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	**D6.15 – Validation Report**	
Workpackage	WP6	System qualification and certification
Task / Use Case	T6.1-T6.4	All tasks in WP6
Subtasks involved	All subtasks in all tasks in WP6	
Lead contractor	Infineon Technologies AG Werner Weber, werner.weber@infineon.com	
Deliverable responsible	AVL List GmbH Georg Macher, georg.macher@avl.com	
Version number	V1.3	
Date	2017-04-25	
Status	Final	
Dissemination level	Public (PU)	

Authors

Partici-pant no.	Part. short name	Author name	Chapter(s)
01O	IESE	Tiago Amorim	2.5
02A	AVL	Georg Macher	1.1, 1.2, 2.1, 3
02C	IFAT	Frank Praemassing Ashish Chauhan	2.7
02G	AIT	Christoph Schmittner Markus Murschitz, Oliver Zendel	2.2, 2.3 2.4
15E	Tecnalia	Alejandra Ruiz	2.8
15P	Telvent (Schneider Electric)	Benito Caracuel	2.6

Document History

Version	Date	Author name	Reason
0.1	2017-03-01	Georg Macher	Document initialisation
0.2	2017-03-22	Georg Macher	1st merging of partner inputs
0.3	2017-03-24	Georg Macher	2nd merging iteration
1.0	2017-03-28	Georg Macher	Draft for external review process
1.1	2017-03-31	Georg Macher	Integration of review comments
1.2	2017-04-12	Georg Macher	Integration of review comments part 2
1.3	2017-04-25	Georg Macher	Final document version
	2017-04-25	Alfred Hoess	Final editing and formatting, deliverable submission

Executive Summary

This document is the Deliverable **D6.15 – Validation Report** of the EMC2 project. The primary objective of D6.15 is to present the validation results of technologies developed in WP6. Therefore, brief descriptions of the developed technologies, an evaluation of their maturity, and the results of the validations performed within WP6 and at living labs are presented.

The scope of the D6.15 is set based on the innovation cycles and the milestones as defined in the EMC2 project. This deliverable describes activities performed to address the business needs, Key Performance Indicators (KPIs) and high-level requirements formulated in the D6.8 deliverable.

Table of contents

List of figures

List of tables

1. Introduction

1.1 Objective and scope of the document

This document gives for each technology developed in WP6 a description of the final implementation and the evaluation results. The requirements of the methods have been previously described in the deliverable D6.8. The validation report presents a brief description of the developed technologies, an evaluation of their maturity, and the results of the validations performed within the work package and in the living labs.

1.2 Structure of the deliverable report

The document is organized as follow: Section 2.1 provides an overview of the technology transfers of WP6 technologies to the individual living labs (WP7 – WP12). While the other sections of Chapter 2 list the individual WP6 technologies. The structure of these technology sections follow the same pattern: First a brief description of the technology is given and second the maturity is evaluated. The third subsection evaluates the validation activities performed in the various living labs. Finally, the forth subsection performs the evaluation of all validation activities.

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

- *D6.8 Final Requirement Set for WP6 – System Qualification and Certification* (EMC Consortium , 2015)

- *D6.9 Safety & Security co-analysis and co-design, (contracts for trust)* (EMC Consortium, 2015)

- *D6.13 Final definition of the runtime certificate approach incorporating solutions with respect to adaptive behaviour* (EMC Consortium, 2016)

- *D6.14 Final definition of a methodology for designing fault-tolerant architectures with FaToMLib* (EMC Consortium, 2016)

2. WP6 Technology Bricks (TB)

2.1 Introduction

The technology bricks developed in WP6 and evaluated in more details within the following sections of this document are on one hand evaluated and validated within the WP6, but are also applied and thus evaluated in the course of different living labs (WP7 – WP10). Table 3 briefly depicts the links between individual WP6 technologies and the living lab applying the technology. The numbers indicate the scope of transfer (see Table 1), while the colour highlighting refers to the transfer state (see Table 2). This table depicts only an excerpt of the EMC² technology transfer matrix for an overview of WP6 technologies, more details and a detailed description of the transfer states and scopes of transfer can be found in the Deliverable D13.27 (EMC Consortium, 2017).

Table 1 Technology transfer progress level scope

Scope 1:	Complete implementation into use cases in the project
Scope 2:	Partial implementation into use case
Scope 3:	Will be transferred to LL (WP7-12) but not implemented into use case
Scope 4:	Topic for future applications; technology transfer subsequent to EMC2

Table 2 Technology transfer phases and color coding

Transfer phase	Color coding
Definition	🟥
Evaluation	🟧
Development	🟨
In Transfer	🟩
Transfer complete	🟩

Table 3 EMC² technology transfer matrix excerpt

		WP7						WP10				WP11					WP12				
TB No.	Technology title	T7.1	T7.2	T7.3	T7.4	T7.5	T7.6	T10.1	T10.2	T10.3	T10.4	T11.1	T11.2	T11.3	T11.4	T11.5	T12.1	T12.2	T12.3	T12.4	T12.5
6.1	WEFACT - Workflow Engine for Analysis, Certification and Test (AIT)			2																	
6.2	FMVEA - Failure Modes, Vulnerabilities and Effect Analysis (AIT)			3									3								3
6.3	Embedded Vision Validation and QA (AIT)										3										
6.4	ConSerts M - Multidirectional Modular Conditional Safety Certificates (FhG, Tecnalia)			2				4													
6.5	Safety & Security co-analysis and co-design, contracts for trust (Telvent)				2											4					
6.6	AMSPS/PSS concept (IFAT)			2																	
6.7	PROSSURANCE tool (Tecnalia)			3																	

2.2 TB 6.1 - WEFACT (AIT)

2.2.1 Technology description

WEFACT (Workflow Engine For Analysis, Certification and Test) (Kristen & Althammer, 2015) originated from the DECOS[1] Test Bench (Schoitsch, et al., 2006), which was a Web-based distributed platform for requirements-based testing with continuous impact-assessment in order to support the safety case with evidences. In SafeCer[2], the test workflow was extended to a workflow for safety certification, and in EMC^2 the tool was re-implemented as an ECLIPSE based tool and the quality attribute of security was started to be integrated.

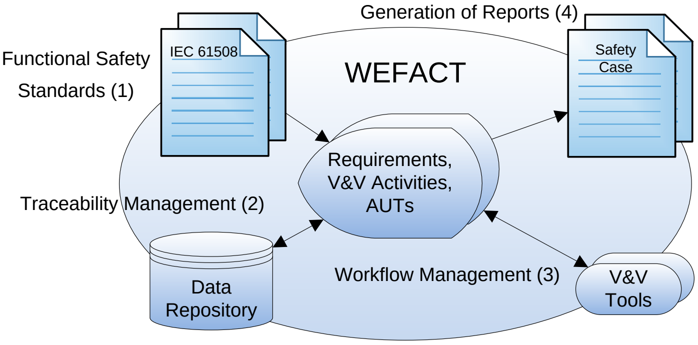

Generation of Reports (4)
Functional Safety Standards (1)
IEC 61508
WEFACT
Safety Case
Requirements, V&V Activities, AUTs
Traceability Management (2)
Data Repository
Workflow Management (3)
V&V Tools

Figure 1: Basic concept of the workflow engine WEFACT

Figure 1 provides an overview of the workflow engine WEFACT Version 1[3], which is based on the requirements management tool DOORS®[4], of which it uses the requirements management functions including the database. WEFACT supports the safety and security case by the following properties: It starts from the system, safety and security requirements, e.g. from functional safety standards (1), which are imported in WEFACT; for each requirement appropriate verification steps are defined. These "V&V Activities" are typically test or analysis activities, which apply a V&V Tool to an AUT (Artefact Under Test). The successful completion provides the evidence for the fulfilment of the respective requirement, and thus contributes to the safety and security case via a report generation tool (4). Requirements, V&V Activities and AUTs are linked to each other; thereby full traceability management (2) is implemented. This enables WEFACT to perform workflow management (3) by continuous impact management through detecting any modification in a requirement or an AUT, identifying the necessary re-verification steps based on the traceability information, and, finally, requesting the re-execution of the respective V&V Activities, e.g. by automatically starting V&V tools, in order to restore the validity of the safety case.

2.2.2 Technology maturity

WP6 internal tests and evaluation results:
Efficient safety and security aware system engineering relies on a process model which guides the user through the engineering process and allows traceability of activities and requirements in the event of changes. EPF (Eclipse Process Modelling Framework) allows to model a process with phases and individual activities and allows, thus, modelling functional safety and security standards in a formal way which enables automating the engineering workflow. Such a process model can be imported in WEFACT and activities can be connected with engineering tools and requirements. WEFACT is than able to execute an engineering workflow, modelled in EPF-C.

[1] FP6 Integrated Project "DECOS" = "Dependable Embedded COmponents and Systems"

[2] Artemis project "SafeCer" = Safety Certification of Software-Intensive Systems with Reusable Components, http://www.safecer.eu/

[3] Currently a new Eclipse-based Version 2 is under development

[4] http://www-03.ibm.com/software/products/en/ratidoor

For process management in the Hybrid Electric Vehicle Powertrain battery system use case, WEFACT was used, which provides an execution model for the processes creating the evidences for assurance case by executing project specific assurance methods and tools. The following Figure 2 presents the WEFACT workflow model.

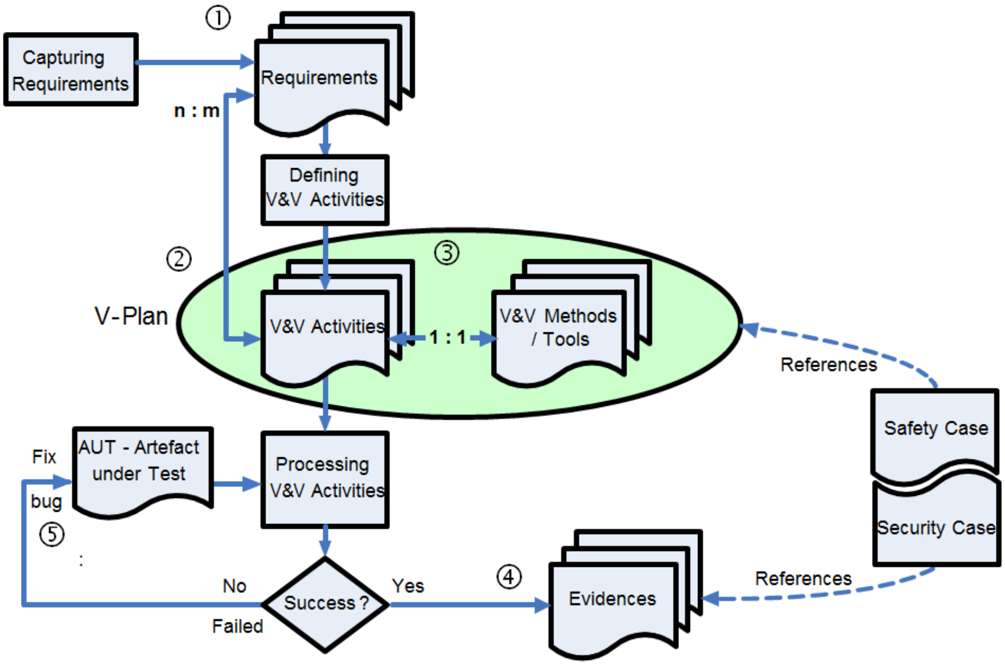


Figure 2: WEFACT workflow model supporting compositional safety and security case

The Requirements-driven workflow starts with capturing requirements ① derived from the system artefacts, from standards, and possibly other, e.g. domain specific sources. In the EMC2 project, WEFACT supports for the first time modelling a combined safety and security workflow based on respective safety and security requirements. For validating them, V-Plans containing the V&V activities are defined ② including the appropriate V&V tools ③, which can be WEFACT internal (e.g. check lists) as well as external tools, started via a test server or an OSLC automation provider. These activities are processed widely automatically; positive V&V results are used to generate the evidences ④ for the safety case, while negative results lead to automatic feedback to the developer ⑤.

