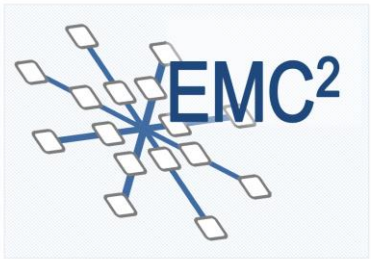


Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments

Project Acronym:

EMC²

Grant agreement no: 621429

Deliverable no. and title	**D6.2 Requirements elicitation**	
Work package	WP6	System qualification and certification
Task / Use Case	T6.1	Certification and Qualification challenges of EMC²-Systems
Lead contractor	Infineon Technologies AG Dr. Werner Weber, mailto:werner.weber@infineon.com	
Deliverable responsible	AVL List GmbH Dr. Eric Armengaud, mailto: eric.armengaud@avl.com	
Version number	v1.0	
Date	01/12/2014	
Status	Final	
Dissemination level	Public (PU)	

Authors

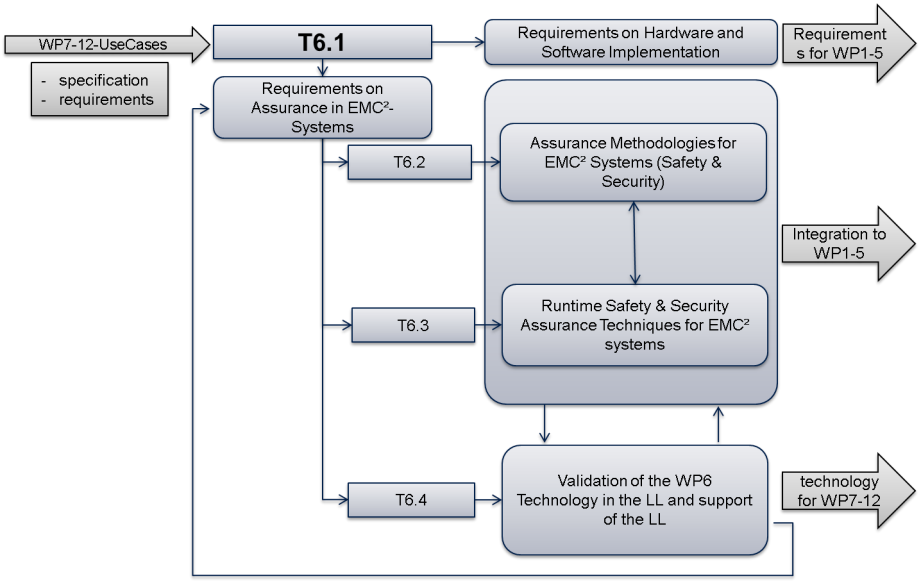
Partici-pant no.	Part. short name	Author name	Chapter(s)
01O	IESE	Daniel Schneider	3.2, 3.3, 4.4
01ZI	TUKL	Max Steiner	4.7
02A	AVL	Eric Armengaud	all
02C	IFAT	Stefan Berger	5
02G	AIT	Christoph Schmittner Erwin Schoitsch Thomas Gruber	2.4, 2.5, 2.6, 3.1, 4.7
04B	Freescale	David Baca	3.2, 4.2
07F	RCF	Françoise Crestey	2.2, 2.3, 3.2, 4.5
09B	UTRC	Stylianos Basagiannis	4.10
11A	Alenia	Renato Campaniello	4.1
15P	Telvent	Benito Caracuel	3, 4.3
18B	IFXUK	Fabio Bruno	3.1, 4.1

Document History

Version	Date	Author name	Reason
v0.1	16/06/2014	Eric Armengaud	Set-up document
v0.2	07/08/2014	Fabio Bruno	IFXUK expected contribution
v0.3	11/08/2014	Fabio Bruno	Split chapter 3.1 in requirements (3.1) and proposed innovations (4.1)
v0.4	21/08/2014	David Baca	High level requirement from Freescale.
v0.5	03/09/2014	Eric Armengaud	Merge from the different partners - Merge with template (A. Hoess) - Input from partner Telvent - Integration from HL requirements
v0.6	26/09/2014	Eric Armengaud	Following inputs integrated - Francoise Crestey (Rockwell Collins France) - Renato Campaniello (Alenia)
v0.7	10/10/2014	Daniel Schneider	Input FhG IESE
v0.8	15/10/2014	David Baca	Modified the text in proposed innovation
v0.9	30/10/2014	Max Steiner	Added proposed innovation, reformatted references
v0.10	03/11/2014	Françoise Crestey	Added overview of Avionics domain. Merge of RCF and Alenia parts for Avionics domain. Addition of detailed technical requirements related to safety/certification and security. Addition of description of involvement of RCF in projects, WGs dealing with multicore use.
v0.11	11/11/2014	Eric Armengaud	Integration of different partners contributions, consolidation of main document
v0.12	12/11/2014	Eric Armengaud	Input from UTRC (Stylianos Basagiannis) integrated
v0.99	27/11/2014	Eric Armengaud	All review comments integrated, release candidate
v1.0	01/12/2014	Eric Armengaud	Released
	01/12/2014	Alfred Hoess	Final editing and submission

Publishable Executive Summary

Scope of this document is to perform requirement elicitation for the WP6 System qualification and certification. Inputs for this task rely on (a) the deliverable D6.1 State of the art for System Qualification and Certification, and (b) on the high-level requirements and business needs coming from the living labs. Figure 1 provides an overview of the WP6 organization. Target of this document is to support T6.1 (a) by the structuring of the high level requirements from the living labs and (b) by the identification and further mapping of the WP6 partners' contributions in this context.



This deliverable provides a mapping between the user needs (coming from the living labs), the requirements from the different relevant standards, and the intended contributions of the EMC² WP6 partners. A review of the safety and security standards from different domains has been provided in Section 2. This has led to the identification of 4 high level requirements for WP6, which have been further mapped to the user needs in Section 3. After that, the contributions of the partners have been identified and finally mapped to the WP6 high level requirement in Table 1. This last mapping shall support the living labs to identify the technologies and partners relevant to their needs.

The four WP6 high level requirements are the following:

HL-REQ-WP06-001: Safety and security co-engineering framework
Investigate, develop, and validate methodologies and technical solutions for a holistic approach to safety and security, throughout system lifetime, while taking into account the mission-critical and real-time requirements. Following standards shall be supported: ISO26262, DO178C, IEC61508, IEC 15408, IEC 62443

HL-REQ-WP06-002: Trust assurance case compilation
Capability to compile seamless argumentation why the developed system or product is sufficiently safe for its intended application. This argumentation should serve as documentation (red story line) for certification activities. Following standards shall be supported: ISO26262, DO178C and IEC61508.

HL-REQ-WP06-003: Modularization of the safety and security co-engineering framework for use in distributed environments at design time
Provide import / export capabilities for the safety / security co-engineering framework at dedicated development milestones, such that specific activities performed by external teams can be integrated into the overall framework. Following standards shall be supported: ISO26262, DO178C, IEC61508.

HL-REQ-WP06-004 Mechanisms for runtime certification of cyber-physical systems
Provide methods for the runtime evaluation of trust certificates. This implies the introduction of suitable means to represent the trust certificates within the systems, so that the systems can utilize the certificates autonomously to reason about the current trust properties of the system (of systems). Moreover, systems must be augmented with corresponding evaluation mechanisms.

Table of contents

1. Introduction....7
1.1 Objective and scope of the document....7
1.2 Structure of the deliverable report....7
2. Overview of the safety and the security engineering domains....8
2.1 Automotive domain....8
2.2 Avionics domain....9
2.3 Railway Domain....11
2.4 Security Engineering according to Common Criteria (ISO/IEC 15408)....14
2.5 Safety Engineering according to the IEC 61508....15
3. Requirements and business needs related to WP6....17
3.1 High level requirements from WP6....17
3.2 Mapping with the high level requirements and business needs from the living labs....19
4. Proposed innovations....23
4.1 Proposed Innovations, high level tasks description – Alenia....23
4.2 Proposed Innovations, high level tasks description – AIT....23
4.3 Proposed Innovations, high level tasks description – AVL....23
4.4 Proposed Innovations, high level tasks description – FhG IESE....24
4.5 Proposed Innovations, high level tasks description – Freescale....24
4.6 Proposed Innovations, high level tasks description - IFX-UK / IFAT....25
4.7 Proposed Innovations, high level tasks description - Rockwell Collins France....26
4.8 Proposed Innovations, high level tasks description - TELVENT....26
4.9 Proposed Innovations, high level tasks description – TUKL....27
4.10 Proposed Innovations, high level tasks description – UTRC....27
5. Conclusions....28
6. References....29

List of figures

Figure 1: WP6 organisation 7
Figure 2: Overview of the different safety disciplines on the example of the ISO26262 8
Figure 3: Relationship between the different safety standards in the avionics domain 9
Figure 4: Security Development as Part of Aircraft Certification Process 10
Figure 5: Illustrative SW route map in EN 50128 12
Figure 6: Structure of a safety case according to EN 50129 13
Figure 7: Overall framework of the IEC 61508 series [14] 15

List of tables

Table 1: Mapping between partner contributions and WP6 HL requirements 28

1. Introduction

1.1 Objective and scope of the document

Scope of this document is to perform requirement elicitation for the WP6 System qualification and certification. Inputs for this task rely on (a) the deliverable D6.1 State of the art for System Qualification and Certification, and (b) on the high-level requirements and business needs coming from the living labs. Figure 1 provides an overview of the WP6 organization. Target of this document is to support T6.1 (a) by the structuring of the high level requirements from the living labs and (b) by the identification and further mapping of the WP6 partners' contributions in this context.

