Collaborative Large-scale Integrating Project

Open Platform for EvolutioNary Certification Of Safety-critical Systems

Industrial use cases: Description and business impact D1.2

Work Package:	WP1: Industrial Use Case Specification and Benchmark
Dissemination level:	PU
Status:	Final
Date:	02 July 2012
Responsible partner:	Fabien Belmonte (Alstom Transport)
Contact information:	fabien.belmonte@transport.alstom.com

Contributors

Names	Organisation
Laurent de la Beaujardière and Fabien Belmonte	ALSTOM Transport
Vincenzo Manni, Giorgio Tagliaferri and Andrea Felicetti	RINA Services SpA
Daniela Cancila	ATEGO France
Florent Pages	Inspearit (before DNV ITGS)
Alberto Melzi	Centro Ricerche Fiat S.C.p.A.
Cédric Chevrel and Marc Fumey	THALES Avionics

Document History

Version	Date	Remarks
V0.1	2012-03-14	Template: Contents of the use cases
V0.2	2012-04-15	First draft version including wide coverage, with some incomplete aspects.
V0.3	2012-04-26	First full version
V0.4	2012-06-08	Ready for WP review
V0.9	2012-06-22	Ready for PB review
V1.0	2012-06-28	Approved by PB

TABLE OF CONTENTS

Executive Summary

This document is the second deliverable of the OPENCOSS Work Package n°1 “Industrial Use Cases Specification and Benchmark”. It provides the results of the task T1.2 “Industrial use case formalization and definition of the business impact”. The three industrial use cases are described in this document: Automotive, Avionics and Railway domain. This document defines and develops the industrial use cases that will enable the proof-of-concept addressed by the OPENCOSS project. It refines the elaboration of user needs by clarifying the expected business impact for the three industrial domains.

The deliverable is structured within four documents. This document is the main ‘header’ document that contains the overall introduction and conclusion of the deliverable D1.2. It contains also the methodological template defined to structure the description of each industrial use case. Three appendix documents are attached, one for each industrial use case: D1.2a for the Automotive Domain, D1.2b for the Avionics Domain and D1.2c for the Railway domain. See Figure 1.

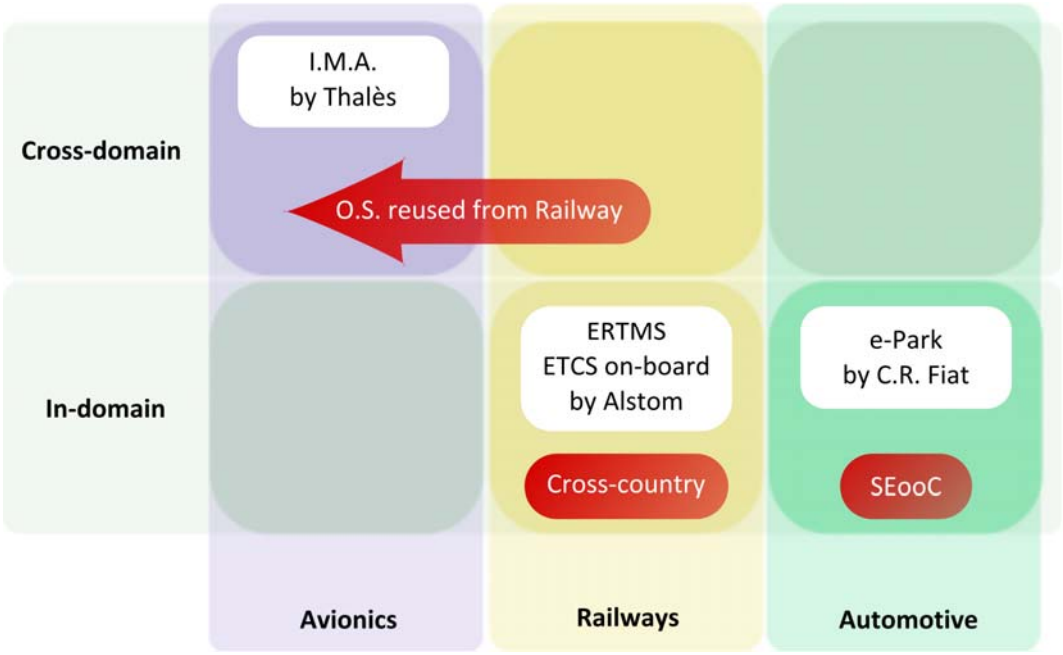

Figure 1: Industrial Use-Cases summary

The Automotive use case presents the ePARK system for an electric vehicle. This system is in charge of the management of the park pawl (mechanical engagement) actuation: this device provides mechanical locking of the transmission when the Parking mode is selected (by the driver or automatically), avoiding unwanted movement of the vehicle when stopped. The system includes specific components for the functionality envisaged, made of conventional parts (mechanics, electronics), and is developed as a Safety Element out of Context (SEooC), according to the standard ISO 26262. This use case describes the compliance of the developed system with ISO 26262 with a particular focus on the application of the SEooC requirements.