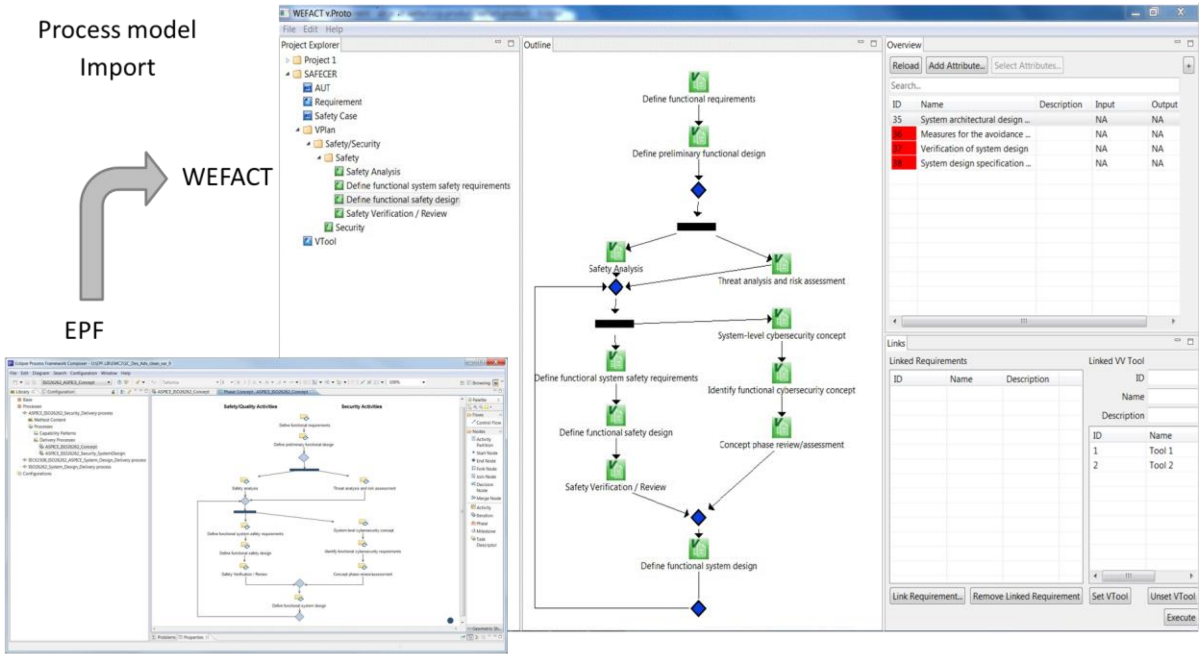
2.2.3 Technology deployment at living labs

The tool WEFACT was extended for safety and security co-engineering and applied in Use Case 7.3 "Design and validation of next generation hybrid powertrain / E-Drive". WEFACT eases, supports and facilitates the safety and security engineering process and coordinates the generation of a complete assurance case.

In the frame of EMC² project, the existing framework and processes were extended towards safety and security co-engineering. First steps were based on the Common Criteria for the security-engineering part. Once SAE J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (SAE, 2016) has been available, it was used to define and develop guidance for safety and security co-engineering. The SAE co-engineering concept is compatible with the safety and security interaction points approach developed during EMC² project and described in D6.12, Trust-based qualification and certification for complex multicore systems – HW and SW co-design.

In cooperation with the project partners AVL and VIF (Virtual Vehicle Research Center), WEFACT was applied in the Use Case 7.3 "Design and validation of next generation hybrid powertrain / E-Drive" for the safety and security case generation of a novel hybrid powertrain. Generation of safety and security (summarized as trust case) cases for complex, integrated and connected automotive systems is a major challenge.

VIF modelled the process for a combined safety and security concept phase in EPF-Composer[5]. The new, ECLIPSE RCP based WEFACT version allows to import and modify the EPF Workflow and connect requirements and activities with engineering tools to partially automate and guide the execution of the engineering process. Figure 3 shows a screenshot from the WEFACT and EPF-Composer tool, depicting the co-engineering process in both tools.


Process model Import
WEFACT
EPF
WEFACT v.Proto
File Edit Help
Project Explorer
Project 1
SAFECER
AUT
Requirement
Safety Case
VPlan
Safety/Security
Safety
Safety Analysis
Define functional system safety requirements
Define functional safety design
Safety Verification / Review
Security
VTool
Outline
Define functional requirements
Define preliminary functional design
Safety Analysis
Threat analysis and risk assessment
System-level cybersecurity concept
Define functional system safety requirements
Identify functional cybersecurity concept
Define functional safety design
Concept phase review/assessment
Safety Verification / Review
Define functional system design
Overview
Reload
Add Attribute...
Select Attributes...
Search...
Links
Linked Requirements
Linked VV Tool
Link Requirement...
Remove Linked Requirement
Set VTool
Unset VTool
Execute

ID	Name	Description	Input	Output
35	System architectural design ...		NA	NA
36	Measures for the avoidance ...		NA	NA
37	Verification of system design		NA	NA
38	System design specification ...		NA	NA

ID	Name
1	Tool 1
2	Tool 2

Figure 3: Import of the EPF model in WEFACT V2

First results were published in ERCIM News 102, July 2015, the issue had the special theme: Trustworthy Systems of Systems (Schmittner, Althammer, & Gruber, Workflow Engine for Analysis, Certification and Test of Safety and Security-Critical Systems, 2015). Additionally the topic contributed to a SAFECOMP publication (submitted, in review) from the EMC2 partner AVL, VIF, Tecnalia and AIT and a book chapter regarding the dependable development of automotive systems.

2.2.4 Evaluation results

SAE J3061 describes two approaches to security engineering for automotive systems. Either as a separate process from safety engineering or as an interacting process with safety engineering, sharing activities or work products with safety engineering. WEFACT allows to import workflows from safety and security engineering, define interactions and connect the workflow with engineering tools for safety, security or co-engineering.

Workflows based on SAE J3061 and ISO 26262 were developed by VIF and imported and executed in WEFACT. VIF developed a concept for dividing process and product-based safety and security argumentation and WEFACT is supporting the approach.

[5] https://eclipse.org/epf/

2.3 TB 6.2 - FMVEA (AIT)

2.3.1 Technology description

Security needs are increasing and represent an issue for safety related systems since such systems get connected to other systems and act according to information received from external systems. Malicious information like manipulated sensor data or changed system updates could influence the safety of a system. In order to detect such risks, safety and security teams/processes need to cooperate during the risk analysis. While there are different approaches, one promising method is the application of safety and security co-analysis. Such methods enable the simultaneous consideration of failures, threats and potential effects. FMVEA (Failure Modes, Vulnerabilities and Effect Analysis) (Schmittner, Gruber, Puschner, & Schoitsch, 2014) extends the established FMEA (Failure Mode and Effects Analysis) Method with security related threat modes and enables the identification and rating of security and safety related risks.

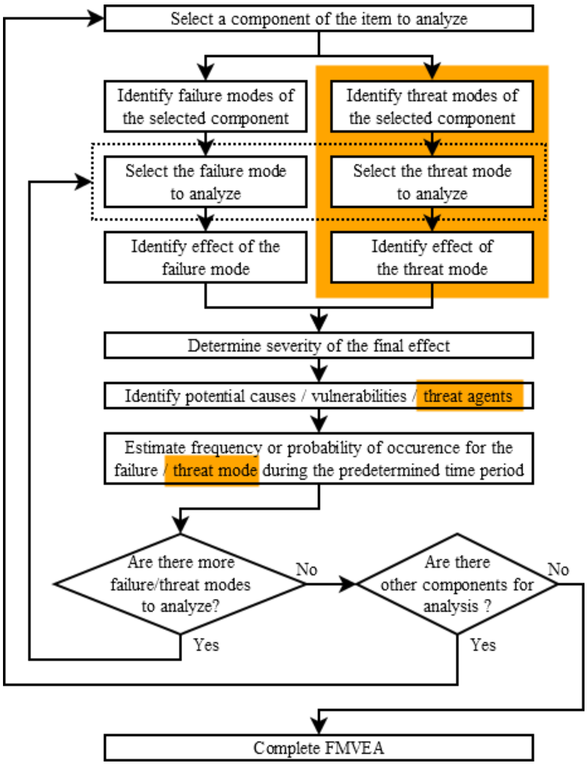

Select a component of the item to analyze
Identify failure modes of the selected component
Identify threat modes of the selected component
Select the failure mode to analyze
Select the threat mode to analyze
Identify effect of the failure mode
Identify effect of the threat mode
Determine severity of the final effect
Identify potential causes / vulnerabilities / threat agents
Estimate frequency or probability of occurence for the failure / threat mode during the predetermined time period
Are there more failure/threat modes to analyze?
No
Yes
Are there other components for analysis ?
No
Yes
Complete FMVEA

Figure 4: FMVEA Flowchart

Figure 4 shows the basic approach for a FMVEA analysis. The system is divided into components and potential threat modes for components. A threat mode describes how an attacker might be able to misuse a component. For each threat mode the effects are identified and the severity is evaluated. Afterwards, potential causes, including vulnerabilities and potential threat agents, are identified and, based on system and threat agent properties, the likelihood is estimated. Unlike safety, only a semi-quantified evaluation of the likelihood is possible. A detailed overview about the developments of safety and security co-analysis is given in D6.9 “Safety & Security co-analysis and co-design, (contracts for trust)”.

2.3.2 Technology maturity

In addition to the development of FMVEA, STPA-SEC (Young & Leveson, 2014) was extended to compare different analysis of security and of the impacts on the control flow.

STPA-Sec (Young & Leveson, 2014) is a safety and security analysis, based on STPA (Systems-Theoretic Process Analysis) (Leveson, An STPA Primer, 2013) and STAMP (Leveson, A new accident model for engineering safer system, 2004). STAMP is a new approach to understanding accidents, based on system theory. Systems are understood as interacting elements with multiple feedback loops, exchanging information and control commands. According to STAMP, accidents happens when safety-related controls and constraints were not in place or did not prevent or detect maladaptive changes. In other words, the absence of controls and constraints in a system lead to an accident.

CHASSIS (Raspotnig, Karpati, & Katta, 2012), STPA-SEC and FMVEA were compared based on the System developed in the T7.3 Use Case (Schmittner, Ma, Schoitsch, & Gruber, 2015) (Schmittner, Ma, & Puschner, Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis, 2016).

In the end, based on SAHARA (Macher, Sporer, Berlach, Armengaud, & Kreiner, 2015), FMVEA and Fault&Attack Tree Analysis, a dependable automotive development approach was developed and is in preparation for publication.