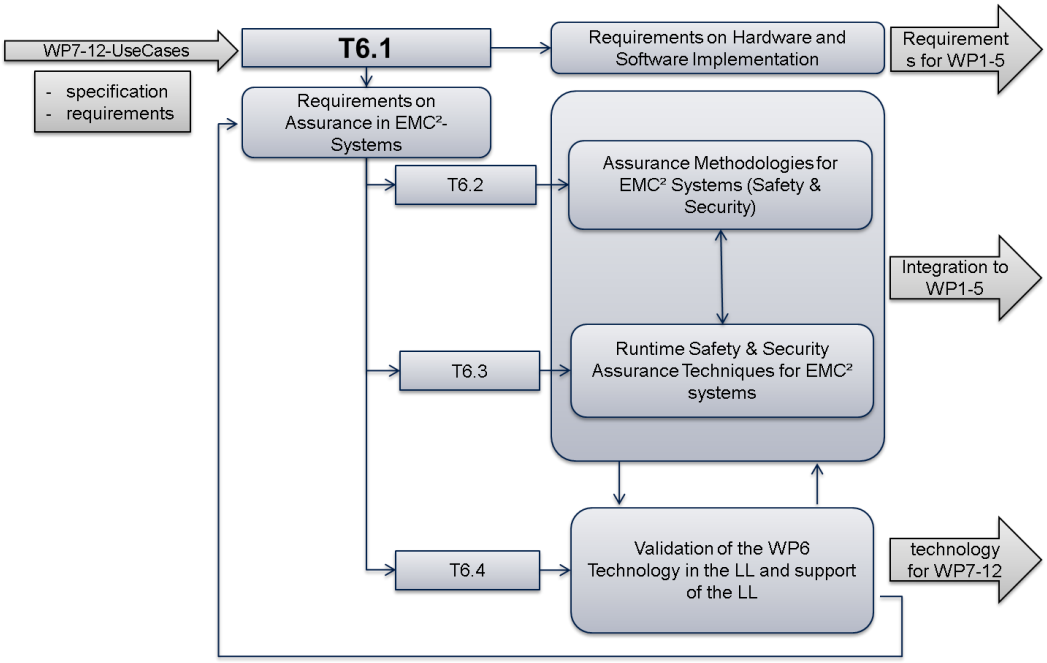


Figure 1: WP6 organisation

1.2 Structure of the deliverable report

The document is organized as follow: Section 2 provides an overview of the main safety and security domains / categories from the different safety standards. Section 3 summarizes the high-level requirements and business needs from the living labs, while Section 4 lists the proposed innovations from the WP6 consortium. Finally, Section 5 performs the mapping between living labs requirements and proposed innovations, and Section 6 lists the references.

Note that the following EMC² deliverables are related to this report:

- *D6.1 State of the art for System Qualification and Certification*: This deliverable shall provide an overview of the state of the art for system qualification and certification (both during development and during runtime)

- *D6.3 Preliminary definition of the runtime certificate approach*: This deliverable shall provide first direction for runtime certification, based on this report and on the deliverable D6.2

2. Overview of the safety and the security engineering domains

2.1 Automotive domain

Safety standards such as ISO 26262 [1] for E/E/EP systems for road vehicles have been established to provide guidance during the development of safety-critical systems. They provide a well-defined safety lifecycle based on hazard identification and mitigation, and they define a long list of activities to be performed and work-products to be generated over the entire lifecycle.

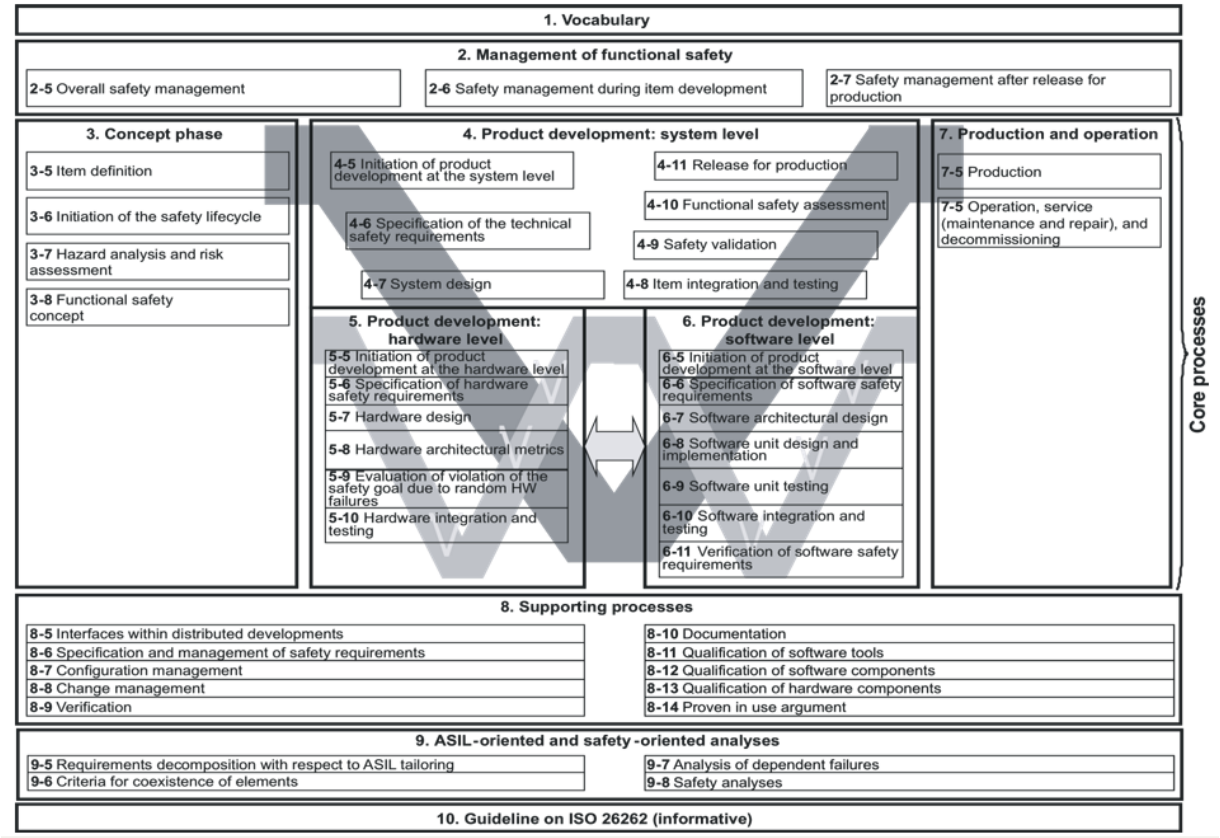


Figure 2: Overview of the different safety disciplines on the example of the ISO26262

One major challenge while dealing with "safety" is the large number of skills that are addressed. In the following, a definition is proposed:

- ***System safety engineering***: activities related to the establishment and consolidation of system concept and system specification. It includes the risks identification (e.g., Hazard Analysis and Risk assessment, System FMEA, FTA). This activity is related to Systems Engineering.

- ***SW safety engineering***: activities related to the specification, analysis, implementation and verification of the SW safety functionalities. This activity is related to Software Engineering

- ***HW safety engineering***: activities related to the specification, analysis, implementation and verification of the HW safety functionalities. This activity is related to Hardware Engineering.

- ***Integration safety engineering***: activities related to the integration, test and validation of the system, assuming the SW and HW components have been verified previously. This activity is related to Integration Engineering

- ***Production safety engineering***: activities related to the preparation of the production with respect to the safety aspects .Especially, the safety related requirements for the production shall be identified and integrated during product development, and the safety know-how generated during product development and which is relevant for production shall be provided, e.g., as guideline.

