ADVANCED DESIGN AND VERIFICATION ENVIRONMENT
FOR CYBER-PHYSICAL SYSTEM ENGINEERING
www.advance-ict.eu

Advance

D.1.4 - ADVANCE CERTIFICATION STRATEGY IN THE RAILWAY DOMAIN

ADVANCE

Grant Agreement:	287563
Date:	30/11/2014
Pages:	10
Status:	Final
Author:	Fernando Mejia, Fabien Belmonte Alstom
Reference:	D1.4
Issue:	1

Partners / Clients:

SEVENTH FRAMEWORK PROGRAMME	
FP7 Framework Programme	European Union

Consortium Members:

University of Southampton	Critical Software Technologies	Alstom Transport	Systerel	Heinrich Heine Universität	Selex ES

Contents

1. Contribution of ADVANCE to certification

ADVANCE Deliverable D1.5 [4] presents the technical activities carried out to develop the formal model of the IXL-DC and to move from an Event-B system model to a Classical-B software model. This deliverable explains how these activities are integrated into Alstom's system development process and explains how they contribute to the certification of Alstom's systems.

The French Standardization Organization (AFNOR) defines certification as "a business process through which a recognized body acting independently with no ties to the parties involved gives written assurance that an organization, a process, a service, a product or a set of professional skills meets the baseline requirements set out in a reference standard."

The CENELEC standards, EN50126 [7], EN50128 [8] and EN50129 [9], are the certification framework of European railway signalling systems. The standard EN50126 defines acceptance requirements on the process, activities and techniques used for the "implementation of a consistent approach to the management of reliability, availability, maintainability and safety" of railway systems. The standard EN50128 defines acceptance requirements on the process, activities and techniques used for the development of software of railway control and protection systems. The standard EN50129 defines acceptance requirements on the process, activities and techniques used for acceptance and approval of safety-related railway electronic systems. ADVANCE Deliverable D1.3 [4] provides an outline of different stages of the EN50126 standard which we briefly outline here.

In order to comply with the requirements defined in CENELEC standards EN50126 and EN50129, Alstom implements a system development process involving design, validation and verification, and safety activities. Alstom's signalling systems in revenue service developed following that process are indeed certified according to these standards. Figure 16 represents Alstom's system development process.

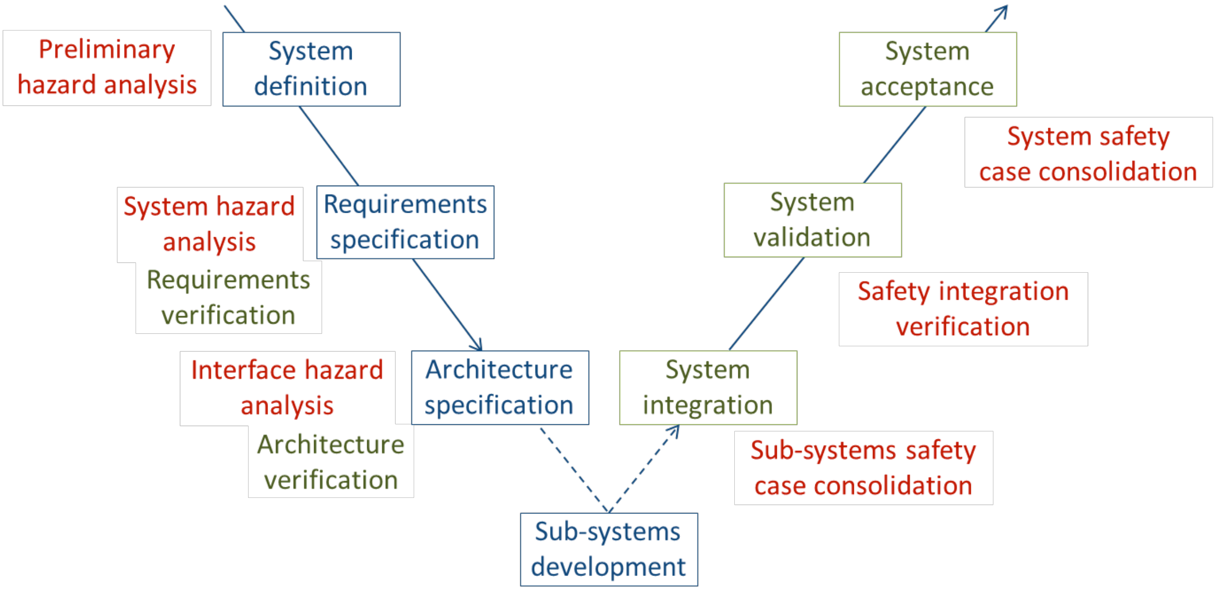
Preliminary hazard analysis
System definition
System hazard analysis
Requirements specification
Requirements verification
Interface hazard analysis
Architecture specification
Architecture verification
Sub-systems development
System integration
Sub-systems safety case consolidation
System validation
Safety integration verification
System acceptance
System safety case consolidation

Figure 1: Alstom's system development process

The blue boxes represent design phases. The green boxes and legends represent respectively validation and verification phases and activities. And the red legends represent safety activities.