2.3.3 Technology deployment at living labs

We applied FMVEA in UC 7.3 "Design and validation of next generation hybrid powertrain / E-Drive" and UC 11.2 "Open deterministic networks". In UC7.3, we analysed a connected Battery Management System as subpart of the hybrid powertrain. The Battery Management System is connected to external systems in order to allow access to the lifetime data for insurance, battery rent or maintenance services. In addition to that, it can be connected as part of an overall connected car in order to enable Over-the-Air (OtA) updates. FMVEA was applied as part of the application of SAE J3061 (SAE, 2016) which proposes a combined concept phase for safety and security development with a co-analysis.

Our analysis identified safety relevant threat modes like manipulation of sensor signals or application of manipulated battery management software. Not all identified threats are caused by harmful intentions. Manipulation of the battery management software could be done by an unofficial repair shop in order to increase the available power or reduce charging times. But both manipulations can have potential safety critical long term effects like overheating or explosion of the battery pack.

In UC11.2 a mixed criticality network system was developed, using multicore systems for network control. Frequentis develops network infrastructure for safety critical communication. Such a safety critical switch consists of two redundant sides with multicore processors. TTTech develops time-critical network systems, enabling over one network infrastructure time-critical and best-effort communication. In UC11.2 both approaches are combined in order to enable safety and real-time critical and potential security critical open communication over one system. Multicore A1 handled the safety-critical part of the communication and A2 handled the security-critical part (depicted in Figure 6). Focus of the safety and security co-analysis was to ensure that there are no malicious effects between both multicores.

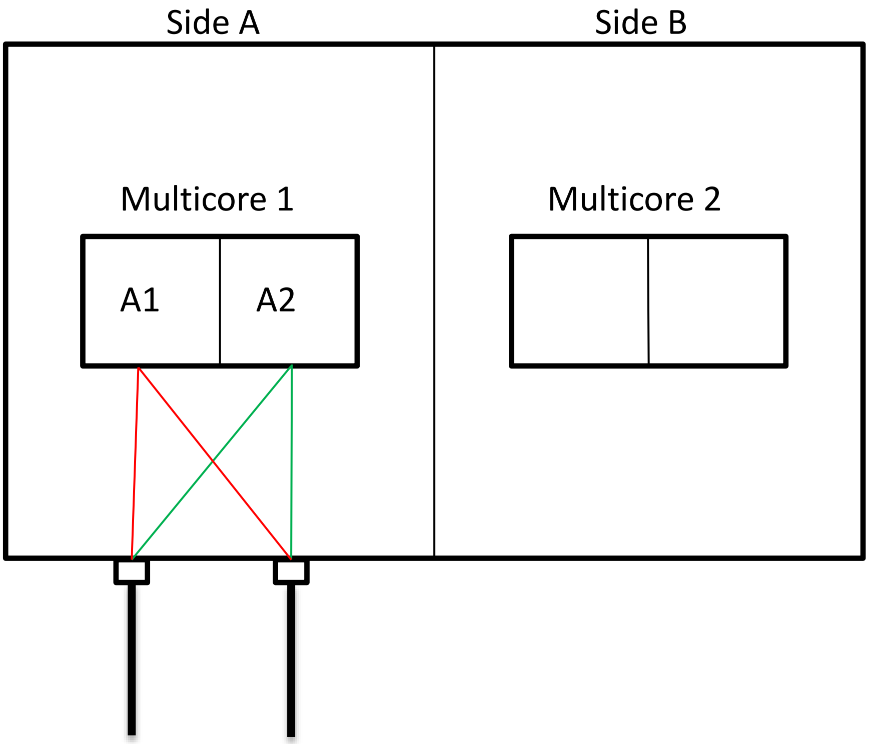


Figure 5: Potential Frequentis system

2.3.4 Evaluation results

Similar to Safety there is no “silver-bullet” for safety&security co-analysis. A combination of methods, developed partially during EMC2 (SAHARA->FMVEA->Fault&Attack Tree Analysis) was evaluated on the BMS Subsystem of the T7.3 Use Case and enabled safety&security co-engineering. While the evaluation on the T7.3 Use Case was successful and delivered good results evaluation on T11.2 was stopped because Frequentis left the project consortium

2.4 TB 6.3 - Embedded Vision Validation and QA (AIT)

2.4.1 Technology description

VITRO (Vision Testing for Robustness) is a toolchain, to automatically generate test cases for testing computer vision applications. Its basis is a test plan and domain knowledge, which is formalized as a domain model, and a selection of visual risks (situations considered hard for the computer vision task at hand). From this knowledge, a number of 3D scenes are composed. For all those scenes rendering is performed with a dedicated renderer, which renders test images and produces ground truth (the expected result) for each scene.

After that, the images are presented to the System under Test (SUT). The results generated by the SUT are compared to the ground truth to further end up in an evaluation result. The result is usually presented in a graphical representation that allows for deep insights into the SUS's limitations.

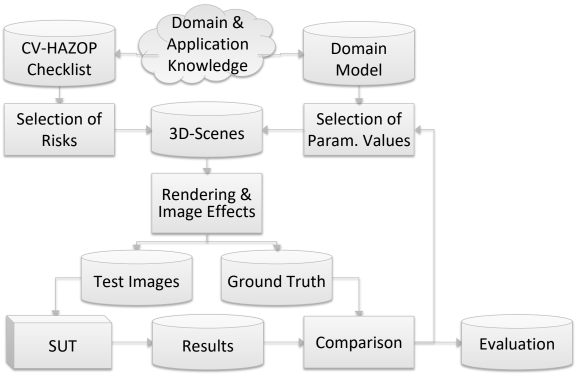


Figure 6: General process flow of the VITRO toolchain

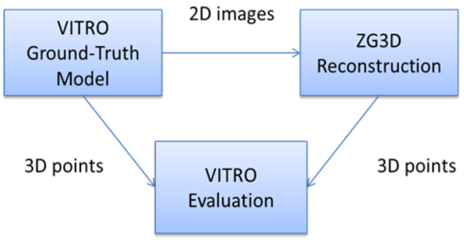
Each of these steps is highly configurable and has a multitude of possible variants how it is actually performed. One of the critical parts is sampling the domain model (describing the required variables and the possible range of input configurations for the SUT) to actually generate test cases.

2.4.2 Technology maturity

The generated test data was evaluated by applying the generated data to a trusted commercially available structure-from-motion system and the results where compared to the ground truth to eliminate possible systematic errors. The ground truth generally matched the result of the commercially available system up to a degree that can be accepted as rounding artefacts and inaccuracies by the commercially available system. The commercially available system required to have highly uncorrelated texture. Evaluation of the sampling methodology is a different story, and is one of the active research topics in the group.

2.4.3 Technology deployment at living labs

During the course of EMC², the testing approach of the VITRO toolchain has been applied to the Zero Gravity 3D (ZG3D) system (UC Manufacturing quality control by 3D inspection, T10.4).



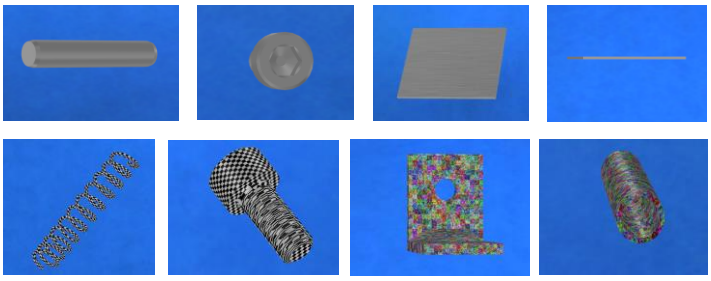


Figure 7: ZG3D test process with VITRO **Figure 8: Examples of test images**

Therefore AIT first developed a test plan in tight corporation with the Zero Gravity 3D team at the Institute of Computer Technology ITI. It is focusing on possible risks and the actual test requirements but on purpose left out possible calibration errors. This is why the exact same arrangement of cameras (calibration) in the real-world system has been generated in the virtual setup. Also, the background has been virtually reconstructed from captures of the real-world system. Then test data has been generated based on the domain restrictions (domain model) and applied to the SUT. The results and graphical analysis were performed by the VITRO team. Finally the results and possible improvements were presented as a test report and in person to the Zero Gravity 3D team.

2.4.4 Evaluation results

To tailor VITRO to the test requirements of Zero Gravity 3D the following parts were extended/improved:

(i) An input interface for the domain model, which allows for reconstruction of the camera arrangement based on the real-world calibration, has been added.

(ii) More control over the domain model samplers was added: The domain model lacked the ability to control the combination of sampling methods. Now each sampler (e.g. low discrepancy, random, cover each, pairwise …) can be linked to a variable and the test set gives a controlled combined result. A simple example: use each object in the object pool (=cover each) and for each of them use the same randomly generated orientations.

(iii) Multi-View test data generation for 16 synchronous virtual cameras was necessary. Therefore the rendering engine was extended to be able to deal with up to hundreds of cameras. All see the same scene in order to produce scene ground truth (the oriented 3D model in the world coordinates) and image ground truth for each of them.

(iv) An evaluation systematic based on the well-established Hausdorff-distance was added to the toolchain to be used for 3D model comparison algorithm.

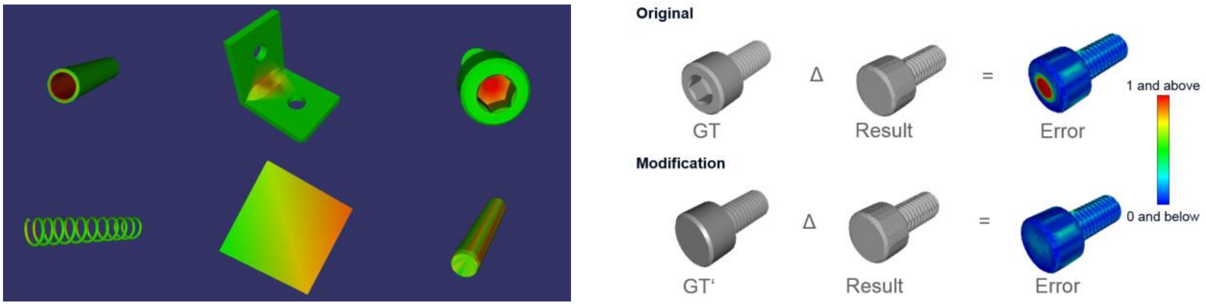


Figure 9: Left: Reconstruction quality evaluation in early stage of the project. | Right: Modification of the ground truth (GT) 3D models in order to mitigate the effect of indents (unit: mm).

The Hausdorff-distance turned out to be one of the most expressive metrics to compare SUT-result and scene based ground truth. It was integrated into the toolchain, in order to allow for fully automatic interactive testing. Interactive in the sense, that changes to the domain model or sampling immediately trigger the entire pipeline and generate new test results.

During result analysis, we found that errors introduced by indents in the objects (see Figure 9) distorted the evaluation metrics and therefore limiting the possible analysis. The reconstruction approach of ZG3D does not detect indents by design because it is based on the object's visual hull. This is why a modified version of each object was created (see Figure 9, right), that lead to more representable results. The goal of each modification was to close the objects which made them equivalent to their visual hull.