- ***Quality management***: activities related to the establishment and maintenance of the quality over the project. This comprises processes such as change management, documentation, requirement engineering. This activity shall be consistent over the different skills, teams, organizations working in the project

- ***Safety management***: activities related to the coordination of the safety activities, management of skills and resources, and finally generation of safety assurance case (communicating a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context[1])

2.2 Avionics domain

Methodologies for safety assessment processes are outlined in SAE document ARP4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" [2]. The ARP4754A [3] addresses the development cycle for aircraft and systems that implement aircraft functions and have failure modes with the potential to affect the safety of the aircraft. This includes requirements and verification of the design implementation for certification and product assurance.

The guidelines are directed toward systems that have failure modes with the potential to affect the safety of the aircraft. Typically, these systems involve significant interactions with other systems in a larger integrated environment. These systems require added design discipline and development structure to ensure that safety and operational requirements can be fully realized and substantiated. A top down iterative approach from aircraft level downwards is key to initiating the system development and safety assessment processes.

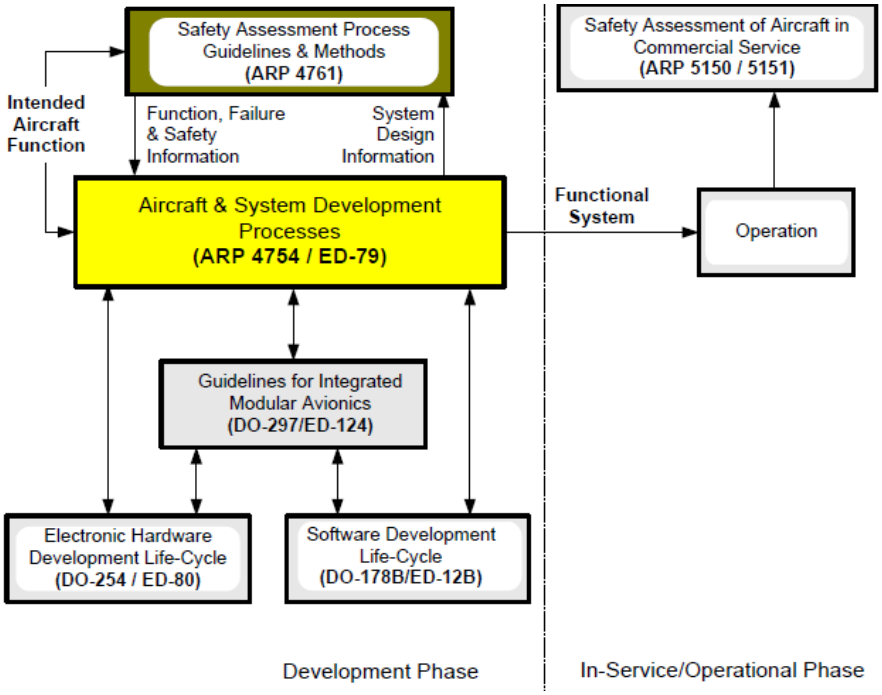


Figure 3: Relationship between the different safety standards in the avionics domain

[1] T. Kelly and R. Weaver, "The goal structuring notation a safety argument notation," in Proc. of Dependable Systems and Networks 2004 Workshop on Assurance Cases, 2004.

More detailed coverage of the software aspects of development are found in RTCA document DO-178C, "Software Considerations in Airborne Systems and Equipment Certification" [4]. Coverage of electronic hardware aspects of development are found in RTCA document DO-254/EUROCAE ED-80, "Design Assurance Guidance for Airborne Electronic Hardware" [5]. Design guidance and certification considerations for integrated modular avionics are found in appropriate RTCA/EUROCAE document DO-297/ED-124 [6].

Details for in-service safety assessment are found in ARP5150, "Safety Assessment of Transport Airplanes In Commercial Service" [7] and ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft In Commercial Service" [8]. Post-certification activities (modification to a certificated product) are covered in section 6 of ARP4754A.

In avionics domain, a specific security development process, as defined in ED-202A "Airworthiness Security Process Specification" [9] is applied, in correlation with system development / safety assessment process, as defined in ED-79A "Guidelines for development of civil aircraft and systems". Following figure illustrates the ED-79A system/aircraft certification process with its interactions with ED-202A security development process.

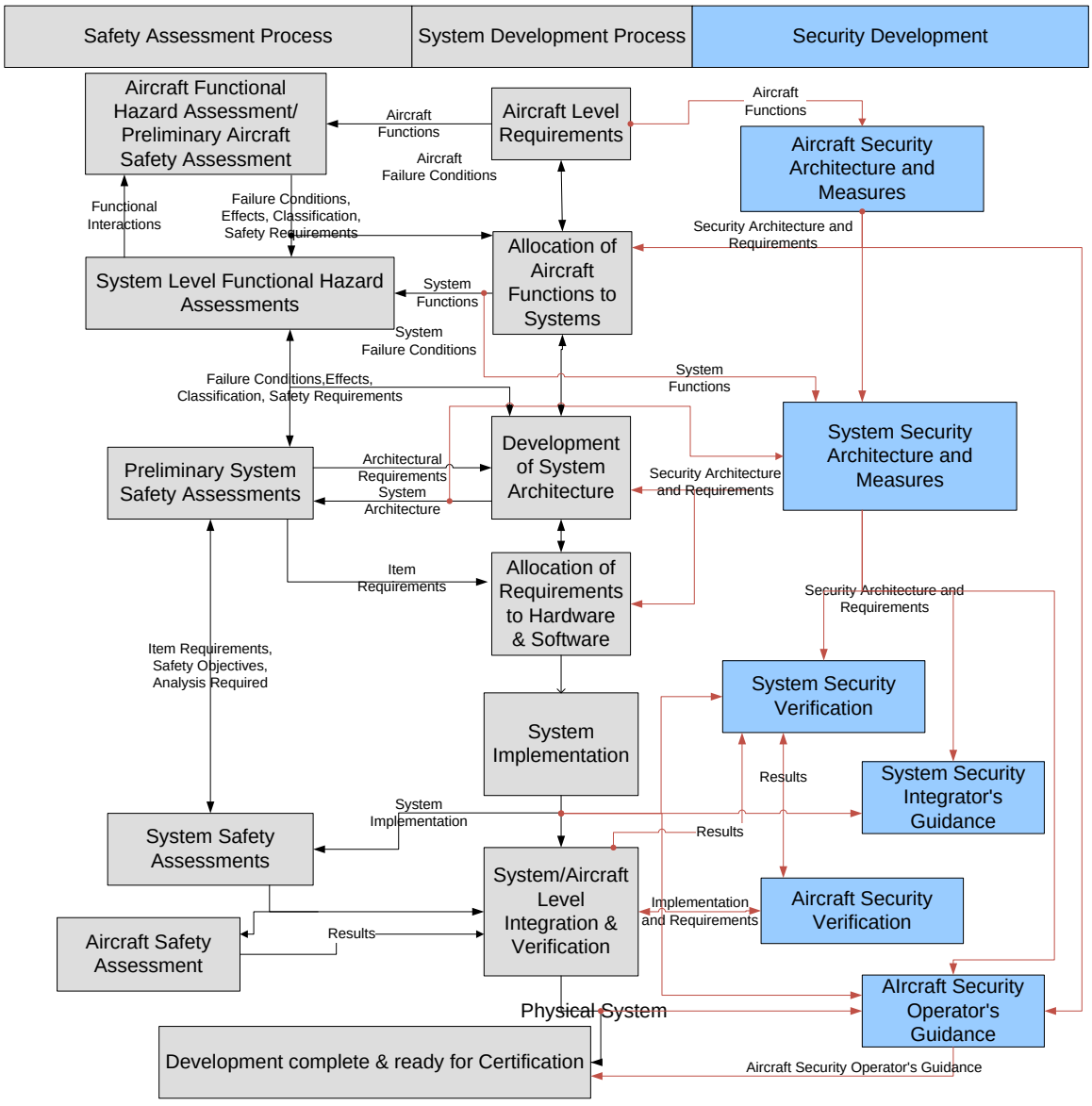


Figure 4: Security Development as Part of Aircraft Certification Process

Regarding ED-202A, the guidance provided by this document and its companion documents constitutes an acceptable means to address the increasing potential for intentional unauthorized electronic interaction with aircraft information systems.

The ED-202A provides guidance by defining activities for supplementing the aircraft development and certification process to demonstrate that the effects on the safety of the aircraft of such unlawful interferences are confined within acceptable levels. As intentional unauthorized electronic interaction includes intentional origin, this document covers some aspects of electronic sabotage.