General context of the Avionics Use-Case is a situation of reuse of product from one domain (Railway) to another domain (Avionic). The goal is to build the Qualification Dossier, based on elements provided with the reused parts. The Qualification Dossier is then presented for certification. It will be taken the example of Execution Platform (Computing Unit and Operating System) to build a scenario where complete Execution Platform or parts of it are provided by an industrial actor in a given domain (Railway) and

installed in architecture in another domain (Avionic). The general way to proceed will be to identify data to be provided by the provider to permit building the qualification dossier of the Execution Platform in its final environment. The industrial use case aims to identify what the OPENCOSS framework should provide to improve certification process efficiency, reducing effort in building the platform qualification dossier.

The OPENCOSS railway use case presents the certification of a Railway signaling system. This industrial use case describes the certification of a European standardized signalling system provided by Alstom Transport. The Railway use-case chosen is a part of the European Railway Traffic Management System (ERTMS). The ERTMS is intended to replace almost all national legacy mainline signalling and train control systems all across Europe. This Use Case is related to the Generic Automatic Train Control Trainborne (GATC) Sub-System of the ALSTOM GATC solution for the European Train Control System (ETCS) of the European Railway Traffic Management System (ERTMS), known as European Vital Computer (EVC) in the architecture of ERTMS.

The GATC Trainborne Sub-System is ALSTOM's Generic solution for ETCS onboard equipment that will be used by ALSTOM ERTMS Application Projects. The main functions of this sub-system are to ensure safe movement of the train and to inform the driver by means of a Cab Display facility. This industrial use case is a generic sub-system that is parameterized for specific project application. This generic sub-system contains also railway generic products. This generic development addresses the both the compositional certification and the reuse of safety argumentation. The industrial use case aims to identify what the OPENCOSS framework should provide to improve certification process efficiency by taking into account the existing approach of generic certification. Since the specific project applications may be in different countries that have different National Safety Authority requirements, OPENCOSS shall provide support for "cross-country" certification.

1 Introduction

Safety assurance and certification are among the most expensive and time-consuming tasks in the development of safety-critical embedded systems. European innovation and productivity in this market is curtailed by the lack of affordable (re)certification approaches. Major problems arise when evolutions to a system entail reconstruction of the entire body of certification arguments and evidence. Further, market trends strongly suggest that many future (embedded) systems will comprise of heterogeneous, dynamic coalitions of systems of systems. As such, they will have to be built and assessed according to numerous standards and regulations. Current certification practices will be prohibitively costly to apply to this kind of embedded systems.

The OPENCOSS project aims to devise a common certification framework that spans different vertical markets in, first of all, the transport sector and facilitates the reuse of assurance assets across and between domains, and to establish an open-source platform or safety certification infrastructure. The infrastructure is being realised as a tightly integrated solution, supporting interoperability with existing development and assurance tools. The ultimate goal of the project is to bring about substantial reductions in recurring safety certification costs, and at the same time to increase product safety through the introduction of more systematic certification practices. Both will boost innovation and system upgrades considerably.

The main OPENCOSS objective is to both reduce time and cost for safety (re)certification via compositional and evolutionary certification and by realizing the first European-wide open safety certification platform spanning different vertical embedded system markets like the railway, avionics and automotive domains.

The overall goals of OPENCOSS, to improve the current situation in safety-critical system development, are (according to the OPENCOSS Description of Work – DoW – nomenclature):

- to demonstrate a potential reduction of recurring costs for component/product safety certification across systems by 40% and across vertical markets by 30% (**G1**)
- to demonstrate a potential reduction of product safety risks by 20% (**G2**)
- to demonstrate a potential gain for product innovation and upgrading by 20% (**G3**)

WP1 shall specify and implement industrial use cases as reference proof-of-concept of the certification framework and services offered by the OPENCOSS platform. The overall system including the conceptual framework and the safety certification management infrastructure will be benchmarked with the aid of these leading use-cases. The objectives of this WP are defined according to the general context:

- legislative background;
- time to market constraints;
- technology changes;
- safety standards evolutions (cross acceptance and certification methods).