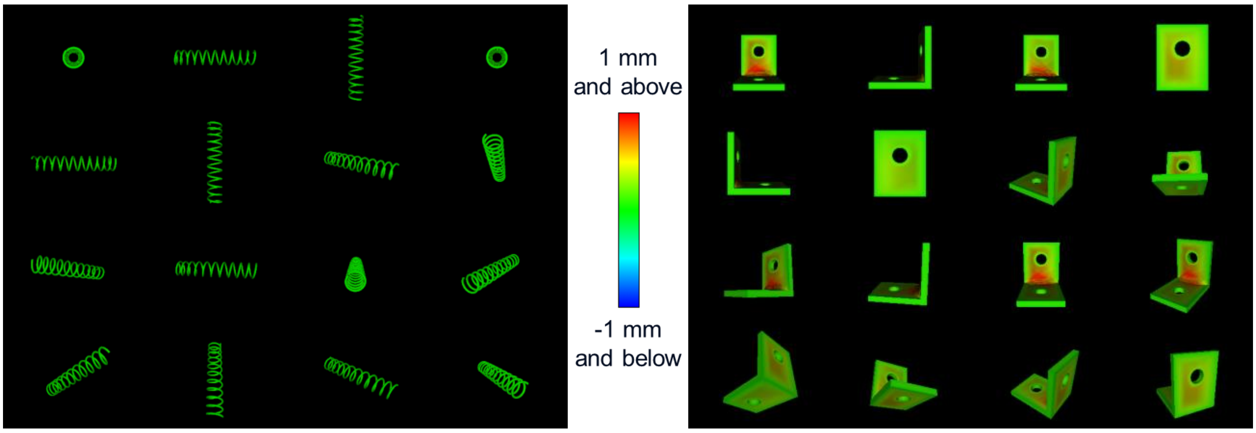


Figure 10: Selected distance results for different objects (indents are not evaluated)

The test verdict can be summarized as follows: The reconstruction performance of the ZG3D Algorithm

- is not influenced by the textures, making it especially robust in case of shining, metal objects
- is hampered by specific shapes, especially if indents are prominent

There is also a notable correlation of error metrics and object placement which can be explained by the contour based approach of the SUT (see Figure 11).

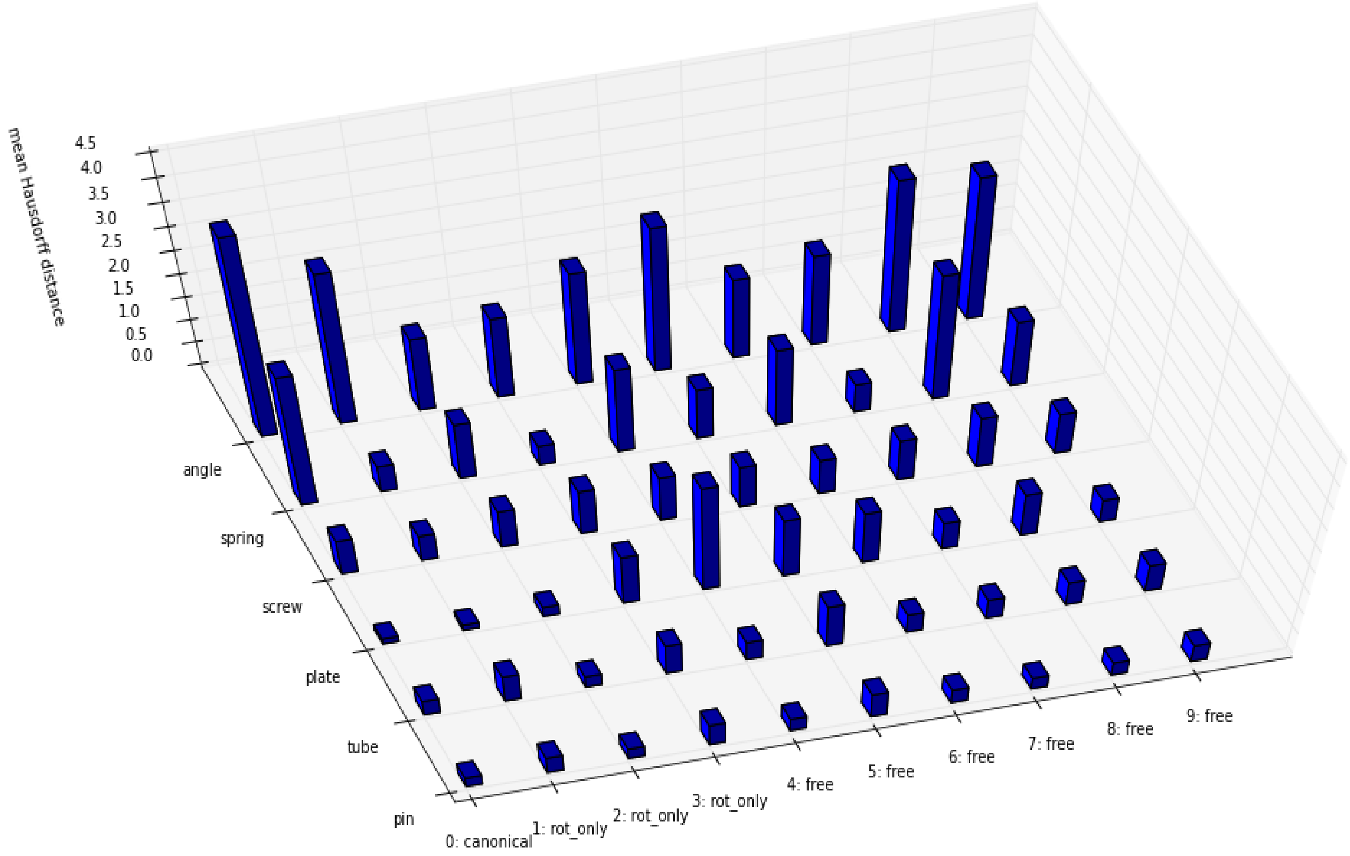


Figure 11: Mean Hausdorff-distances for the test set (16 samples per bin).

In conclusion, it can be stated that the approach taken for UC10.4 not only showed the advantages quality of the embedded computer vision development taken, but also that systematic testing of visual quality and robustness of such approaches with generative techniques such as VITRO supports is a viable and efficient means for embedded vision validation and quality assurance.

2.5 TB 6.4 - ConSerts M (FhG, Tecnalia)

2.5.1 Technology description

ConSerts M is a technology based on modular contracts designed to enable runtime safety assessment of dynamically composed systems. The contracts describe safety properties of services provided or required by components to build other services that are more complex.

Established safety engineering approaches require complete understand of the system before assessing its safety aspects. As technology drives towards more interoperability between systems and a trend of "platformization" that allows systems to be used in ways not envisioned by its own creators, expecting engineers to foresee all possible usage scenarios of such systems is unreal. To address this uncertainty, ConSerts M contracts have open ends called demands, which are requirements meant to the environment. To achieve the desired safety level, demands must be fulfilled by other services of cooperating components and this should be verified by the systems themselves before the provision of the services.

The contracts also support different configurations and different levels of safety as well as different means to reach those levels. The contracts can be described at the granularity of applications and platforms to system of systems. With ConSert M contracts, safety engineers are able to address functional and technical safety requirements.

This new technology allows system to continuously evolve as new functionalities can be easily incorporated throughout the lifetime of a system. More detailed information can be found in deliverable *D6.13 Final definition of the runtime certificate approach incorporating solutions with respect to adaptive behaviour* (EMC Consortium, 2016).

2.5.2 Technology maturity

The technology maturity can be grasped through the following efforts:

- The language developed to create contracts have suffered minor changes since its creation. The language ties functional and technical safety requirements and eases the machine validation of the contracts relation.
- A tool was developed to help engineers with the task of creating and validating contracts by verifying if the demands have appropriate guarantees. The tool creation was a joint work of Tecnalia and Fraunhofer IESE and it was presented as demonstrator in the EMC2 project second year review meeting.

Overall, the technology is ready to be used with minor adjustments, depending on the domain applied.

2.5.3 Technology deployment at living labs

ConSerts M was implemented in the Automotive Living Lab (WP7), more specifically to the use case *"Design and validation of next generation hybrid powertrain / E-Drive"*. Contracts were designed for applications and platforms responsible to control an electric engine. The initial setting of applications was modified by replacing existing application for new ones. The goal was to simulate a software update and the safety assessment of the new configuration. The implementation of ConSerts M in this living lab was a result of the joint work of Virtual Vehicle, TNO, TU Wien, Tecnalia and Fraunhofer IESE.

ConSerts M was also applied in the Industrial Living Lab (WP10), more specifically to the use case *"Drives and electric motors in industrial applications"*. The focus was on postponing the binding time of industrial applications thus enhancing flexibility without jeopardizing safety properties. The results achieved were on a conceptual level.

Publications

Amorim, T., Ruiz, A., Dropmann, C., & Schneider, D. (2015). Multidirectional Modular Conditional Safety Certificates. *4th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems - SAFECOMP.* Delft.

2.5.4 Evaluation results

The results showed promising ways to bind together safety assurance and dynamic composition of system of systems. Benefits of this new technology are manifold:

- *Support for software updates*: Systems are more likely to undergo software updates, for dependability reasons or to extend its lifetime with improved functionalities. Contracts at runtime can assure that updates do not jeopardize the system safety.
- *Shorter time to market*: Safety contracts, in general, allows building safety concepts with less effort when compared to regular safety engineering approaches.
- *Easier interoperability of systems*: safety contracts establish a common ground for systems to cooperate, allowing different manufacturers to build systems that are able to cooperate in a safe manner.
- *Safety assurance for adaptive systems*: Safety critical adaptive systems are not covered by current safety engineering practices. ConSerts M enhance those practices, allowing adaptive systems to also be safety assured.

2.6 TB 6.5 - Contracts for trust (Telvent)

2.6.1 Technology description

Telvent (Schneider Electric) has developed in WP6 an innovative technology that allows estimating the Safety Integrity Level (SIL) of the system and include security assessments. The technique is mainly focused on the verification and assessment of safety and security standards that affect the hardware and software parts. It is divided in three different components that have been integrated in the same development framework (Eclipse-based tool). The block diagram of the integration is presented in Figure 12.

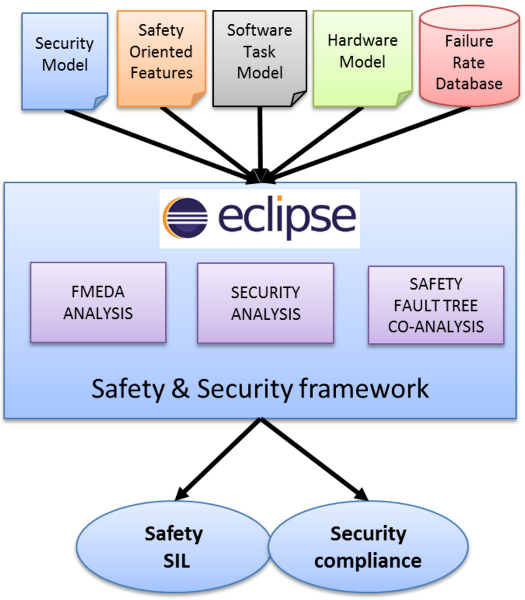


Figure 12: Integration of techniques in the framework

The first technique FMEDA (Failure Modes, Effects, and Diagnostic Analysis) is applied to the Hardware Design phase of the IEC 61508-based development process. The developed technique enables the automatization of the hardware model capture using EDIF (Electronic Design Interchange Format) and/or BOM (Bill of Materials) files. This allows reducing the certification times while increase the process efficiency. Additionally, a data base of component reliability has been created and completed with specific and general components. The database is easily expandable by introducing new components using an excel file. Using this technique is possible to estimate SIL of the system HW components. A FMEDA and a Test reports with the necessary information for the safety certification is automatically generated. These reports include the tables with the Failure Modes of each component and additional parameters (such as SFF -Safe Failure Fraction-, DC -Diagnostic Coverage- or FIT -Failure In Time- among others) that are required to calculate the SIL of the hardware sub-system.