D1.3 also outlines proposals on how ADVANCE methods and tools could contribute to certification according to the CENELEC standards. During the final period of ADVANCE, we organised the safety activities and the activities of creation, validation and verification of Event-B models within the system development life cycle and we defined the evidence that these activities must provide according to recommendations of the representatives of Alstom in the European FP7 project OPENCOSS [10].

More precisely, the ADVANCE activities correspond to activities imposed by the CENELEC standards which are the framework of certification of railway systems and the results of ADVANCE activities will contribute to create and maintain the Hazard Log of the developed system which is a centrepiece for its certification.

A Hazard Log is created and maintained throughout the safety life-cycle of the developed system. It documents all identified hazards together with the measures and actions taken or to be taken to eliminate or mitigate them to tolerable levels. Independent safety assessors and certifiers examine carefully the Hazard Log to ensure that all hazards have been eliminated or sufficiently mitigated by effective and appropriate actions.

So, on the one hand, hazard analysis with STAMP/STPA will provide the hazards and requirements that are the basis of the Hazard Log. And, on the other hand, the development of an Event-B formal model will provide evidence that effective actions have been taken to eliminate or mitigate some of the identified hazards. The fact that the evidence is based on formal models and formal verification should strengthen the confidence of assessors and certifiers in the effectiveness of the actions taken to eliminate or mitigate the hazards.

Table 1 presents the contribution of ADVANCE to certification in railway domain in a structured way. The first column lists the phases/activities of the system development process; the second column presents the goals of the correspondent phase/activity; the third column presents the ADVANCE methods and tools used to achieve the goals of the correspondent phase/activity; and the fourth column presents the evidence provided to certifiers by the corresponding ADVANCE methods and tools.

Phase	Goals	ADVANCE M&T	Evidence provided by ADVANCE M&T
System definition	· Establish system mission profile, · Prepare system description, · Identify operation and maintenance strategies, · Identify operating conditions, · Identify maintenance conditions, · Identify Influence of existing infrastructure constraints.	--	--
Preliminary hazard analysis	· Identify the hazards at the boundary of the system under consideration (resulting from the use of the system in a specified context, as defined in the system definition) · Classify the consequences (possible accidents) of these hazards, · Identify the necessary mitigations for the system or the elements of the system (including preliminary SIL allocation to functions), in order to lower the risk to an acceptable level, · (optional) predict Hazardous Failure Rate (HFR) achievable (to be confirmed by Fault Tree Analysis or equivalent method after detailed design).	--	--
Requirements specification	· Undertake requirements analysis, · Specify system, Specify environment, · Define system demonstration and acceptance criteria, · Establish validation plan, · Establish management, quality and organisation requirements, · Implement change control procedure.	Event-B Method: · Creation of an Event-B model by stepwise refinement, · Proof of the Event-B model using Rodin, · Definition of test scenarios, · Animation of the Event-B model with the scenarios using ProB.	· Event-B model of the system · Proof report of the Event-B model of the system · Test scenarios

Phase	Goals	ADVANCE M&T	Evidence provided by ADVANCE M&T
System hazard analysis	· Identify the cause and consequences of the failures of the functions and interfaces supported by the system on the basis of system requirements specification and external interfaces description, · Identify the mitigations necessary to control the hazards and to lower the risk at an acceptable level, · Confirm the SIL allocation to the functions and interfaces of the system, · Record the hazards identified with their effects and the associated risk mitigation recommendations.	STAMP/STPA: · Creation of the control structure of the system, · Hazardous controls analysis, · Causal factor analysis.	· System control structure · Hazardous controls analysis tables · Causal factor scenarios
Requirements verification	· Verify completeness and consistency of system requirements and external interface description.	Event-B Method: · Verification of the traceability of system requirements in the Event-B model of the system, · Verification of the correctness of the proof rules created manually for the proof of the Event-B model of the system, · Verification of the adequacy of test scenarios.	· Event-B model verification report · Tests scenarios verification report
Architecture specification	· Apportion System Requirements, · Specify sub-systems and component requirements, · Define sub-systems and component acceptance criteria.	Event-B Method: · Creation of the Event-B models of the subsystems by stepwise refinement and composition/decomposition of the Event-B model of the system, · Proof of the Event-B model of the subsystems using Rodin, · Definition of test scenarios for the Even-B models of the subsystems, · Animation of the Event-B models with the scenarios using ProB.	· Event-B models of the subsystems · Proof report of the Event-B models of the subsystems · Test scenarios

Phase	Goals	ADVANCE M&T	Evidence provided by ADVANCE M&T
Interface hazard analysis	· Identify the cause and consequences of the failures of internal interfaces of the system on the basis of system architecture and internal interfaces description, · Identify the mitigations necessary to control the hazards and to lower the risk at an acceptable level, · Confirm the SIL allocation to the components of the system, · Record the hazards identified with their effects and the associated risk mitigation recommendations	STAMP/STPA: · Hazardous controls analysis, · Causal factor analysis.	· Hazardous controls analysis tables · Causal factor scenarios
Architecture verification	· Verify consistency and completeness of system architecture and internal interfaces descriptions.	Event-B Method: · Verification of the traceability of subsystems requirements in the Event-B models of the subsystems, · Verification of the correctness of the proof rules created manually for the proof of the Event-B models of the subsystems, · Verification of the adequacy of test scenarios.	· Event-B models verification reports · Tests scenarios verification reports
Sub-systems development	· Specify subsystems · Develop subsystems, · Validate and verify subsystems.	· If the subsystem is not an elementary subsystem, the present process is followed, · Otherwise , if the subsystem involves safety-critical software, transition from Event-B to Classical-B.	· Safety-ca se of subsystems involving evidence provided ADVANCE M&T · Safety-case of subsystems involving evidence of Classical-B developed software.