2.3 Railway Domain

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

- EN 50126 Railway Applications – the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) [10]:
  - 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, signalling and processing systems – Software for railway control and protection systems (IEC June 2011) [11]
- EN 50129 Railway applications - Communication, signalling and processing systems – Safety related electronic systems for signaling (IEC 2003, corrigenda 2010). [12]

The standard EN 50126 covers the railway system in total and addresses risk analysis, reliability and safety issues. The standards EN 50128 and EN 50129 are more specific. EN 50129 describes in detail the contents of a safety case. EN 50128 covers all critical software-related issues in a satisfactory and comprehensive manner, providing very detailed guidance what to do in each of the Safety Life Cycle phases, listing requirements, documents etc. (see Figure 5) It follows the SIL (safety integrity level) concept of IEC 61508, but starting with SIL 0, which is rather software quality management according to EN ISO 9001.

In EN 50128 Annex A there are very detailed normative clauses and tables, particularly

- Table A1: Lifecycle issues and documentation (clause 5.3)
- Table A2: Software Requirements Specification (clause 7.2)
- Table A3: Software Architecture (clause 7.3)
- ….
- Table A23: Object Oriented Detailed Design

Annex B (normative) provides key software roles and responsibilities.
Annex C is informative providing a useful documents control summary.
Annex D (informative) integrates a bibliography of techniques into the standard (partially taken and updated from IEC 61508, Part 7).

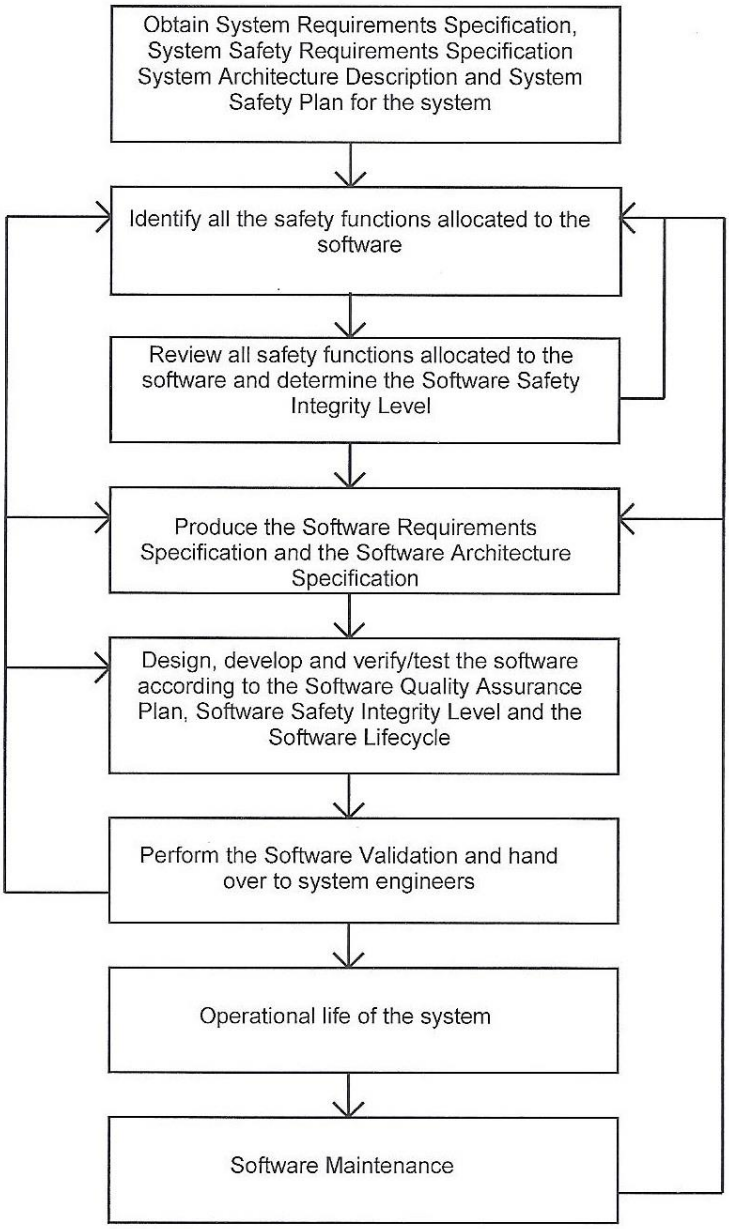


Figure 5: Illustrative SW route map in EN 50128

EN 50129 defines the requirements for the Safety Case. It provides details for safety related HW and SW for railway control and protection systems and for the overall system. The structure of such a Safety Case is shown in Figure 6. This detailed description of how to achieve safety approval with the Safety Case makes this standard different from IEC 61508 which does not require a safety case. This approach supports very effectively the developer as well as the assessor/licensing authority. Additionally, EN 50129 gives a clear description of the different levels of safety cases that could be developed:

- Generic product safety case (independent of application): A generic product can be re-used for different independent applications. It is one of the building blocks for the applications.
- Generic application safety case: A generic application can be re-used for a class/type of application with common functions. It is configurable, but it is not particularly configured.
- Specific application safety case: It is used for only one particular installation.

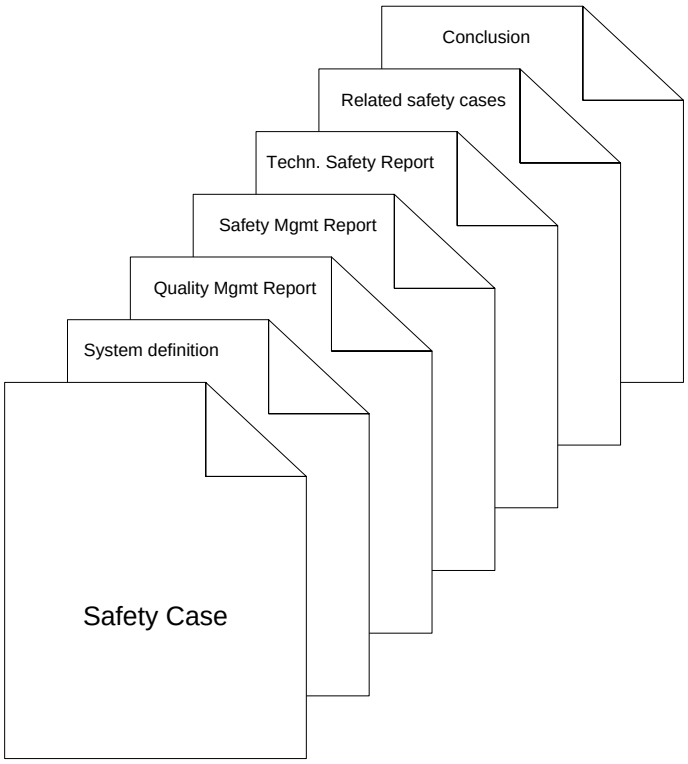


Figure 6: Structure of a safety case according to EN 50129

Security issues like 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".

Similar to IEC 61508 Ed. 2 (2010), where the relation of security to safety was defined later, we find in EN 50129:

- 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 networks and wireless communication even to transmit critical information and data, system security issues can impact safety severely and have to be taken into account in future. An adaptation of the standard will be necessary, at least similar as IEC 61508 has evolved towards IEC 61508 Ed 2 (2010).

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 risen 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[2]) 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 most of the 41 requirements for security level 1 (SL 1) of IEC 62443 ("Protection against casual or co-incidental violation") are whether explicitly covered by requirements of EN 50129 or usually fulfilled in the context of EN50129-based development, and 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).

2.4 Security Engineering according to Common Criteria (ISO/IEC 15408)

Common Criteria (ISO/IEC 15408) [13] focus mainly on the evaluation of information security. It defines the process for the specification, implementation, and evaluation of security-critical, high-assurance systems. Part 1 presents the general model for the evaluation of IT security, Part 2 describes a set of security functional components for common functional security requirements, and Part 3 defines assurance categories and levels and matches them to the Evaluation Assurance Levels (EALs). The general approach for evaluating the security of a system is divided in two abstraction levels: Protection Profile (PP) as an implementation independent specification of security needs for a type of product; Security Target (ST) as an implementation specific security concept.

Protection Profile: The implementation independent Protection Profile includes a functional description of the system, assumptions about potential operation environments and threats, the security objectives which solves the security problem and functional security requirements which specifies and formalizes the security objectives. The security assurance requirements specify how the Target of evaluation should be evaluated.

Security Target: The Security Target is an implementation specific security concept. A Security Target can claim compliance with a Protection Profile. The Protection Profile then defines the minimal level of security for the Security Target. A Security Target that claims compliance with a Protection Profile needs to deliver at least the level of security specified in the Protection Profile. It can deliver a higher level of security, e.g. a better encryption. A Security Target specification includes at least a description of the system (target of evaluation), conformance claims to any Protection Profiles, a definition of the security problems, assumption about the operational environment, security objectives which solve the security problems, security requirement which implement the security objectives and the security assurance requirements.

