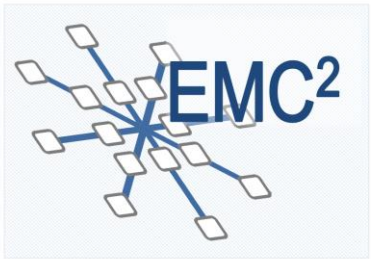

Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments

Project Acronym:

EMC²

Grant agreement no: 621429

Deliverable no. and title	**D13.25 Intermediate Standardization Report**	
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	2016-04-23	
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
02A	AVL	Christian El Salloum, Eric Armengaud	Part on IOS (Interoperability Specification)

Document history

Version	Date	Author name	Reason
0.1	2016-03-31	Erwin Schoitsch, Eric Armengaud	Set-up document
0.2	2016-04-01	Erwin Schoitsch	Update of Summary, Introduction, Standardization areas and description of progress in IEC TC65 Ad-Hoc Groups, ISO 26262, IEC 61508 and Railways
0.3	2016-04-14	Eric Armengaud, Christian el Salloum	Interoperability Specifications
0.95	2016-04-15	Petr Böhm, Christoph Schmittner	Review
1.0	2016-04-19	Erwin Schoitsch, Christian El Salloum, Eric Armengaud	Final Version
	2016-04-23	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 to be reviewed, as part of market impact. Further on, standardization is considered by the EC as a very important part of exploitation of results of research projects although it is a medium to long term issue compared to the duration of a research project (normally three years), whereas standardization schedules cover 5 years and more, and an immediate uptake requires a "window of opportunity", i.e. 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 may take five years or more.

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 labs work packages. This deliverable is the report on progress in standardization since edition of the two initial 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 – Intermediate report about relevant standardization activities of the second year, particularly in the area of
    - Combined approaches to security issues in safety critical systems (IEC, ISO); work started 2014 and 2015; this 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.
    - 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). In the meantime, it turned out that it 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 and an ICF – IOS Coordination Forum, work that is planned and done by CP-SETIS partners which are partners in several ARTEMIS projects which are devoted to IOS contributions (CRYSTAL, EMC² and to a certain degree ARROWHEAD), and members of the ARTEMIS Standardization Working Group. In EMC², this is particularly part of WP5, a first overview was provided in D5.23 – Interoperability and Standardization, State-of-Art analysis.
    - Domain specific standardization activities of the work packages will be covered in the upcoming annual reports and specific WP-deliverables.

Table of contents

List of Figures

1. Introduction

1.1 Objective and scope of the document

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 (2) on 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 D13.25.

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

1.2 Structure of the document

The document consists of five 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

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 in the automotive domain, where just now **ISO/CD 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):

- **IEC TC65 AHG1: "Framework towards coordinating safety, security (in industrial automation)**
- **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.

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, so that 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. So 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 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 current 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.

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 life time 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".

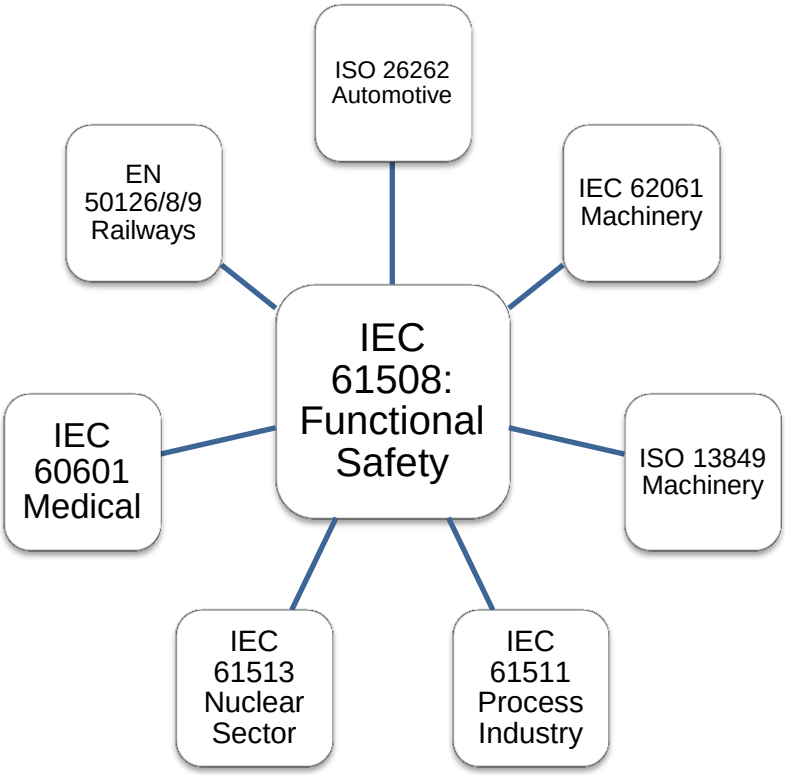

Figure 1: Functional Safety Standards – Security Awareness needed to be included as issue (WP6, WP13.5)

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, APIs and 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 that cannot be 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 will be 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).