According to this, the objectives:

- to identify and to define the constraints of the certification process;
- to identify and to define the Business impact;
- to develop the OPENCOSS industrial use cases that will enable the achievement of the three main goals of the project G1, G2 and G3 (cited before);
- to identify the OPENCOSS industrial stakeholder needs as a baseline for WP2 (Requirements and Architecture Design);
- to provide a common evaluation framework and quality metrics to validate the OPENCOSS solution;
- to validate the functionalities of the OPENCOSS platform and monitor its performance and related cost savings;
- to provide feedback to project development teams regarding usability and overall acceptance level;

- to demonstrate the technical and economic feasibility of the OPENCOSS technologies developed within the technical WPs in real environments;
- To benchmark the three main goals of OPENCOSS G1, G2 and G3 cited before.

The task T1.2 will define and develop the Industrial Use Cases that correspond to the scope addressed by OPENCOSS. The deliverable D1.2 formalizes these three Industrial Use Cases and states the business impact addressed by the three specific domains. The business impacts are defined with regard to the following OPENCOSS main objectives (O1, O2 and O3 as described in the DoW):

- define a common conceptual safety certification language to improve mutual recognition agreement of safety approvals and to be employed to discuss abstract notions from different industrial markets.(**O1**);
- define a compositional and evolutionary approach that reuses safety arguments, in a way that it is easily certifiable and that such certification is re-usable when integrating the product in higher level systems and interconnected systems. (**O2**);
- develop a fully-fledged open-source tool infrastructure that will allow developers and other safety assurance stakeholders to (**O3**):
    - reduce uncertainty and (re)certification costs by following a measurable and auditable process (**O3.a**),
    - assess their compliance with safety standards and practices (**O3.b**).

The industrial case studies provided in the present deliverable are use cases (examples) of the outputs of the safety case activities and certification process in the automotive, avionics and railway domains.

The industrial case studies presented here are descriptions of systems and certification scenarios; the actual industrial work-products to be collected separately (WP3) for use by the downstream activities for the following purposes:

- to illustrate the elaboration of user needs;
- to provide test cases for platform integration and validation;
- to allow benchmarking for measuring the OPENCOSS platform benefits.

Each industrial use case provides:

- A technical description of the industrial use case in the scope of the OPENCOSS goals. This includes a definition of the stakeholders' use cases , presentation of functional and non-functional aspects of the industrial system being considered, some materials that support the case for safety, along with the identification of the current state of the art and expected improvements;
- An analysis of the relationship to the other conceptual and technical work packages;
- The identification of the expected results (business impact) from their corresponding outcomes/prototypes with regard to O1, O2 and O3 project objectives and the technical Work packages to which those objectives are related (WP4 to WP7).

This document illustrates in particular the practices developed by the stakeholders which are related to the re-use and compositional certification in the following processes:

- development process;
- safety assurance process;
- certification process.

The three industrial use cases are presented using the following format, as detailed in 2.1:

- System Description;
- Development Lifecycle Activities;
- Engineering Environment;
- Description of the Compositional Approach;

- Summary of main argument for safety;
- System lifetime events;
- Relationship to conceptual and technical work packages.

The industrial use cases provided here satisfy the requirements described in Task T1.1 [1]. They must allow the demonstration of re-use and compositional certification.

The methodology adopted to present the description of the industrial use cases is defined in §2. This methodology is straightforward as it consists of the definition of a common format for the three industrial use cases description. This format includes a description of the industrial system being studied and its design and safety development lifecycle. It allows the reader to capture the main activities performed and the arguments provided to acquire the certification or standard compliance. Finally, the business impact of the industrial use case is discussed by relating the industrial use case with the conceptual and technical work packages of OPENCOSS.

This document D1.2 constitutes the head document of the deliverable where the objectives, the methodology and the overall conclusion are stated. Three appendixes document are attached, each one corresponds to the description of one industrial use case. They follow the template defined in the methodology section see §3.1.

Consequently, the D1.2 document is structured as follow:

- Head document (this file): contains the introduction, the methodology and the conclusion;
- Automotive Use Case description: D1.2a [2];
- Avionic Use Case description: D1.2b [3];
- Railway Use Case description: D1.2c [4].

2 Methodology

A template has been defined to harmonize the description of the industrial use cases. It contains all the descriptions necessary to understand the Safety Cases. It can therefore follow an agreed vision common to all three domains.