The second technique covers the HW/SW integration and provides a SIL estimation of complete hardware-software system. It is applied in the Hardware and Software Design phases of the IEC 61508-based development process. The description of the hardware components technology is completed with models of the software components (software tasks and/or functions) and HW/SW mapping (allocation of software task/functions to hardware resources). Additionally, the system could integrate several safety-oriented features. With this information the technique generates a FTA (Fault Tree Analysis) to estimate the THR (Tolerable Hazard Rate) that is defined on the standard EN 50129 “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling”. The THR is related with the SFF (Safe Failure Fraction) parameter. With this information, it is possible to estimate the safety level of a certain system. This technique generates a scheme of the tree and a table with the information that helps to detect the weakest branches of the tree in order to improve the safety parameters.

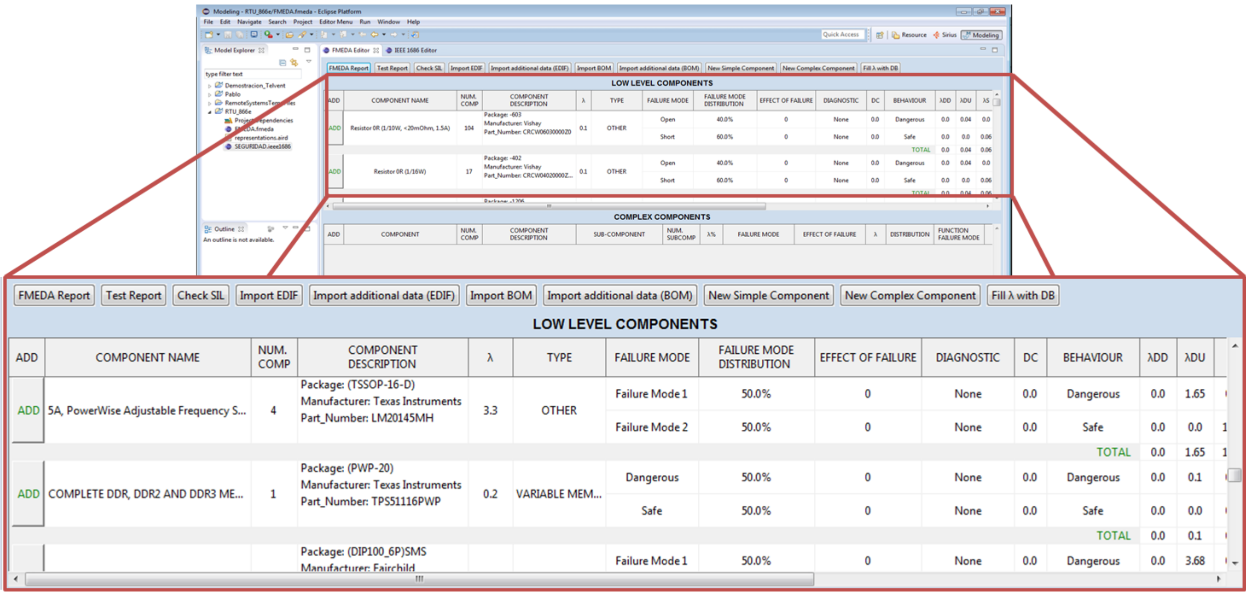
The last technique is based on the standard IEEE 1686 “Standard for Intelligent Electronic Devices Cyber Security Capabilities” . This standard establishes clauses that the system has to comply. These clauses are grouped in a Table of Compliance. The technique facilitates the information capture of the security clauses. With the information the framework generates a complete report with statistics and graphs showing the suitability of the system with the security standard.

2.6.2 Technology maturity

The technology has been validated and tested with different systems including relevant systems such as two high technology devices design for real time control and automation electrical subcenters applications. These systems are the RTU (Remote Terminal Unit) devices: SM_CPU866e (control and communications) and SM_SM_DO32T (acquisition).

2.6.3 Technology deployment at living labs

The main tests of the technology are done with the characteristics of the SM_CPU866e and SM_SM_DO32T devices. These modules are relevant systems that are complex enough to validate the presented technology. In order to validate the safety integrity level of the hardware system, its characteristics are capture automatically with the EDIF and the BOM files generated during the hardware design phase of the development process. The RTU SM_CPU866e system is composed of more than 1200 electronic/electrical/mechanical components. The SM_DO32T system has about 900 components. All these components are automatically introduced in the application and his main characteristics are captured from the database (Figure 13).



LOW LEVEL COMPONENTS

ADD	COMPONENT NAME	NUM. COMP	COMPONENT DESCRIPTION	λ	TYPE	FAILURE MODE	FAILURE MODE DISTRIBUTION	EFFECT OF FAILURE	DIAGNOSTIC	DC	BEHAVIOUR	λDD	λDU	λS
ADD	Resistor 0R (1/10W, <20mOhm, 1.5A)	104	Package: -603 Manufacturer: Vishay Part_Number: CRCW06030000Z0	0.1	OTHER	Open	40.0%	0	None	0.0	Dangerous	0.0	0.04	0.0
						Short	60.0%	0	None	0.0	Safe	0.0	0.0	0.06
											TOTAL	0.0	0.04	0.06
ADD	Resistor 0R (1/16W)	17	Package: -402 Manufacturer: Vishay Part_Number: CRCW04020000Z...	0.1	OTHER	Open	40.0%	0	None	0.0	Dangerous	0.0	0.04	0.0
						Short	60.0%	0	None	0.0	Safe	0.0	0.0	0.06
											TOTAL	0.0	0.04	0.06
			Package: -1206											

COMPLEX COMPONENTS

ADD	COMPONENT	NUM. COMP	COMPONENT DESCRIPTION	SUB-COMPONENT	NUM. SUBCOMP	λ%	FAILURE MODE	EFFECT OF FAILURE	λ	DISTRIBUTION	FUNCTION FAILURE MODE

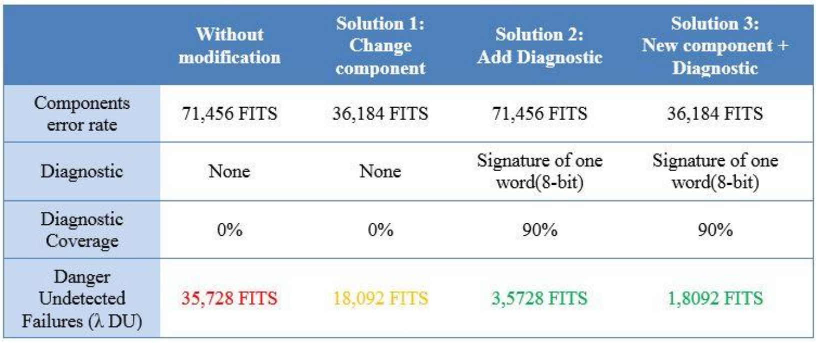
LOW LEVEL COMPONENTS

ADD	COMPONENT NAME	NUM. COMP	COMPONENT DESCRIPTION	λ	TYPE	FAILURE MODE	FAILURE MODE DISTRIBUTION	EFFECT OF FAILURE	DIAGNOSTIC	DC	BEHAVIOUR	λDD	λDU
ADD	5A, PowerWise Adjustable Frequency S...	4	Package: (TSSOP-16-D) Manufacturer: Texas Instruments Part_Number: LM20145MH	3.3	OTHER	Failure Mode 1	50.0%	0	None	0.0	Dangerous	0.0	1.65
						Failure Mode 2	50.0%	0	None	0.0	Safe	0.0	0.0
											TOTAL	0.0	1.65
ADD	COMPLETE DDR, DDR2 AND DDR3 ME...	1	Package: (PWP-20) Manufacturer: Texas Instruments Part_Number: TPS51116PWP	0.2	VARIABLE MEM...	Dangerous	50.0%	0	None	0.0	Dangerous	0.0	0.1
						Safe	50.0%	0	None	0.0	Safe	0.0	0.0
											TOTAL	0.0	0.1
			Package: (DIP100_6P)SMS Manufacturer: Fairchild			Failure Mode 1	50.0%	0	None	0.0	Dangerous	0.0	3.68

Figure 13: FMEDA tool with SM_CPU866e hardware components

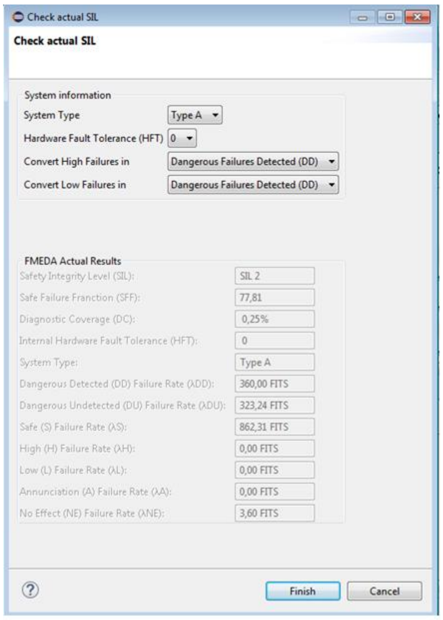
In order to increase the safety and reduce the undetected dangerous fails, there are checked the more critical components (with higher Dangerous Undetected rate). A diagnostic mechanism is added to these components that allows to increase the diagnostic coverage and therefore to reduce the critical fails. For example, it is tested an example system that has eight NAND flash memory with an error rate (λ) of 8,932 FIT. The standard defines these memories as “invariable memories”, and it recommended different diagnostics (Table A5 in IEC 61508) to reduce the dangerous undetected failures. Depend on the selected diagnostic, the diagnostic coverage reduces the undetected failures with a specific percentage. In order to increase the SIL value, it is recommended three main solutions (see Table 4). The first one is obvious and consists on change the component replacing it with one more reliable. The second one is to add a diagnostic coverage to reduce the danger undetected failure and increase the SFF. The last solution is to perform both.

Table 4: Solution example of 1Gb x8 NAND Flash Memory



	Without modification	Solution 1: Change component	Solution 2: Add Diagnostic	Solution 3: New component + Diagnostic
Components error rate	71,456 FITS	36,184 FITS	71,456 FITS	36,184 FITS
Diagnostic	None	None	Signature of one word(8-bit)	Signature of one word(8-bit)
Diagnostic Coverage	0%	0%	90%	90%
Danger Undetected Failures (λ DU)	35,728 FITS	18,092 FITS	3,5728 FITS	1,8092 FITS

The framework allows checking dynamically the SIL rate of the sub-system to check the impact of each improvement without effort. In the next figure, it can be appreciated an example of the window used to check the SIL dynamically.