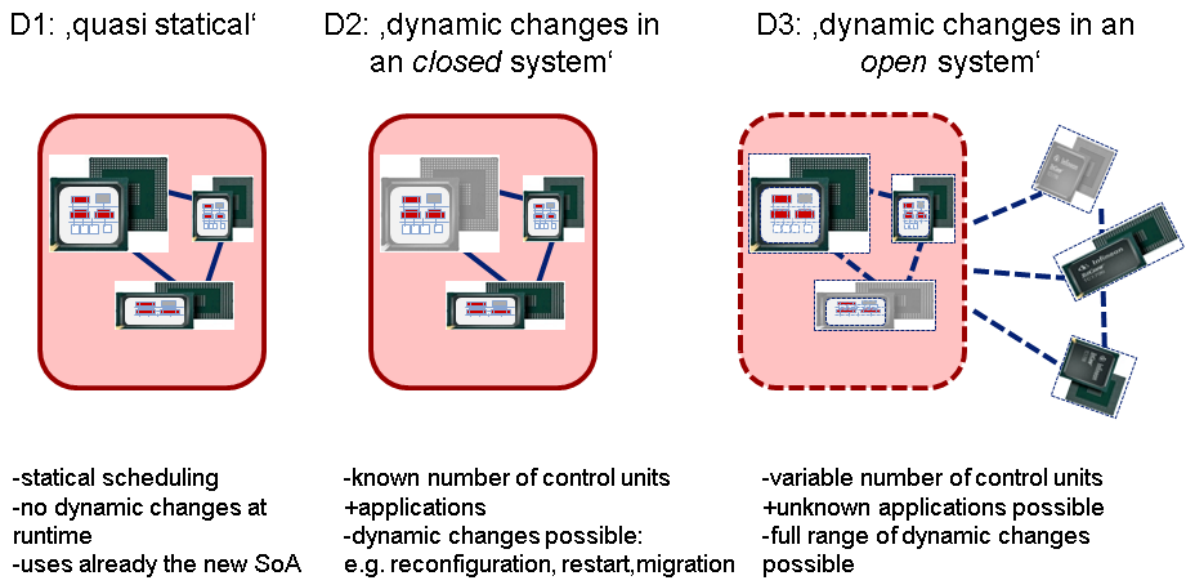

Figure 2: EMC² - from closed to open systems

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 to be considered in system engineering and safety analysis.

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

IEC 61508 Ed. 2.0 [IEC 04] finished 2010, took as first functional safety standard into account that security may impact 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.

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.

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. In particular:*

……

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

In Annex D: ….

m) 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.

In Annex F:

s) 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 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 is 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."

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 mean 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, 2016, in Dalian, China, and continues its work via telephone conferences and internet/emails. The next Face-to-Face meeting will be in Vienna at AIT, June 1-3, 2016.

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;*
> *- to recognize the acknowledged references,*
> *- to identify gaps between the models and the needs of the industry.*

This is relevant not only for top-level considerations in EMC² but even more for related ARTEMIS projects, e.g. ARROWHEAD. AIT will take part in this AHG3, the Kick-off is in Paris, April 4 – 6, 2016.

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 a more integrated approach was preferred by the proposer (AIT, Austria). 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 should be 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 2015 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 and Part 4 (Product development at the system 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.
- 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.

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

4.5 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.

Security issues and unauthorized access issues are not addressed in the current version of EN 50126-1. It states

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

Nevertheless, similar as later 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. But 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. Therefore 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.

5. Interoperability Specifications

A second important activity is related to interoperability specifications. This work was started in the ARTEMIS project CESAR, then handed over to further European projects such as MBAT, nSafeCer and CRYSTAL. 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** *(Towards Cyber-Physical Systems Engineering Tools Interoperability Standards***)**. The CP-SETIS proposal is coordinated by SafeTrans, and the initiative has been driven by 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 stared in March 2015.

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/

- 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.

[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/

- 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.

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.

6. 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.

[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*, paper accepted at AMAA 2015 (Advanced Microsystems for Automotive Applications), Springer Proceedings, Berlin July 7-8, 2015.