2.1 Template of use-case presentation

Each application domain uses as a writing guide the following list of sections with explanatory remarks *[italics inside brackets]* and sample text to illustrate the proposal.

1. Introduction

[Presentation of introductory generalities about the use-case. This serves as an executive summary of the rest of the chapter. Give regulatory context, three-line description of the safe item, and identify any other pertinent remarks to guide comprehension (assumptions, reminder of info essential to comprehension, ….)]

The industrial use case presents … development, submitted to … authorities, for approval for use in … applications. The system includes … generic products

2. System Description

[Presentation of involved actors, operational scenarios, architectural model of the system and main functions.]

2.1. Industrial use case actors and environment

[*Diagram describing the interfaces between the system and the actors*]
The system environment is constituted by the following actors: driver, maintainer, the rolling stock, the tracks devices, *etc*. The driver communicates with the system through the Man-Machine Interface…

2.2. Industrial use case operational scenarios

Scenario 1: The system receives mission orders from the driver and supervises the train movement constraints (Movement authorities speed, *etc.*) [*Diagram*]

Scenario 2: *etc.*

2.3. Main functions provided by the system

Train separation
Management of the Train speed profile
…

2.4. Architecture of the system

[Block diagram(s) and description of each component.]

2.5. General characteristics of the system

[Provide non-functional aspects, such as environmental constraints, performance requirements, safety targets.]

3. Development Lifecycle Activities

3.1. Engineering and certification stakeholders

Design teams, quality staff, safety manager, Airworthiness Assurance Manager …

3.2. Activities executed by stakeholders

[*Describe the activities executed during the development lifecycle that are relevant to certification. Provide example materials achieved within these activities.*]

- Quality management process
- Safety management process
  1...1. Safety Plan
    1...1.1. Organization chart
- Technical safety process
  1...1. Failure Mode and Effect Analysis (FMEA)
  1...2. Hazard Log
- Independent safety assessment

4. Engineering Environment

[Describe your tools that are used during system development that are relevant for the certification process. Explain the purpose and main functions of each. Explain the method or need for interoperability between the tool and the OPENCOSS platform (interface technology).]

Examples are:
Word, Excel, read-only PDFs,
Rectify and Doors, and other
Document Manager (in-house tools),

- Managing document review cycles, including recording and acceptance of individual remarks
- Support document approval cycle with electronic signatures

Configuration Manager, Change Management (ClearQuest) and other

5. Description of the Compositional Approach

[Description of which items in the industrial use case are re-used from other contexts. Identification of which components are pre-existing but undergo modification.]

The system reuses Generic Products in the sense of EN50129, including the Eurobalise product delivered by one Independent Safety Assessor and cross-accepted by another ISA, the one performing assessment of the overall Trainborne Generic Application…

6. Summary of main argument for safety

[This is a capsule summary of the case for safety that is presented in the use case, to facilitate identification of the most important aspects. Optionally in GSN format.]

Example:
The Trainborne Generic Application is judged to be adequately safe based on the following arguments

- Re-use of proven-in use Generic Products associated with ISA reports;
- Development practices under quality management and safety management processes for elimination of systematic failures;
- Use of a vital computer providing protection against random failures through the application of composite fail-safety.

7. System lifetime events

[Presentation of the main events that guide the overall system lifetime.]

7.1. Planning
7.2. Development Milestones
- End of Design (start of HW/SW execution);
- End of Prototype development (start of functional testing);
- End of Prototype testing (start of production).

7.3. Production
7.4. Qualification trials in target environment or on final customer site
- Installation;
- static and dynamic testing;
- trial running.

7.5. Certification, approval or award of qualification
7.6. Operation and Maintenance

8. Relationship to conceptual and technical work packages and expected results

[Provide a recap by forward reference of the parts of the industrial use case that are flagged as particular needs that should be taken into account by specific OPENCOSS features (composability, re-use, Common Certification Language, …]

3 Industrial Use Case description files

The Automotive Use-Case is described in the **D1.2a** document [2].
The Avionic Use-Case is described in the **D1.2b** document [3].
The Railway Use-Case is described in the **D1.2c** document [4].