Check actual SIL

Check actual SIL

System information

System Type: Type A

Hardware Fault Tolerance (HFT): 0

Convert High Failures in: Dangerous Failures Detected (DD)

Convert Low Failures in: Dangerous Failures Detected (DD)

FMEDA Actual Results

Safety Integrity Level (SIL): SIL 2

Safe Failure Franction (SFF): 77,81

Diagnostic Coverage (DC): 0,25%

Internal Hardware Fault Tolerance (HFT): 0

System Type: Type A

Dangerous Detected (DD) Failure Rate (λDD): 360,00 FITS

Dangerous Undetected (DU) Failure Rate (λDU): 323,24 FITS

Safe (S) Failure Rate (λS): 862,31 FITS

High (H) Failure Rate (λH): 0,00 FITS

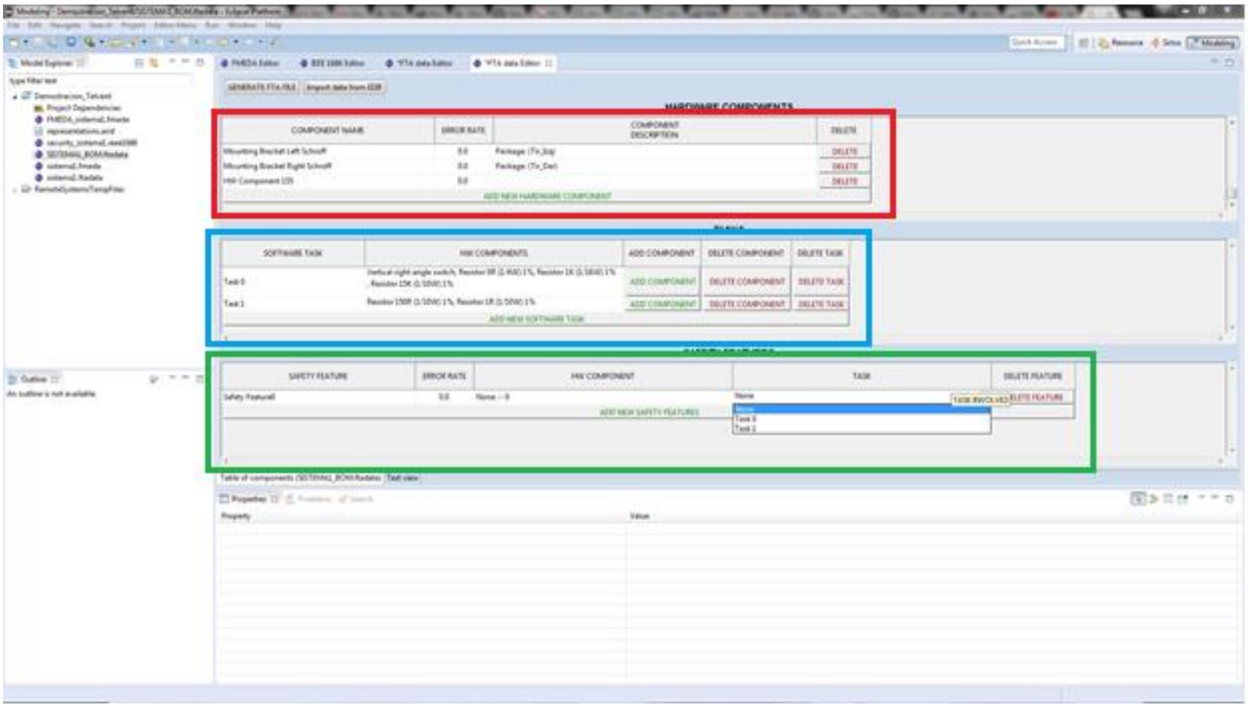
Low (L) Failure Rate (λL): 0,00 FITS

Annunciation (A) Failure Rate (λA): 0,00 FITS

No Effect (NE) Failure Rate (λNE): 3,60 FITS

Figure 14: Check SIL window

The FTA technique is checked with the hardware and the software of the SM_CPU866e. The hardware components are captured from the BOM and the EDIF file and the software and safety features are introduced in the tool manually. An example of the tool is presented in the next Figure 15. The first table (red) shows the hardware components with his error rate. The second table (blue) shows the defined software task with the components involved in its execution. The third table (green) presents the safety features and the software/hardware components that are affected by the method.



COMPONENT NAME	ERROR RATE	COMPONENT DESCRIPTION	DELETE
Mounting Bracket Left Schroff	0.0	Package: (Tx_Izq)	DELETE
Mounting Bracket Right Schroff	0.0	Package: (Tx_Der)	DELETE
HW Component 155	0.0		DELETE

SOFTWARE TASK	HW COMPONENTS	ADD COMPONENT	DELETE COMPONENT	DELETE TASK
Task 0	Vertical right angle switch, Resistor 0R (1/4W) 1%, Resistor 1K (1/16W) 1% , Resistor 15K (1/16W) 1%	ADD COMPONENT	DELETE COMPONENT	DELETE TASK
Task 1	Resistor 150R (1/16W) 1%, Resistor 1R (1/16W) 1%	ADD COMPONENT	DELETE COMPONENT	DELETE TASK

SAFETY FEATURE	ERROR RATE	HW COMPONENT	TASK	DELETE FEATURE
Safety Feature0	0.0	None -- 0	None None Task 0 Task 1	DELETE FEATURE

Figure 15: FTA tool with SM_CPU866e components

With these information, the framework can generate automatically a tree diagram and a table (see following Figure 16 and Figure 17) with the system error probabilities. This diagram helps developers to detect the more critical tasks and components and allow to introduce safety features to increase the reliability of the sub-system.

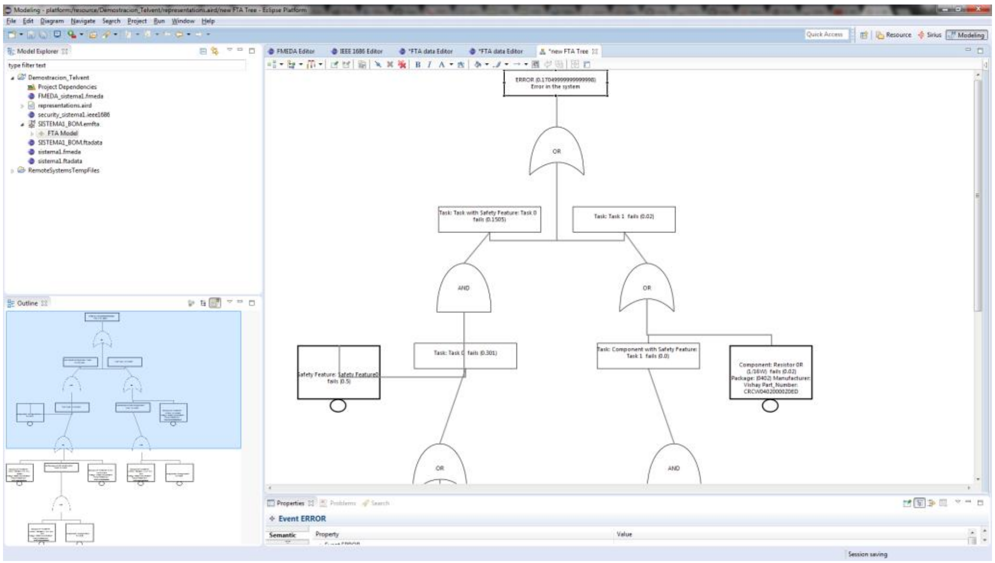
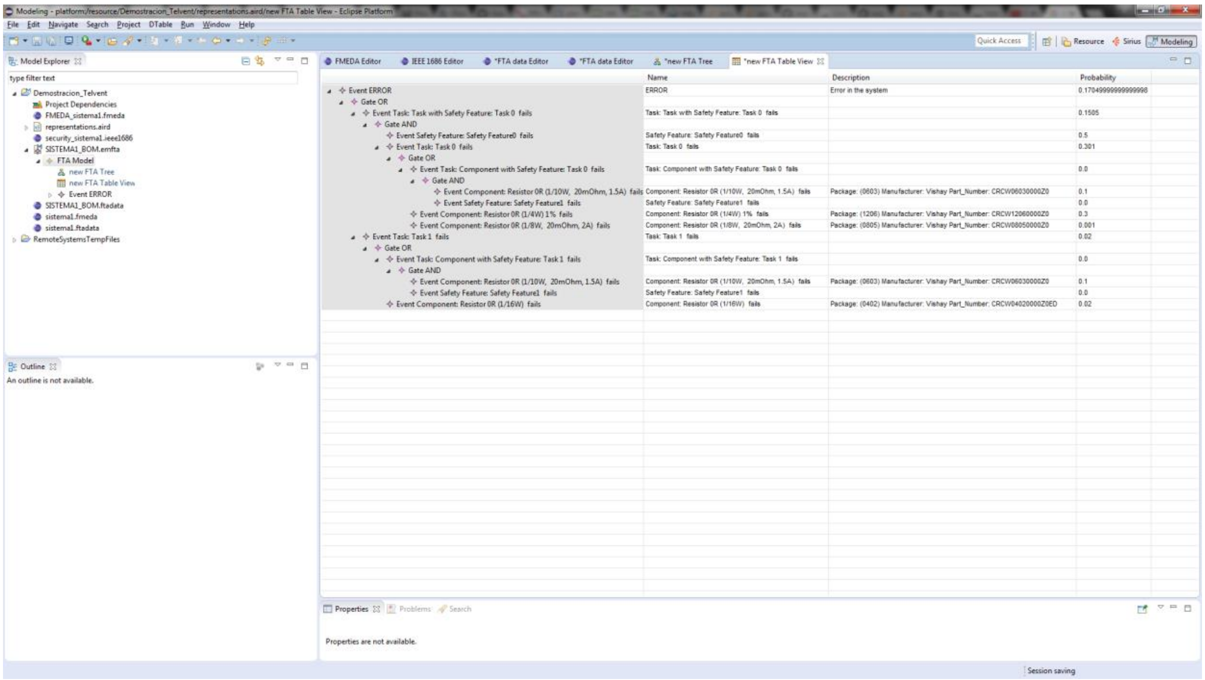

FMEDA Editor
IEEE 1686 Editor
*FTA data Editor
*FTA data Editor
*new FTA Tree
ERROR (0.17049999999999998)
Error in the system
OR
Task: Task with Safety Feature: Task 0 fails (0.1505)
Task: Task 1 fails (0.02)
AND
OR
Safety Feature: Safety Feature0 fails (0.5)
Task: Task 0 fails (0.301)
Task: Component with Safety Feature: Task 1 fails (0.0)
Component: Resistor 0R (1/16W) fails (0.02) Package: (0402) Manufacturer: Vishay Part_Number: CRCW04020000Z0ED
OR
AND
Properties
Event ERROR
Semantic
Property
Value
Session saving