Part 2 of ISO 15408 focuses on functional security components and a description of the Target of Evaluation (TOE) definition. A TOE is the product or system under evaluation. The presented concepts can be used in Protection Profiles and Security Targets for functional security requirements. While the list of functional security components is not conclusive, it represents a state of the art baseline of security measures. Security Functional Requirements (SFRs) regulate access to active objects (e.g. processes) and passive objects (e.g. data). In Part 2, components are grouped in functional families and functional classes regarding the type of functional security requirement they fulfill. A functional security component can

[2] "Deutsche Kommission Elektrotechnik Elektronik Informationstechnik" = German commission responsible for elaborating standards in the fields of electrotechnics, electronics and information technology

support multiple security functional requirements. All parts of a TOE that are involved in enforcing the security functional requirements of a system can be summarized as the TOE Security Functionality.

Part 3 is concerned with the evaluation of security. Similar to Part 2, security evaluation is structured in Security Assurance Requirements (SARs) and Security Assurance Class, Family and Components. There are 27 Security Assurance Families and the components for each family form a chain of more rigor requirements. Evaluation Assurance Levels are predefined levels for each of the 27 categories which form a reasonable set of assurance requirements. The EALs are rated from 1 to 7 where 1 has the lowest requirements and 7 the highest. The evaluation is divided in the validation of the Protection Profile / Security Target and in the verification of the Security Functional and Assurance Requirements.

In general, an ST consists of descriptions of: (1) TOE and its operational environment, (2) the TOE's security objectives, (3) SFRs and SARs, (4) security functions and assurance measures that meet the requirements, (5) claims on the conformance of one or more PPs, and (6) rationale and evidence supporting the security claims.

2.5 Safety Engineering according to the IEC 61508

IEC 61508 [14] is the generic Functional Safety Standard, which is by international agreement the basis of all ISO and IEC functional safety standards. It has been updated by Ed. 2.0 in 2010. It describes techniques and procedures for analyzing, realization and operation of safety critical systems and covers the complete system lifecycle.

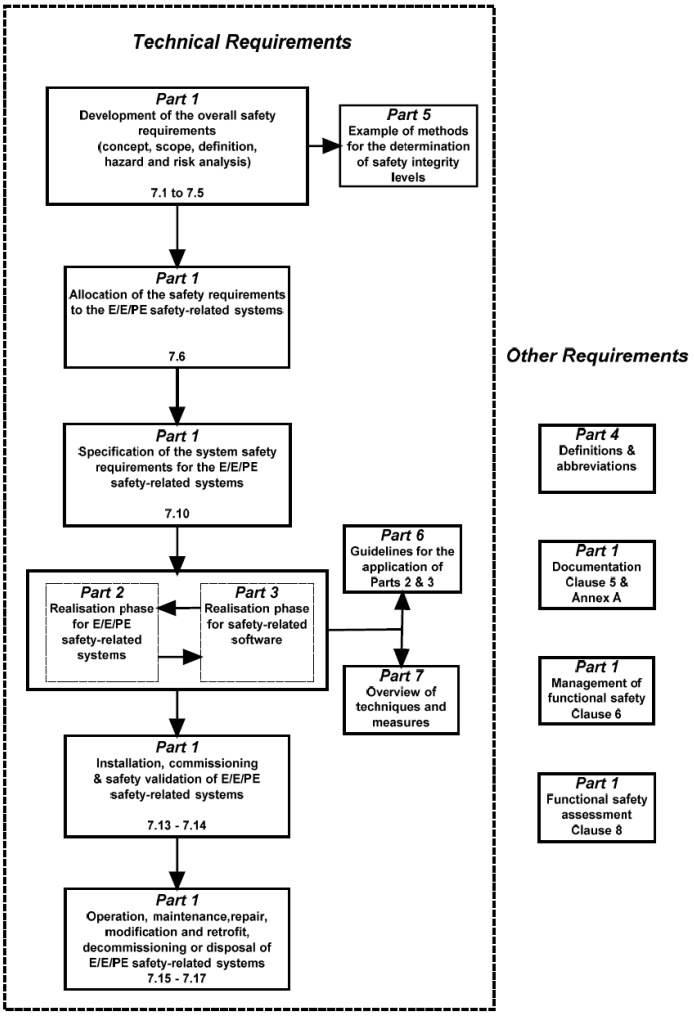


Figure 7: Overall framework of the IEC 61508 series [14]

The IEC 61508 Ed 2.0 (2010) was the first Functional Safety Standard which included security. Although security engineering itself is excluded in the description of the scope of the standard:
"In particular, this standard: (...) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;" (IEC 61508, Part 1, 1.2, m)). Further on, it does not cover "*the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety of E/E/PE safety related systems above);* (Part 1, 1.2, l).

Nevertheless, the standard states that it *requires* ***malevolent and unauthorised 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 [15] and ISO/IEC TR 19791 [16] (Part 1, 1.2, k).

Security is mentioned in multiple requirements for the safety engineering lifecycle. Security threats needs 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).

If a security threat is identified as a potential cause for a hazard a security threat analysis should be conducted. For guidance on security risks analysis the IEC 61508 refers to the IEC 62443 series (*Industrial communication networks – Network and system security*). It is explicitly noted that malevolent or unauthorized action includes security threats. If the security threat analysis identified safety critical security threats a vulnerability analysis should be undertaken to specific security requirements. *"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). For guidance on security risks analysis the IEC 61508 refers again to the IEC 62443 series and to ISO/IEC/TR 19791.

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, with the goal to build on the well-known safety certification processes of EN 50129 and integrate security requirements based on IEC 62443/ISA 99 [17].

It should be noted, that during the process of developing IEC 61508 Ed. 2.0 part of the committee were well aware that even more should be done, e.g. relating rigor of security evaluation levels (EALs of Common Criteria) to the potential impact on safety (SIL level), but there was no consensus found.

3. Requirements and business needs related to WP6

This section presents and discusses the high level requirements and business needs related to WP6 system qualification and certification. The first sub-section list the WP 6 high level requirements, and the next sub-section makes a mapping with the high level requirements received from the living labs (WP7 to WP12).

3.1 High level requirements from WP6

Requirement ID	**HL-REQ-WP06-001**
Category	Non-Functional
Sub category	Safety
Short description	Safety and security co-engineering framework
Description	Investigate, develop, and validate methodologies and technical solutions for a holistic approach to safety and security, throughout system lifetime, while taking into account the mission-critical and real-time requirements. Following standards shall be supported: ISO26262, DO178C, IEC61508, IEC 15408, IEC 62443
Verification method	Framework for safety and security co-engineering covering the entire product lifecycle is available
Rationale	Security might have an impact on safety giving advice on how to integrate the security aspect as an additional hazard (risk) for the safety-critical system, i.e. to look at the safety impact of security breaches and then derive requirements for the safety critical system, based on a joint hazard, risk and vulnerability analysis.

Requirement ID	**HL-REQ-WP06-002**
Category	Non-Functional
Sub category	Safety
Short description	Trust assurance case compilation
Description	Capability to compile seamless argumentation why the developed system or product is sufficiently safe for its intended application. This argumentation should serve as documentation (red story line) for certification activities. Following standards shall be supported: ISO26262, DO178C, IEC61508.
Verification method	Capability to automatize generation of trust assurance case.
Rationale	

Requirement ID	**HL-REQ-WP06-003**
Category	Non-Functional
Sub category	Safety
Short description	Modularization of the safety and security co-engineering framework for use in distributed environments at design time
Description	Provide import / export capabilities for the safety / security co-engineering framework at dedicated development milestones, such that specific activities performed by external teams can be integrated into the overall framework. Following standards shall be supported: ISO26262, DO178C, IEC61508.
Verification method	Capability for import / export of dedicated safety / security attributes in order to enable efficient development of part of the system by external teams and integration of their results into the overall framework
Rationale	

Requirement ID	**HL-REQ-WP06-004**
Category	Non-Functional
Sub category	Safety
Short description	Mechanisms for runtime certification of cyber-physical systems
Description	Provide methods for the runtime evaluation of modular trust certificates. This implies the introduction of suitable means to represent the trust certificates within the systems, so that the systems can utilize the certificates autonomously to reason about the current trust properties of the system (of systems). Moreover, systems must be augmented with corresponding evaluation mechanisms.
Verification method	Availability of mechanisms for runtime certification
Rationale	This aspect is mandatory to enable adaption of the system to its environment, while taking into account external information for decisions impacting the safety of the system. This is required to achieve a vision of safe and secure interconnected CPS and "systems of cyber-physical systems"

3.2 Mapping with the high level requirements and business needs from the living labs

During this sub-section, the high-level requirements related to SP6 are extracted and – if relevant – mapped to WP6 high level requirements.