4 Conclusion

The Industrial Use-Cases formalization is included in the three appendixes of this document by using a common format described in section 2.1. This common format enabled the description of the underlying information provided by the industrial use cases that tackle the objectives of the OPENCOSS project. Indeed, the description of the three systems provided characterizes the compositional and re-use approach addressed. The Automotive compositional and reuse-approach is related to the application of the SEooC concept. The Avionics approach is a cross-domain reuse proof-of-concept and applies for the Integrated Modular Avionic (ARINC standard) compositional approach. The Railway case refers to the development of a generic system and generic products as a compositional and re-use approach. The description of the safety case and safety related activities of the industrial use cases show the concepts and artifacts manipulated by each industrial domain. This provides concrete illustrations to identify the set of concepts addressed by each industrial domain in order to design the common conceptual safety certification language. The systems lifecycle description and the business impact definition included in the common template of this document provides the rationale to motivate the development of practical features in the OPENCOSS platform allowing to enact the certification process and provide engineering assistance.

The Automotive use case presented the ePARK system for an electric vehicle, a case study about a safety critical system developed as Safety Element out of Context (SEooC), which is a system developed outside of the context of a specific vehicle, but as a product on the shelf, with reference to specific assumptions for generic types of vehicles to which it can apply.

This concept is used for the development of most innovative automotive components: these wait “on the shelf” for their application to the various types of vehicles identified as targets during the formulation of the assumptions related to their intended use.

The Automotive case study represents the main scenario of re-use in the automotive domain, aiming at developing a component according to ISO 26262 for the installation in several vehicles, saving time and costs related to its conformity assessment and production.

The general context of the Avionics Industrial Case Study is a scenario of reuse of a product (an Execution Platform, i.e. Computing Unit & Operating System) from one domain (Railways) to another domain (Avionics). The goal is to build the Qualification Dossier, based on elements provided with the reused parts.

The proposed Avionics Case Study is intended to highlight the benefits expected from the OPENCOSS platform, to the extent that it will provide the following list of (non-limitative) capabilities:

- means to express complex argumentation logic linking various elements (generic common language and tools for building argumentation);
- means for any user of any domain (providing an item) to get access to a reduced set of necessary elements to provide for certification in another domain;
- means for any user of any domain (reusing an item) to identify usable data provided and ensure an easy check of correctness or completeness;
- means to link various elements such as specification items and verification elements, through advanced traceability means.

The Railway Industrial Case Study is based on an existing and certified ERTMS subsystem: an onboard equipment providing the following main functions:

- to supervise train speed and application of braking when needed, to ensure safe movement based on signaling information received from the trackside;
- to provide the driver a Cab Display facility, the Driver's Machine Interface (DMI).

This subsystem and the methodology that led to its certification have been presented. Among the industrial needs that this Case Study aims to address in OPENCOSS are the following:

- to build progressively the case for safety, to build incrementally the argumentation and to facilitate its assessment;
- to provide support allowing to overcome the barriers set by each country to apply cross-acceptance from one country to another;
- to support and generalize compositional certification;
- to capture emergent properties related to constraints of use of a certified generic product.

5 References

[1] OPENCOSS, “D1.1 Constraints of the certification process,” 2012-06-28.

[2] OPENCOSS, "D1.2a Automotive Use Case," 2012-06-28.

[3] OPENCOSS, "D1.2b Avionic Use Case," 2012-06-28.

[4] OPENCOSS, "D1.2c Railway Use Case," 2012-06-28.

[5] OPENCOSS, "D1.2a Automitive Use Case," 2012-06-28.

[6] CENELEC, "EN 50126 - Railway applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS)," 1999.

[7] CENELEC, "EN 50129 - Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling," 2003.

[8] CENELEC, “EN 50128 - Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems,” 2011.

[9] ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS, "FIS for Man-Machine Interface".

[10] ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS, "FIS for the Train Interface".

[11] ALCATEL * ALSTOM * ANSALDO SIGNAL * BOMBARDIER * INVENSYS RAIL * SIEMENS, "System Requirement Specification".

[12] P. Ward and S. Mellor, Structured Development for Real-Time Systems, New Jersey: Prence Hall, 1985.

[13] EC, Commission Decision 2012/88/EU on the 25th January 2012 on the technical specification for interoperability relating to the control-command and signalling subsystems of the trans-European rail system.

[14] EC, "Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community," *Official Journal L191 vol 51,* 2008.

[15] EC, "Council Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system," *Official Journal L235 ,* pp. 6-24, 1996.

[16] EC, "Directive 2001/16/EC of the European Parliament and of the Council of 19 March 2001 on the interoperability of the trans-European conventional rail system," *Official Journal L110,* pp. 1-27, april 2001.

[17] OMG, 2012. [Online]. Available: http://www.omgsysml.org/. [Accessed 8 June 2012].

[18] Artisan, 2012. [Online]. Available: http://www.atego.com/products/artisan-studio/. [Accessed 20 June 2012].