Figure 16: Fault tree analysis diagram

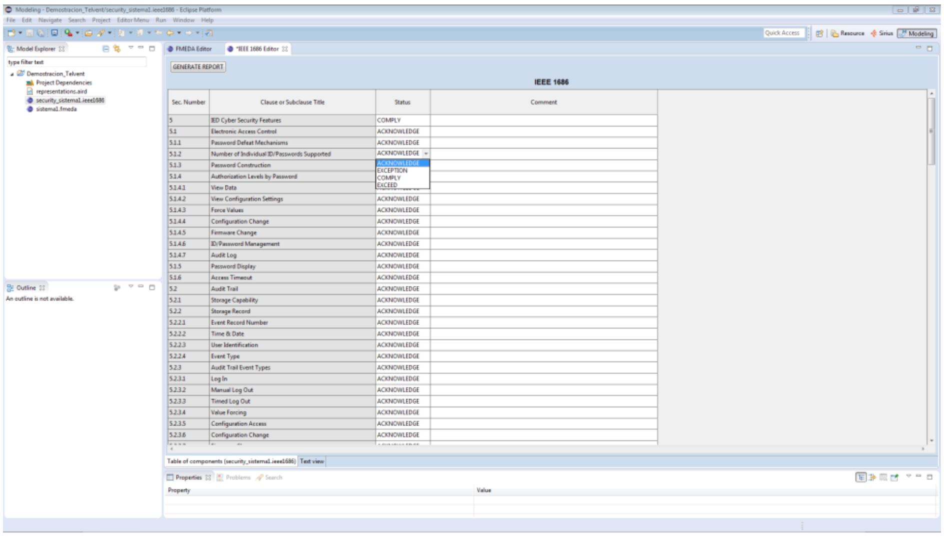


	Name	Description	Probability
Event ERROR	ERROR	Error in the system	0.17049999999999998
Gate OR			
Event Task: Task with Safety Feature: Task 0 fails	Task: Task with Safety Feature: Task 0 fails		0.1505
Gate AND			
Event Safety Feature: Safety Feature0 fails	Safety Feature: Safety Feature0 fails		0.5
Event Task: Task 0 fails	Task: Task 0 fails		0.301
Gate OR			
Event Task: Component with Safety Feature: Task 0 fails	Task: Component with Safety Feature: Task 0 fails		0.0
Gate AND			
Event Component: Resistor 0R (1/10W, 20mOhm, 1.5A) fails	Component: Resistor 0R (1/10W, 20mOhm, 1.5A) fails	Package: (0603) Manufacturer: Vishay Part_Number: CRCW06030000Z0	0.1
Event Safety Feature: Safety Feature1 fails	Safety Feature: Safety Feature1 fails		0.0
Event Component: Resistor 0R (1/4W) 1% fails	Component: Resistor 0R (1/4W) 1% fails	Package: (1206) Manufacturer: Vishay Part_Number: CRCW12060000Z0	0.3
Event Component: Resistor 0R (1/8W, 20mOhm, 2A) fails	Component: Resistor 0R (1/8W, 20mOhm, 2A) fails	Package: (0805) Manufacturer: Vishay Part_Number: CRCW08050000Z0	0.001
Event Task: Task 1 fails	Task: Task 1 fails		0.02
Gate OR			
Event Task: Component with Safety Feature: Task 1 fails	Task: Component with Safety Feature: Task 1 fails		0.0
Gate AND			
Event Component: Resistor 0R (1/10W, 20mOhm, 1.5A) fails	Component: Resistor 0R (1/10W, 20mOhm, 1.5A) fails	Package: (0603) Manufacturer: Vishay Part_Number: CRCW06030000Z0	0.1
Event Safety Feature: Safety Feature1 fails	Safety Feature: Safety Feature1 fails		0.0
Event Component: Resistor 0R (1/16W) fails	Component: Resistor 0R (1/16W) fails	Package: (0402) Manufacturer: Vishay Part_Number: CRCW04020000Z0ED	0.02

Figure 17: Fault tree analysis diagram in table format

The last technique is based on the IEEE 1686 Security standard. This technique facilitates the capture of the security information of the system and generates a report to check the compliance of the system to the IEEE 1686 standard (see next figures). These clauses are introduced in a table of compliance that vendors shall indicate the level of compliance for the product or system. As it is defined in the standard, the status shall be complete with the following responses:

- ACKNOWLEDGE – Used as a placeholder when no requirement is presented in the subclause
- EXCEPTION – Product fails to meet one or more of the stated requirements of the subclause.
- COMPLY – Product fully meets the stated requirements of the subclause.
- EXCEED – Product exceeds one or more of the stated requirements of the subclause

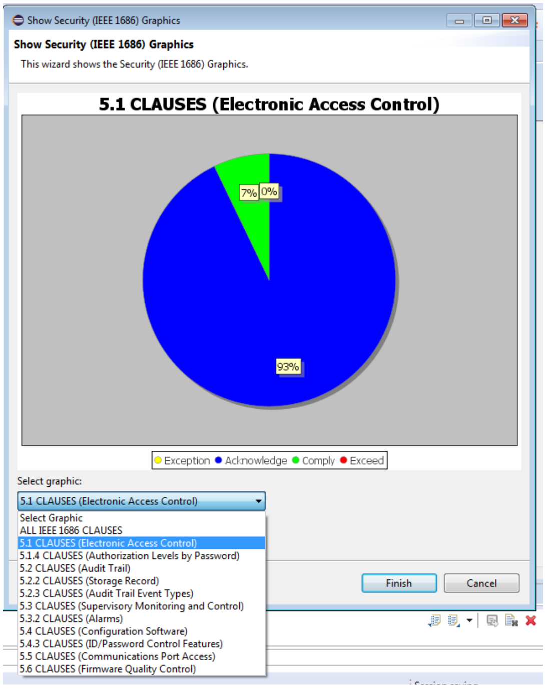


IEEE 1686

Sec. Number	Clause or Subclause Title	Status	Comment
5	IED Cyber Security Features	COMPLY	
5.1	Electronic Access Control	ACKNOWLEDGE	
5.1.1	Password Defeat Mechanisms	ACKNOWLEDGE	
5.1.2	Number of Individual ID/Passwords Supported	ACKNOWLEDGE	
5.1.3	Password Construction		
5.1.4	Authorization Levels by Password		
5.1.4.1	View Data		
5.1.4.2	View Configuration Settings	ACKNOWLEDGE	
5.1.4.3	Force Values	ACKNOWLEDGE	
5.1.4.4	Configuration Change	ACKNOWLEDGE	
5.1.4.5	Firmware Change	ACKNOWLEDGE	
5.1.4.6	ID/Password Management	ACKNOWLEDGE	
5.1.4.7	Audit Log	ACKNOWLEDGE	
5.1.5	Password Display	ACKNOWLEDGE	
5.1.6	Access Timeout	ACKNOWLEDGE	
5.2	Audit Trail	ACKNOWLEDGE	
5.2.1	Storage Capability	ACKNOWLEDGE	
5.2.2	Storage Record	ACKNOWLEDGE	
5.2.2.1	Event Record Number	ACKNOWLEDGE	
5.2.2.2	Time & Date	ACKNOWLEDGE	
5.2.2.3	User Identification	ACKNOWLEDGE	
5.2.2.4	Event Type	ACKNOWLEDGE	
5.2.3	Audit Trail Event Types	ACKNOWLEDGE	
5.2.3.1	Log In	ACKNOWLEDGE	
5.2.3.2	Manual Log Out	ACKNOWLEDGE	
5.2.3.3	Timed Log Out	ACKNOWLEDGE	
5.2.3.4	Value Forcing	ACKNOWLEDGE	
5.2.3.5	Configuration Access	ACKNOWLEDGE	
5.2.3.6	Configuration Change	ACKNOWLEDGE	

Figure 18: Security compliance tool

The column for comments and explanations may be included to provide additional information the vendor deems useful for clarification of the response. The tool can generate dynamically graphics to check the security clauses (see Figure 19).


Show Security (IEEE 1686) Graphics

Show Security (IEEE 1686) Graphics

This wizard shows the Security (IEEE 1686) Graphics.

Select graphic: 5.1 CLAUSES (Electronic Access Control)

5.1 CLAUSES (Electronic Access Control)
7%
0%
93%
● Exception ● Acknowledge ● Comply ● Exceed
Select Graphic
ALL IEEE 1686 CLAUSES
5.1 CLAUSES (Electronic Access Control)
5.1.4 CLAUSES (Authorization Levels by Password)
5.2 CLAUSES (Audit Trail)
5.2.2 CLAUSES (Storage Record)
5.2.3 CLAUSES (Audit Trail Event Types)
5.3 CLAUSES (Supervisory Monitoring and Control)
5.3.2 CLAUSES (Alarms)
5.4 CLAUSES (Configuration Software)
5.4.3 CLAUSES (ID/Password Control Features)
5.5 CLAUSES (Communications Port Access)
5.6 CLAUSES (Firmware Quality Control)
Finish
Cancel

Figure 19: Security statistics clauses

2.6.4 Evaluation results

The developed safety & security framework is based on Hardware FMEDA, HW/SW FTA and security analysis. It enables a fast SIL and security estimation of the system. The results obtained from the evaluation of the RTUs, validate the technology and demonstrate that the HW/SW development and integration process effort can be reduced. This is achieved by automating some typical steps (such as details system capture) in the safety evaluation process. The automation of the procedures reduces the effort and the time for re-validation of the systems after making hardware changes. In case of HW/SW system changes, the framework re-estimates the safety & security values with minimal efforts. It is estimated that the effort reduction that this technology provides is about 15%. Additionally, the developed safety & security framework allows the reduction of the certification time thanks to the generation of some required parameters and documents. It is estimated that the effort and time reduction is close to 15%.

The framework generates some reports such as a FMEDA report or the security report. Thanks to these reports we obtain information about how it could be possible to increase the SIL level with a few minor improvements. The improvements could be some solutions such as: adding redundancy, a diagnostic coverage or others.

2.7 TB 6.6 - AMSPS/PSS concept (IFAT)

2.7.1 Technology description

The rapidly increasing computing power in many applications and the further trend of integration of many system functions leads to new and demanding challenges for micro-controller development of various application fields (e.g. for automotive or industrial sub-systems). The power supplies for multicore multifunctional microcontrollers must meet all the requirements in terms of start-up conditions, voltage levels, static and dynamic accuracies etc.

The AMSPS architecture has been designed to fulfil all the above requirements. It has the following main sub-blocks:

- EVR_ANA: analog subsystem (e.g. Bandgap, ADC's, oscillators…)
- EVR_DIG: digital control of the Voltage-Regulators and interface to peripherals
- RBB DUT: Mixed Signal IP targeting to reduce static current consumption (e.g. channel leakage) of a digital core area.

2.7.2 Technology maturity

To achieve high verification coverage of the AMSPS as a Mixed Signal IP, a detailed and robust verification strategy is applied.

Documentation of the verification plans, setup of test benches and simulation results finally have been stored on a versioned file system (certificated for ISO26262 (International Organization for Standardization)).

Furthermore, the technology has been implemented on a test chip and electrical validation results are being captured as well. It has been made sure that the technology is validated for all possible combinations of supply sequencing, load transients and the plans are being extended for robustness validation and functional safety validation.

2.7.3 Technology deployment at living labs

The following cases were covered as an example of technology deployment:

- Power Sequencing
- Transient Low Voltage behaviour (e.g. cranking case)
- Hybrid Electric Vehicle (HEV) Inverter System Solution
- Battery Management

The related criteria are verified within some automotive applications in WP7 (UC7.1, UC7.3, and UC7.6).

2.7.4 Evaluation results

After development and fabrication of the AMSPS embedded in an Infineon Microcontroller (c40fl, Global Foundry), the steady state and the dynamic performance of the LC-based DCDC (EVRC) & linear voltage regulator (EVR33) have been demonstrated by laboratory measurements. Special attention was paid to the following topics:

- Analog Test Board Layout Guidelines
- Power-Up Sequencing of AMSPS
- Core Supply generated by LC-DCDC
- Digital EVR33 LDO

2.8 TB 6.7 - OpenCert (Tecnalia)

2.8.1 Technology description

OpenCert is an open source tool for product and process assurance/certification management to support the compliance assessment and certification of safety-critical systems in sectors such as aerospace, railway and automotive. OpenCert was originally created as a result of the FP7 project OPENCOSS[6].
The main tool functionalities are shown which include:

- Knowledge Management from Standards - This feature deals with knowledge management, captures information from standards, e.g. interpretations about intents.
- Assurance Project Management - It factorizes aspects such as the creation of assurance projects. This module manages a “project repository”, which can be accessed by the other modules
- Argumentation Management - This feature manages argumentation information applying GSN graphical notation. It also includes mechanisms to support compositional safety assurance, and assurance patterns management.
- Evidence Management - It manages the full life-cycle of evidences and evidence chains. In addition, this module is in charge of communication with external engineering tools (req. management, implementation, V&V, etc.)