Requirement ID: *<Participant>-<Req. ID>*	**Short Description:** *<Req. Name>*	**Description:** *<Req. Description>*	**WP6 analysis:**
HL-REQ-WP07-008	SW architectures - safety mechanisms	Scalable safety mechanisms shall be defined and implemented on the multicore platform to cover all automotive safety levels.	Description in HL-REQ-WP06-001 Implementation in WP3
HL-REQ-WP07-009	Safety case generation - automated compilation	The safety case information shall be automatically compiled based on existing information from product development.	HL-REQ-WP06-002
HL-REQ-WP07-011	Simulation environment - safety analysis	A simulation environment shall be specified and implemented in order to be able to provide support for the ISO26262 defined safety analysis of automotive safety critical applications.	Specification of the parameters to exchange for simulation performed in HL-REQ-WP06-001 Implementation : to be defined (Support of ISO 26262)
HL-REQ-WP07-014	System architecture and functional requirements modeling in semi-formal language (e.g. UML/SysML) from Item Definition according to ISO 26262.	The available characteristics and functionalities, taking into account also the mixed criticality, from the product description should be modeled in semi-formal language (e.g. UML /SysML) within a suitable environment/framework (e.g. Enterprise Architect), in compliance with the Item Definition guidelines according to ISO 26262 standard.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools: to be defined
HL-REQ-WP07-015	Bi-directional translation and link between formal structure (e.gf. Simulink) modeling and semi-formal (e.g. UML/SysML) modeling of the system architectures.	The available models of the system architecture in a formal modeling/simulation environment (e.g. Simulink) should be translated and linked to a semi-formal modeling/simulation environment (e.g. UML/SysML in Enterprise Architect) and vice versa.	Specification of the parameters to be exchanged for tool integration: HL-REQ-WP06-001 Implementation (tool interface): WP5
HL-REQ-WP07-016	ISO 26262 Hazard Analysis and Risk Assessment results translation/modeling in semi-formal language/environment (e.g. UML/SysML in Enterprise Architect).	ISO 26262 Hazard Analysis and Risk Assessment starts from the functional requirements and operational situations from the Item Definition and leads to the safety goals, with safe states, definition as the top level safety requirements. The modeling environment in semi-formal language (e.g. UML/SysML in Enterprise Architect) can encompass the results of this step of ISO 26262 process.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools: to be defined

HL-REQ-WP07-017	ISO 26262 safety requirements chain definition and derivation (starting from the safety goals) modeled in semi-formal language (e.g. UML /SysML).	From the safety goals the safety requirements chain is derived (functional safety req., technical safety req, HW safety req., SW safety req., design spec.) and modeled in a semi-formal language (e.g. UML/SysML), taking into account also the mixed criticality, according to the safety requirements specifications prescribed by ISO 26262 standard.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools: to be defined
HL-REQ-WP07-018	ISO 26262 safety requirements allocation to the system architecture (simulink and semi-formal language).	According to the ISO 26262 standard the safety requirements should be allocated to the elements of the system architecture. Links to these elements should be established through the modeling environment in semi-formal (e.g. UML/SysML) e the formal (e.g. Simulink) languages.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools: to be defined
HL-REQ-WP07-019	ISO 26262 safety requirements internal compliance demonstration from lower level requirements to higher level requirements.	Each safety requirement derived and modeled should be demonstrated compliant towards its predecessor at upper level, according to ISO 26262 specification, provided a suitable mean of automatic demonstration of this coherence.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools for requirement validation: to be defined
HL-REQ-WP07-020	ISO 26262 safety requirements verification tests automatic generation.	Automatic generation of test patterns and their execution for each safety requirement, according to ISO 26262 standard.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools for test case generation: to be defined
HL-REQ-WP07-021	ISO 26262 safety requirements traceability management.	The safety requirements modeled in the semi-formal language (e.g. UML/SysML) should be traceable according to ISO 26262 standard.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the tools for requirement management: to be defined
HL-REQ-WP07-022	ISO 26262 safety case (before integration/validation) automatic generation from the results consequent to the above requirements.	The results available from the previous steps can be automatically collected and linked for the assembly of the safety case (before integration/validation).	HL-REQ-WP06-002
HL-REQ-WP07-026	Dependability enhancement.	Concepts for dependability (functional safety, reliability, fault tolerance, security, and availability), both at the E/E architecture level and at the ECU level, shall be defined in the context of available resources of multicores.	HL-REQ-WP06-001
HL-REQ-WP07-027	Mixed criticality support.	Separation, i.e. freedom from interferences, among applications with different criticality levels (as defined in ISO 26262) shall be ensured in one and the same ECU.	Mechanisms to be implemented in WP3 Argumentation to be provided in HL-REQ-WP06-002

HL-REQ-WP07-029	Service-oriented architecture concepts.	Concepts and techniques related to Service-oriented Architecture (SoA) for real-time functional safety-related automotive systems shall be defined.	HL-REQ-WP06-003. Further related to HL-REQ-WP06-004 since a service concept is typically a means to foster dynamic changes in the system.
HL-REQ-WP07-030	Runtime optimization.	Concepts and techniques related to run-time optimizations for real-time safety-related automotive systems shall be defined.	HL-REQ-WP06-004
HL-REQ-WP07-044	Real Time Data Communication for safety critical and safety relevant applications	Platform and backbone data communication for safety relevant data communication based on real-time data communication	Specification of safety / security co-engineering framework: HL-REQ-WP06-001Implementation of the network management: WP4 (HW) and WP3 (Fault tolerant communication)
HL-REQ-WP07-051	security on demand	It shall be possible to request specific communication to be secured. The secure communication shall have configurable key strength, include authorization, authentication, liveness, encryption, integrity, etc. on demand. Symmetric keys and PKIs shall be supported.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Conditional Safety (and Security) Certificates HL-REQ-WP06-004 Implementation of the network management: WP4 (HW) and WP3 (Fault tolerant communication)
HL-REQ-WP07-052	safety on demand	Spatial and temporal protection (e.g., reserve own core own memory with MPU protection) shall be possible on request (at configuration time). Redundant calculations (either in parallel or in sequence) with comparison shall be automated on request.	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Conditional Safety Certificates HL-REQ-WP06-004 Implementation of the configuration tool and SW library: WP3
HL-REQ-WP08-002	Fault tolerance	It shall be able to manage multiple providers of the same services/data to guarantee the system availability also in case of single/multiple fault.	Specification of framework in HL-REQ-WP06-003 Implementation of required (SW) safety mechanisms in WP3
HL-REQ-WP08-003	Safety-data integrity	It shall be able to prevent misleading data with a sort of auto-silent mechanism that stop the services and data if the build in test detect a failure (In safety avionic applications, no data is better than misleading data).	Specification of framework in HL-REQ-WP06-003 Implementation of required (SW) safety mechanisms in WP3
HL-REQ-WP08-004	DO178C Certification	The SoA shall be structured to facilitate the DO178C certification process.	HL-REQ-WP06-002 (Support of DO178C)
HL-REQ-WP08-005	Data Synchronization	Design tools shall provide mechanism to synchronize data from different applications on different cores having different criticality and frequency.	Related to WP3 (dedicated SW libraries for synchronization between cores)

HL-REQ-WP08-006	Quality of services	The services provided by the run time support to manage the intracore communication shall be able to guarantee a different quality of service and provide error condition when such quality of services is not kept	Specification of safety / security co-engineering framework: HL-REQ-WP06-001 Implementation of the configuration tool and SW library: WP3
HL-REQ-WP08-010	Fault tolerance	It shall be able to manage multiple providers of the same services/data to guarantee the system availability or integrity also in case of single/multiple fault.	Same requirement as HL-REQ-WP08-002
HL-REQ-WP08-011	Aerospace Certification	The SoA shall be structured to facilitate the aerospace certification process.	Same requirement as HL-REQ-WP08-004
HL-REQ-WP08-012	Safety-data integrity	Identical with WP8-T8.1-11D-003: It shall be able to prevent misleading data with a sort of auto-silent mechanism that stop the services and data if the build in test detect a failure (In safety avionic applications, no data is better than misleading data).	Same requirement as HL-REQ-WP08-003
HL-REQ-WP08-013	Real time performance	Identical with WP8-T8.1-11D-001: It shall be able to guarantee a pre-defined determinism and latency in term of time to complete the service required and data delivery.	Same requirement as HL-REQ-WP08-001
HL-REQ-WP10-010	Directed towards WP 6: Binding Time	It shall be possible to control the Binding Times to fulfil different safety, performance and reliability characteristics. E.g. Compile Time, Load Time and Run Time (Configuration Mode and Operation Mode)	Related to HL-REQ-WP06-004, different times of integration and configuration require a flexible safety approach. Related to WP3 (SW development process)
HL-REQ-WP11-002	Effective use of multicore embedded systems in the energy domain.	Enable the effective use of multicore embedded systems in the energy domain with special attention to synchronization and safety as defined in the relevant standards.	HL-REQ-WP06-001
HL-REQ-WP12-005	Effective use of multicore architectures in the railway domain.	Enable the effective use of multicore architectures in the railway domain with special attention to predictability, performance and safety as defined in the relevant railway safety standards.	HL-REQ-WP08-001, HL-REQ-WP08-002 (Support of IEC 61508)

4. Proposed innovations

4.1 Proposed Innovations, high level tasks description – Alenia

The MULCOR Report [18] provides recommendations that can be used by applicants in the determination of compliance of COTS Multicore Processors with certification requirements. The use of this guidance material can be used in the effort to establish communication and understanding with the certification authorities.

