[SAE 01]ARP-4761 System Safety Assessment, 1996.

[Sch 01] E. Schoitsch, Ch. Schmittner, Z. Ma and T. Gruber: *The Need for Safety & Cyber-Security Co-engineering and Standardization for Highly Automated Automotive Vehicles*, AMAA 2015 (Advanced Microsystems for Automotive Applications), Springer Proceedings, Berlin July 7-8, 2015.