Phase	Goals	ADVANCE M&T	Evidence provided by ADVANCE M&T
Sub-system safety-case consolidation	· Assess the Safety Cases of the sub-systems, · Identify and record the hazards closed by sub-system development, · Analyse the consequences on safety of the constraints exported by the sub-systems and, if necessary, integrate them into the Hazard Log.	ADVANCE contributes indirectly to this activity through hazard analysis and verifications reports produced by the safety and verifications teams during the development of the sub-systems.	. Verification reports provided by ADVANCE M&T applied for the development of subsystems
System integration	· Assemble all the sub-systems, · Test compliance with system architecture and internal interface descriptions.	Requirements on the interface of a sub-system that have been formalised and proved in an Event-B model need not to be tested if the software of the sub-system has been formally developed and if its Classical-B model captures these requirements too.	· Architecture specification proof report
System integration verification	· Verify that safety requirements closing hazards related to architecture and internal interfaces have been effectively satisfied either by testing or by formal proof of Event-B and Classical-B models.	ADVANCE contributes indirectly to this activity through hazard analysis and verifications reports produced by the safety and verifications teams during the development of the sub-systems.	· Hazard analysis reports · Architecture specification proof and tests verification reports
System validation	· Perform tests ensuring fulfilment of system requirements, · Analyse system verification and integration reports, · Analyse sub-system verification and validation reports.	As for system integration, requirements on the system that have been formalised and proved in an Event-B model need not be tested if they have been refined and apportioned between subs-systems formally developed and proved.	· Requirement specification proof report
System safety case consolidation	· Produce a System Safety Case compliant with CENELEC EN 50129 standard.	ADVANCE contributes indirectly to this activity through hazard analysis and verifications reports produced by the safety and verifications teams during the development of the system.	· Hazard analysis reports · Requirement specification proof and tests verification reports

Phase	Goals	ADVANCE M&T	Evidence provided by ADVANCE M&T
System acceptance	· Assess that the signalling system meets the customer requirements, · Assess reliability, availability and maintainability demonstration, · Assess application specific System Safety Case.	ADVANCE contributes indirectly to this activity through hazard analysis and verifications reports produced by the safety and verifications teams during the development of the system.	· Hazard analysis reports · Verification reports.

Table 1 : Evidence provided by ADVANCE Methods and Tools for certification

2. Conclusions

In this deliverable we defined an industrial system development process by integrating ADVANCE technology in Alstom's system development process. The process is compliant with CENELEC EN50126 and EN50129 certification standards because Alstom's process is already compliant and because the integrated techniques are techniques recommended by the standards that support and formalise current practices. The process is inspired by Alstom's software development process and just like it takes full advantage of formal development in the sense that it avoids integration and validation tests covered by simulation and proof. The certification strategy will serve as a basis for Alstom's plans for exploitation of the ADVANCE results as outlined in ADVANCE Deliverable D6.8 [6].

References

[1] Case Study in Railway Domain. ADVANCE project. Deliverable D1.1 – Workpackage 1. September 25th 2012.

[2] Proof of Concept Application in Railway Domain. ADVANCE project. Deliverable D1.2 – Workpackage 1. September 25th 2012.

[3] Intermediate Report on Application in Railway Domain. ADVANCE project. Deliverable D1.3 – Workpackage 1. October 21st 2013.

[4] Final Report On Application On Railway Domain. ADVANCE project. Deliverable D1.4 – Workpackage 1. November 30th 2014.

[5] ADVANCE Process Integration III. ADVANCE project. Deliverable D5.3 – Workpackage 5. November 30th 2014.

[6] Plan to Disseminate and Use Foreground Knowledge. ADVANCE project. Deliverable D6.8 – Workpackage 6. November 30th 2014.

[7] CENELEC Standard EN 50126: Railway applications — The specification and demonstration of Reliability Availability, Maintainability and Safety (RAMS); 1999.

[8] CENELEC Standard EN 50128: Railway applications — Communication, signalling and processing systems -Software for railway control and protection systems; October 2011.

[9] CENELEC Standard EN 50129: Railway applications — Communication, signalling and processing systems —Safety related electronic systems for signalling. February 2003.

[10] Constraints of the certification process. D1.1, OpenCoss: Open Platform for the Evolutionary Certification of Safety-critical systems, 28 March 2012. EC 7th Framework Programme.