Target of this contribution will be the evaluation of the MULCOR report ref. [18] and identification of the list of Recommended GuideLines (RGL) that are valuable to be adopted in the scope of the specific demonstrator. Rationale is to adopt specific guidelines on the use of Multicore Processors in safety-critical airborne systems. Material that has been discussed and known by certification authorities (i.e. EASA) should be preferable instead of developing new guidelines from the beginning.

4.2 Proposed Innovations, high level tasks description – AIT

AIT contribution is targeting 3 aspects:

- ***Safety & Security Co-Analysis***: Safety and Security Analysis are usually carried out separated. There is only a restricted information exchange between safety and security regarding potential failures, threats and resulting requirements. Proposed innovation is a Safety & Security Co-Analysis that considers Vulnerabilities in the Safety Assessment and examines the effect of Failures on Security. FMVEA is a Model-based Method for a combined Safety and Security Analysis. FMVEA is further developed and evaluated.

- ***Safety & Security Verification***: WEFACT is a Workflow Engine for Analysis, Certification and Test. It supports the management of safety-related V&V activities and automates the V&V process and the safety-case generation. Proposed innovation is an extension to WEFACT towards security and enable a combined safety and security certification process. Similar to the existing safety workflow WEFACT will be managing security requirements and integrate security related V&V tools for a largely automated workflow.

- ***Assuring robustness of multi-camera sensing***: Current situation is the limitation for life testing, or testing with recorded data due to (a) Unknown coverage of relevant scenarios, (b) Dangerous situations hard to test and (c) Expected results have to be added manually (expensive and error-prone). Proposed contribution is related to AIT's tool box VITRO (www.ait.ac.at/vitro). VITRO allows generation of realistic test data for computer vision solutions from geometric models with measurable coverage of visual challenges and relevant aspects. It will be extended for providing test data for all involved cameras. This will also cover variances in recording times, jitter, glitches caused by network and multicore processing.

4.3 Proposed Innovations, high level tasks description – AVL

From AVL point of view, the following business needs related to our use-case (WP7.3 "Design and validation of next generation hybrid powertrains systems") are the following:

1 ***Simulation environment for multicore application***: Enhancement of simulation environments to emulate parallel applications for early architecture exploration and improved safety analysis
2 ***Seamless modeling method***: Capability for seamless architecture modeling including system, SW, HW, behavior and safety aspects

3 ***SW design and development guidelines for highly parallel HW platforms***: Availability of guidelines for SW architecture / SW development including all (AUTOSAR) relevant SW layers
4 ***Tailored safety architectures for multicore platforms:*** Availability of new safety concepts, architectures & services for multi-core platforms
5 ***Integrated tool chain***: Availability of integrated and consistent tool chains for control system development
6 ***Safety case generation***: Automated compilation of safety case information based on existing information from product development
7 ***New networking solutions for multicore platforms***: Availability of improved networking solutions for heterogeneous automotive systems
8 ***Data exchange and communication strategies***: Availability of new solutions for the configuration and handling of complex communication channels during development, calibration and diagnosis

In the context of WP6, the business needs 02, 04 and 06 will be of special interests. Business need 02 ("Seamless modeling method") targets the capability to model the system and its safety / security attributes during the development, generate evidences of correct (local) component development that can be later on integrated into a (global) assurance case, as described in BN06 ("safety case generation"). BN04 ("Tailored safety architectures for multicore platforms") targets the development of software safety and security strategies efficiently including underlying hardware mechanisms.

4.4 Proposed Innovations, high level tasks description – FhG IESE

EMC² has a specific focus on open and adaptive systems where safety assurance gets very challenging. Adaptive behavior can easily lead to a combinatorial explosion and safety-relevant characteristics of the system elements that are to be integrated at runtime might be completely unknown. This can even lead to a situation where safety assurance at development time is not possible at all. A general solution concept is to shift parts of the safety engineering lifecycle into runtime at the same rate as parts of the general engineering lifecycle have been shifted. As an example consider the case of open systems where the integration step is partially postponed into runtime. In contrast to development time integration, there is no human safety expert to ensure the safety of the integrated system. Rather, the system must assure its safety on its own. This requires new kinds of safety assurance approaches that integrate tightly with established development time safety engineering activities but extend into runtime. Thus, we propose to introduce corresponding concepts and mechanisms for runtime assurance and certification that are suitable for the context of EMC² systems. This proposed innovation will be based on state of the art methodologies and techniques on the topics of modular certification, conditional certification and contract based safety. Moreover, it is our aim to extent the scope of the assurance and certification beyond safety to include important security aspects. A main focus in this regard will be to consider "security for safety", i.e. security issues that might constitute a cause for safety hazards. Most of the research activities related to this proposed innovation will be located in WP6.3, whereas the security-related aspects will be tightly integrated with WP6.2.

4.5 Proposed Innovations, high level tasks description – Freescale

The objective of FaToMLib research, EMC2 WP3, is to develop fault-tolerant algorithms for multi-core and multi-processor architectures. While certain deployments of those algorithms are to be envisioned during the research, additional work is needed to conceive FaToMLib deployment architectures. FaToMLib deployment shall be both effective and efficient. Effectiveness of the developed architectures shall enable fault tolerance in the employing applications. Efficiency is needed to reduce the overhead associated with the redundancy used to achieve fault tolerance.

4.6 Proposed Innovations, high level tasks description - IFX-UK / IFAT

Reuse of functional verification environment and results for safety qualification:
Despite the use of functional verification test patterns for the final safety qualification, nowadays there is a big disconnect between functional verification and safety qualification, meaning that test patterns are not easily reusable for safety verification (because for instance too long, or because using some verification environment mechanisms not compatible with the later fault injection environment, or even because of the self-checking implementation), but also that functional verification could be used proactively to find some of the safety shortfalls at an early stage. Additionally certain functional verification methods, such as formal verification, are already accepted as a replacement of safety qualification, depending on the logic verified; finally functional verification of certain functionalities uses mechanisms very similar to the ones that will be used for safety qualification, e.g. lockstep comparator block functional verification already consists of injecting faults and checking the comparator's detection capability, so the safety qualification could mostly leverage the results from functional verification, if this has been performed in a certain way and with a certain level of accuracy.

The intended contributions includes the following aspects

- Derive recommendations in order to improve reuse of functional verification environment and results for safety qualification. Different types of safety mechanisms will be analysed and recommendations will be provided for functional verification methods and techniques that would allow higher reuse between functional verification and safety qualification.

- Correlate Diagnostic Coverage (DC) between different abstraction levels, in particular RTL and Gate. The aim is to investigate the possibility to move away from post layout netlist safety qualification, by raising the abstraction level for the fault qualification. In this activity we will compare RTL and Gatelevel (post and pre-layout) DC and derive correlation factors or margin of errors for different types of logic. We will perform the analysis in modules with different ratio of sequential logic and control logic, and different typologies, such as register banks and alu components (e.g. multipliers, adders).

- Comparison of DC derived from stuck-at faults against DC from logical faults. The aim of this activity is to investigate the possibility to move away from physical faults by proving the equivalence to logic faults, reducing the gap between functional verification and safety qualification and again rising the abstraction level for safety qualification. We will use Certitude tool to insert logic faults, such as condition TRUE, condition FALSE, connectivity faults and find correlation of detection coverage against RTL and Gatelevel stuck-at and direct current fault model (d.c. fault model includes stuck-at, but also shorts, open, stuck-open, transient and transition faults). As for the abstraction level task we will perform the analysis in modules with different ratio of sequential logic and control logic, and different typologies, such as register banks and alu components (e.g. multipliers, adders).