2.8.2 Technology maturity

The tool has already been validated, but a more detailed and robust verification strategy has been applied. One of the keys for validation has been the use in collaboration with other tools which has been served as inputs for OpenCert to work, as well as to use outputs of OpenCert such as requirements and activities reference in to ISO26262 (International Organization for Standardization) to be used in a requirements management tool. Overall, the technology is ready to be used with minor adjustments.

2.8.3 Technology deployment at living labs

OpenCert has been applied in the Automotive Living Lab (WP7), more specifically to the use case *“Design and validation of next generation hybrid powertrain / E-Drive”*. Contracts were designed for applications and platforms responsible to control an electric engine. The first step was to model the ISO 26262 and applied it to a battery management system in order to comply with the standard requirements. OpenCert has been used in collaboration with Visure Requirements and WEFACT. The goal was to simulate the activities required for assure the product compliance within the functional safety standard. OpenCert has successfully been used to the safety case edition. The appliance of OpenCert in the context of this living lab and in collaboration with other methods and tools was a result of the joint work of Virtual Vehicle, AVL, Tecnalia and AIT.
Publications
Helmut Martin, Robert Bramberger, Christoph Schmittner, Zhendong Ma, Alejandra Ruiz, Thomas Gruber and Georg Macher. “Safety and Security Co-Engineering and Argumentation Framework” submitted to SAFECOMP 2017 (waiting to approval notification)

2.8.4 Evaluation results

The results of the application of OpenCert in the living lab showed promising ways to for defining a safety and security methodology. Experience gained here has reached standardization committees and influenced developments of new editions of standards with the goal of supporting trust case establishment, for example IEC 61508 Ed. 3.0 or ISO 26262 Ed. 2.0, but also IEC TC65 “Framework towards coordination of safety and security (in industrial automation)” benefits from approaches developed here.
The following list shows some important benefits of the presented methodology for safety and security argumentation applied to automotive domain:

- GSN structures connect processes and evidence with argumentation. The graphical depiction provided by OpenCert of links between these elements improves the stakeholder’s understanding.
- OpenCert provides the possibility to manage patterns and create GSN structures which speeds up the process development activities.

[6] OPENCOSS: http://www.opencoss-project.eu/node/7

2.9 TB 6.8 FaToMLib (FSL/NXP)

2.9.1 Technology description

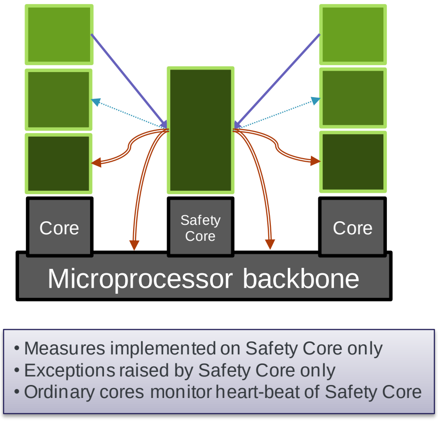
The objectives of the work on FaToMLib fault-tolerant architectures were to generate the most suitable deployment architectures for FaToMLib safety mechanisms and to ensure a compliance with ISO 26262. FaToMLib comprises algorithms that support safety-related applications to withstand faults by providing fault detection and fault reaction mechanisms. FaToMLib algorithms are conceived and developed as a part of work done within WP3 of EMC^2 project. The library is targeted for multi-core and mixed-criticality architectures. The library algorithm implementation is assumed to comprise both hardware and software components.

FaToMLib enables fault-tolerant mechanisms for coping with faults in embedded applications. The faults in the FaToMLib scope are faults affecting the application execution. Thus, in-scope are faults originating from SW, application complexity, race conditions, and HW computational shell such as CPU, memory, data acquisition peripherals.

FaToMLib algorithms shall detect HW random faults, shortly HW faults, in such a way that compliance with ISO 26262 is achieved. Therefore, the research on FaToMLib deployment addressed methodologies that enable computing the HW metrics as required by ISO 26262.

2.9.2 Technology maturity

For the FaToMLib deployment architectures several elementary architectures and implementations were considered. The investigation of different combinations of architectures and mechanism implementations showed that only some are feasible. Furthermore, the qualitative analysis of the architectures showed that Master in Charge architecture, Figure 21, allows for a better scalability versus performance degradation with the increasing demand for safety-related functionality. The selection of Master in Charge architecture was also supported by initial FaToMLib implementation in FaToMLib Pilot-bed, Figure 20, and its qualitative evaluation.



- Measures implemented on Safety Core only
- Exceptions raised by Safety Core only
- Ordinary cores monitor heart-beat of Safety Core

Figure 21: Master in Charge

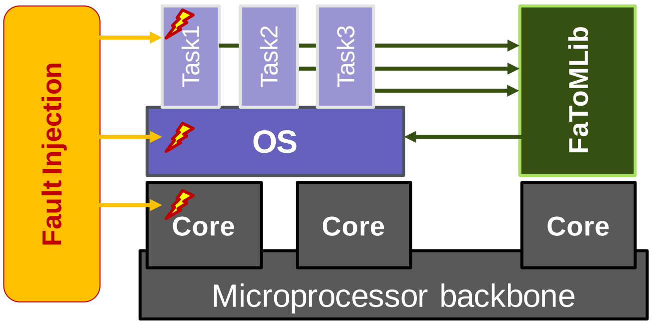


Figure 20: Pilot-bed architecture

In order to reason about and ensure freedom from interference with respect to the FaToMLib safety mechanisms, the definition of HW local independence was established. Local independence allows for defining the FaToMLib deployment to sufficiently independent HW elements on multi-core platforms.

FaToMLib FMEDA was established to enable a calculation of HW fault diagnostic coverage as required by ISO 26262 when the high-level FaToMLib safety measures are deployed. The calculation starts from determining a detection coverage (DeC) of the deployed FaToMLib safety measures with respect to potential safety goal violations. Next, the detection coverage is applied to the microcontroller components to compute the failure rate of non-detected faults. That failure rate is then used to compute the total failure rate of the non-detected faults and in turn to the calculation of the diagnostic coverage. Overall, an ISO 26262 compliant calculation of the diagnostic coverage is achieved.

2.9.3 Technology deployment at living labs

The FaToMLib deployment architectures were first implemented in FaToMLib pilot-bed and then converted into a specific HW IP that is currently under design at NXP. The design work is performed out of the scope and the funding of the FaToMLib effort sponsored by EU Artemis under EMC2 grant agreement.

3. Conclusion

This document gave a description of the final implementation and the evaluation results for each technology developed in WP6. The validation report briefly describes the developed technologies, an evaluation of their maturity, and the results of the validations performed within the work package and in the living labs.

For each technology the deployment at the different living lab and results providing evidences for the integration and development maturity are provided; as well as further evaluation activities are described.

4. References

EMC Consortium . (2015). *D6.8: Final Requirement Set for WP6 – System Qualification and Certification.*

EMC Consortium. (2015). *D6.9: Safety & Security co-analysis and codesign (contracts for trust).*

EMC Consortium. (2016). *D6.13: Final definition of the runtime certificate approach incorporating solutions with respect to adaptive behavior.*

EMC Consortium. (2016). *D6.14: Final definition of a methodology for designing fault-tolerant architectures with FaToMLib, including examples of fault-tolerant architectures employing FaToMLib and a summary assessing the meeting of the objectives defined above.*

EMC Consortium. (2017). *D13.27: Period 3 Report.*

IEEE Standards Association. (2013). 1686-2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.

International Organization for Standardization. (n.d.). ISO 26262 Road vehicles Functional Safety Part 3 - Concept phase.

Kristen, E., & Althammer, E. (2015). FlexRay Robustness Testing Contributing to Automated Safety Certification. *International Conference on Computer Safety, Reliability, and Security* (pp. 201-211). Springer.

Leveson, N. (2004). A new accident model for engineering safer system. *Safety Science*, 237 - 270.

Leveson, N. (2013). *An STPA Primer.* Cambridge.

Macher, G., Sporer, H., Berlach, R., Armengaud, E., & Kreiner, C. (2015). SAHARA: a security-aware hazard and risk analysis method. *Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 621 - 624). IEEE.

Raspotnig, C., Karpati, P., & Katta, V. (2012). A combined process for elicitation and analysis of safety and security requirements. *Enterprise, business-process and information systems modeling* (pp. 347 - 361). Springer.

SAE. (2016). *J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.*

Schmittner, C., Althammer, E., & Gruber, T. (2015, July). Workflow Engine for Analysis, Certification and Test of Safety and Security-Critical Systems. *ERCIM News 102 "Trustworthy Systems of Systems"*, pp. 29-30.

Schmittner, C., Gruber, T., Puschner, P., & Schoitsch, E. (2014). Security application of failure mode and effect analysis (FMEA). *International Conference on Computer Safety, Reliability, and Security* (pp. 310 - 325). Springer.

Schmittner, C., Ma, Z., & Puschner, P. (2016). Limitation and Improvement of STPA-Sec for Safety and Security Co-analysis. *International Conference on Computer Safety, Reliability, and Security* (pp. 195 - 209). Springer.

Schmittner, C., Ma, Z., Schoitsch, E., & Gruber, T. (2015). A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, (pp. 69 - 80).

Schoitsch, E., Athammer, E., Eriksson, H., Vinter, J., Laszlo, G., Andras , P., & György , C. (2006). Validation and Certification of Safety-Critical Embedded Systems–The DECOS Test Bench. *International Conference on Computer Safety, Reliability, and Security,* (pp. 372-385). Springer Berlin Heidelberg.

Young, W., & Leveson, N. (2014). An integrated approach to safety and security based on systems theory. *Communications of the ACM.*

5. Abbreviations

Table 5: Abbreviations

Abbreviation	Meaning
AMSPS/PSS	Analog-Mixed-Signal Power System
BN	Business Need
BOM	Bill of Material
ConSertsM	modular contracts designed to enable runtime safety assessment of dynamically composed systems
DC	Diagnostic Coverage
DEC	detection coverage
DECOS	Dependable Embedded COmponents and Systems
EPF	Eclipse Process Modelling Framework
EDIF	Electronic Design Interchange Format
ECU	Electronic Control Unit
EMC^2	Embedded multi-core systems for mixed criticality applications in dynamic and changeable real-time environments
FMVEA	Failure Modes, Vulnerabilities and Effect Analysis
FMEA	Failure Mode and Effects Analysis
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
FIT	Failure In Time
FTA	Fault Tree Analysis
HW	Hardware
KPI	Key Performance Indicator
LL	Living Lab
OSLC	Open Systems for Lifecycle Collaboration
PROSSURANCE	a model-based tool to validate, verify, assure and certify based on different standards and regulations
RTU	Remote Terminal Unit
RCP	Eclipse Rich Client Platform
SFF	Safe Failure Fraction
SIL	Safety Integrity Level
SW	Software
SUT	System under Test
SAHARA	Security Aware Hazard Analysis and Risk Assessment
STAMP	Systems-Theoretic Accident Model and Processes
STPA-SEC	System-Theoretic Process Analysis – for security analysis
µC	Micro-Controller
VITRO	Vision Testing for Robustness
V&V	Verification and Validation
WEFACT	Workflow Engine For Analysis, Certification and Test