- Investigate use of software solutions (e.g. SBST) to address safety case with a reduced HW redundancy system. We will analyse synergies between HW and SW safety mechanisms, trying to reduce the overlap between the two; we will also analyse the development flow of complex SW based safety mechanisms, such as the SBST, deriving recommendations on flow improvement; we will finally investigate the use of SW emulation rather than fault insertion for the safety qualification; in order to decrease the simulation effort.

As a baseline for all the tasks described above the state of the art of functional verification for complex multi-core systems and the state of the art for safety qualification will be analysed.

4.7 Proposed Innovations, high level tasks description - Rockwell Collins France

Rockwell Collins France (RCF) is involved in several Multicore processors working groups, and is very active on certification aspects, being in constant relationship with the FAA and EASA organizations. Taking into account general certification requirements, an airborne embedded system provider has to ensure the system will perform the intended functions, will meet the safety conditions and sustain the environment conditions.

Regarding security topic, RCF has supported several programs for embedded systems development having security functional and assurance objectives. To comply with such needs, RCF has developed security process, methods and tools applicable along the overall product development life cycle (e.g. security assessment, penetration testing).

Rockwell Collins works on architecture embedding Multicore Processor. These systems host Multicore for different capabilities like Display, Communication router, Radar, Mission System and Weapon System. RCF has gained security expertise on that domain by assessing security aspects on these architectures (features that may be implemented, security concerns etc.). As an example, Rockwell Collins has figured out how native security features provided by multicore architecture can improve the embedded system security.

Moreover, RCF actively contributes to the EUROCAE Working Group WG-72, titled "Aeronautical Information Systems Security". The objectives of WG-72 group are the following:

- Provide methodology / guidelines to tackle data security issues during the whole aeronautical system life-cycle,
- Set the standards for means of compliance with forthcoming Safety regulations update (when security issues overlap with safety ones),
- Provide means of compliance with regard to other existing regulations (e.g. US: CALEA, EU: ETSI),
- Define security issues related to Aeronautical system.

In this context, the Rockwell Collins contribution will be the definition of recommendations, objectives and requirements leading to a common (Safety and Security aspects), consistent certifiable approach for multicore based products.

Rockwell Collins will identify the main avionics system requirements to implement for the conception of avionics calculators ensuring applications isolation/segregation through information flow control. The interconnect of the multicore architecture being a major key point where all the accesses are performed, special attention will be given on interconnect management between cores.

The results from this high level objectives/requirements definition will serve as an input for all other work packages. These high level objectives/requirements should be discussed, refined and implemented as needed. Rockwell Collins will participate in reviewing further activities results.

4.8 Proposed Innovations, high level tasks description - TELVENT

Telvent will define an innovative safety analysis technique for multi/many-core remote terminal units that are integrated in a Smart Grid. The technique will be mainly focused on the verification and validation aspects of safety standards that affect the hardware and software parts. It could be integrated in a model-based open-source design framework (for example, POLARSYS[3] / TOPCASED[4]) that will integrate the

[3] http://polarsys.org
[4] http://topcased.org/

requirement capture and verification process management. Telvent contribution fits HL-REQ-WP06-001 and HL-REQ-WP11-002.

4.9 Proposed Innovations, high level tasks description – TUKL

With HL-REQ-WP06-001 it is clear that one particular focus of WP6 shall be placed on the interaction between safety and security. Sound co-engineering is required, implying suitable combined analyses of safety and security. TUKL has extensive experience in the fields of fault tree analysis and component fault trees. Recently, component fault trees have been augmented to also cover security-based causes for the analyzed top-level hazards [19]. Consequently, TUKL will contribute in relation toHL-REQ-WP06-001 by integrating the CFT-based co-analysis of safety and security into the EMC² co-engineering framework.

4.10 Proposed Innovations, high level tasks description – UTRC

In safety critical applications, several redundant control units are used to control a specific mechanical load, where this redundancy is required by the safety regulation. Therefore, in case of a control unit failure, the other control unit can replace the faulty one. Furthermore, prognostics and health management (PHM) processes have to be concurrently executed for the motor operation by a mean of resources (e.g. CPU) in order to support the motor's monitoring and maintainability. The transition of the technologies developed under EMC^2, specifically focusing on system safety and certification to be incorporated into the product development cycle in the aerospace domain, is of high importance for UTRC.

Typically in industrial applications non-safety and safety-related functions are separated by means of dedicated micro-processors, that ensure physical separation between non-safety and safety related functions implemented in software. For verifying system safety and reliability within multi-core devices integrating both non-safety and safety related functionality in the same device, will require temporal and spatial separation between software elements. UTRC can contribute in HL-REQ-WP06-001by developing a theoretical framework for proving safety requirements for motor drive actuation used in aerospace today. Our main challenge will be to respond to the restrictive certification regulations provided from aerospace authorities, with respect to the usage of multicore architectures in the motor-actuation technologies on the aircraft. To this end, analysis tools such as product line engineering methods or formal verification will reassure and quantify that the above implementation will be acceptable compared to certain constraints.

5. Conclusions

This deliverable targets the mapping between the user needs (coming from the living labs), the requirements from the different relevant standards, and the intended contributions of the EMC² WP6 partners. A review of the safety and security standards from different domains has been provided in Section 2. This has led to the identification of 4 high level requirements for WP6, which have been further mapped to the user needs in Section 3. After that, the contributions of the partners have been identified and finally mapped to the WP6 high level requirement in Table 1. This last mapping shall supports the living labs to identify the technologies and partners relevant to their needs.

	Application domain				**HL-REQ-WP06-001**				**HL-REQ-WP06-002**	**HL-REQ-WP06-003**	**HL-REQ-WP06-004**
					Safety and security co-engineering framework				Trust assurance case compilation	Modularization of the safety and security co-engineering framework	Mechanisms for runtime certification of cyber-physical systems
	Automotive	Avionics	Rail-way	Smart grid	Analysis	System	Software	Hardware			
Alenia		X				X	X	X			
AIT			X		X	X	X	X			
AVL	X								X	X	
FhG IESE	X	X	X						X	X	X
Freescale	X						X	X			
IFAT	X							X			
IFX-UK	X							X	X		
Rockwell Collins France		X							X		
Telvent				X	X						
TUKL	X	X	X		X						
UTRC		X			X						

Table 1: Mapping between partner contributions and WP6 HL requirements

6. References

[1] „ISO 26262 Road vehicles – Functional safety," ISO TC22/SC3/WG16, 2011.

[2] „ARP4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," SAE international, 1996.

[3] „ARP4754 - Guidelines for Development of Civil Aircraft and Systems," SAE international, 2010.

[4] „DO-178C, Software Considerations in Airborne Systems and Equipment Certification," RTCA, 2011.

[5] „RTCA/DO-254, Design assurance guidance for airborne electronic hardware," RTCA, 2012.

[6] „DO-297 Integrated Modular Avionics (IMA) Development Guidance and Certification Considerations," RTCA, 2005.

[7] „ARP5150 - Safety Assessment of Transport Airplanes in Commercial Service.," SAE International, 2013.

[8] „ARP5151 Safety Assessment of General Aviation Airplanes and Rotorcraft in Commercial Service.," SAE International, 2013.

[9] „ED-202A - Airworthiness Security Process Specification," EUROCAE, 2014.

[10] „DIN EN 50126 - Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)," VDE, 2011.

[11] „DIN EN 50128 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems," VDE, 2011.

[12] „DIN EN 50129 Railway applications - Communications, signalling and processing systems - Safety related electronic systems for signalling," VDE, 2003.

[13] „Information technology — Security techniques — Evaluation criteria for IT security," ISO/IEC 15408, 2009.

[14] „IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)," International Electrotechnical Commission, 2010.

[15] „IEC 62443 (all parts), Industrial communication networks – Network and system security," International Electrotechnical Commission, 2009.

[16] „ISO/IEC/TR 19791, Information technology – Security techniques – Security assessment of operational systems," ISO/IEC/TR, 2006.

[17] J. Braband, „Towards an IT Security Framework for Railway Automation," in *ERTS 2014*, Toulouse, France, 2014.

[18] EASA, EASA/2011/6 - The Use of Multicore Processors in Airborne Systems (MULCORS), 2012.

[19] M. Steiner und P. Liggesmeyer, „Combination of Safety and Security Analysis - Finding Security Problems That Threaten The Safety of a System," in *Proceedings of Workshop DECS (ERCIM/EWICS Workshop on Dependable Embedded and Cyber-physical Systems) of the 32nd International Conference on Computer Safety, Reliability and Security*, 2013.

[20] RTCA, DO-178C - Software Consideration in Airborne Systems and Equipment Certification, 2012.

[21] SAE, ARP4754A - Guidelines for Development of Civil Aircraft and Systems, 2010.

[22] SAE, ARP4761 - Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems, 1996.