openETCS/WP4/D4.5.1

ITEA2 Project
2012 – 2015

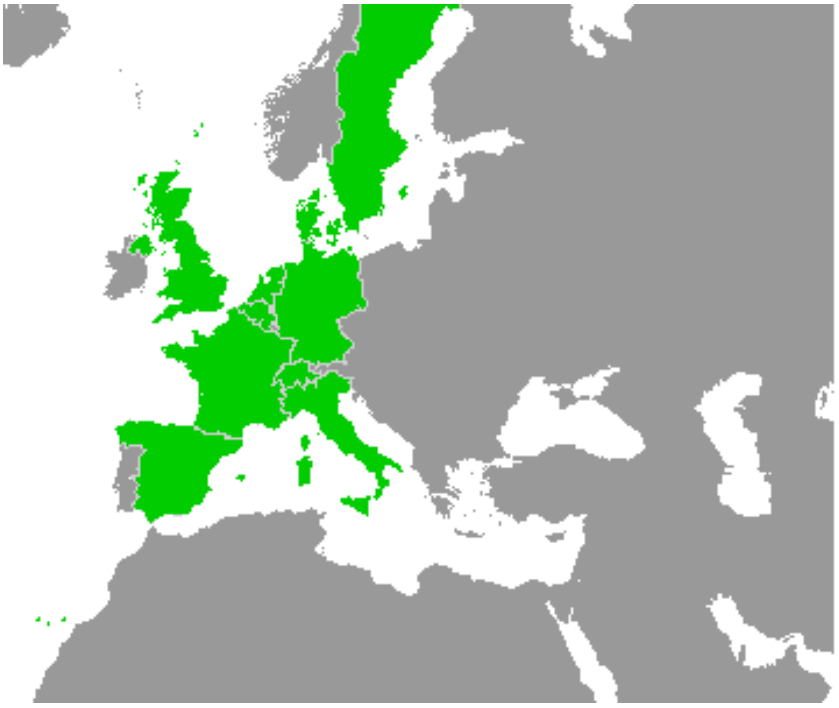
Work-Package 4: "V&V Strategy"

openETCS D4.5.1: OpenETCS Internal Assessment Plan

Planning and Description of tasks that are performed within Internal Assessment Activities in the Open ETCS project

Cyril Cornu (All4tec)

February 2013



openETCS

openETCS D4.5.1: OpenETCS Internal Assessment Plan

Planning and Description of tasks that are performed within Internal Assessment Activities in the Open ETCS project

Cyril Cornu (All4tec)

All4tec
2-12, Rue du Chemin des femmes
91 300 MASSY
France

Preliminary Report draft version

Prepared for ITEA2 openETCS consortium
Europa

Abstract: The Internal Assessment Plan describes the Internal Assessment strategy and plan in the Framework of Safety, Quality and V&V activities in the Open ETCS project. The assessment is a P̈rocess of analysis to determine whether software, which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements, and to form a judgment whether the software is fit for its intended purpose.¨
The dates, highlights, deliverables and activities split is willing to be changed in accordance with the FPP final version.

Table of Contents

Introduction ..... **iv**

0.1 project context iv
0.2 Internal Assessment Plan objectives v

Project Quality Assessment ..... **vi**

0.3 Quality Assurance Plan - QAP vi
0.4 Project Deliverables compliance with QAP vi
0.5 The Management and Responsibilities management vii
0.6 Quality Log and Traceability vii

V&V Activities Assessment ..... **ix**

0.7 V&V Plan ix
0.8 Verification and Testing Activities ix
0.9 Validation Activities x
0.10 V&V log and traceability for Model x
0.11 V&V log and traceability for Code x

Safety Activities Assessment ..... **xi**

0.12 Safety Evaluation Criteria xi
0.13 Safety Requirements Traceability xi
0.14 Semi-Formal and Formal Models xi

Internal assessment activities planing ..... **xii**

Conclusion ..... **xiii**

Introduction

The role of the Assessor is to perform an assessment of the software developed during the project OpenETCS. An assessment is a Ṗrocess of analysis to determine whether software, which may include process, documentation, system, subsystem hardware and/or software components, meets the specified requirements, and to form a judgment whether the software is fit for its intended purpose.˙
According to the standard EN 50128 and the software safety integrity level (SIL4) of the project, it is very important to remind that the Assessor shall be independent from the project and shall be given authority to perform the software assessment. Then, the Assessor shall not be part of project stakeholders, and is totally independent from the project teams. Furthermore, the Assessor shall have the knowledge of the both ERTMS and ETCS, of the dependability and of the standard EN 50128, even if only ETCS EVC Software part in the project scope.
For these reasons, the need of an internal assessment has been identified at the beginning of the project. This activity would simulate a real external assessment process, that would be enhanced by people part of the Open ETCS project, and responding to the 2 main skills conditions to perform such a task: the technical knowledge on the ETCS OBU and the technical independency regarding the whole Software development and project activities.

0.1 project context

The aim of the internal assessment is to simulate a real assessor activity regarding a standard Railway signaling system design and production by a railway company. The Open ETCS project main objectives are:

- Transformation of higher-level, informal (i.e. expressed in natural language) ETCS requirements in formal and semi-formal requirements that will be used for validation and verification activities of embedded control systems.
- Adaptation of modelling languages such that train control systems can be designed in suitable formalisms and verified against ETCS requirements in early design phases.
- Integrating and developing formal and semi-formal validation and verification techniques in order to prove the correctness of train control systems against formalized ETCS requirements.
- Generating symbiotic effects of large companies, R&D institutes, and SMEs in order to bring together all relevant experts in the field taking advantage from their diverse knowledge within a value adding chain (so called âĂIJeco-systemâĂİ or âĂIJCo-CompetitionâĂİ).

These four objectives are all related to specific steps of an On Board Unit Software design and development (European Vital Computer). Moreover, they all encompass underneath performance, reliability, availability, maintainability and safety objectives, that are usually translated into a Safety Integrity Level (SIL), and the conditions regarding quality, process and overall development activities are gathered in the CENELEC standards EN50128, EN20126 and EN50129. Therefore, apply the common development strategy for such a railway system makes sense, and allows the project to base the whole OBU EVC Software development on existing CENELEC standards for such Railway signaling systems allows us to meet these both conditions on design process and Safety Level.

0.2 Internal Assessment Plan objectives

This document provides the overall assessment plan and objectives that will be followed in the frame of internal assessment activities. The activities are shared according to the main software development categories they deal with:

- Quality insurance
- Verification & Validation
- Safety

For each assessment activities, this assessment plan will identify the relevant deliverables, and the criteria that will be especially considered during the assessment phase.

As the project deliverables will be issued simultaneously whatever the category they belong to, the internal assessment activity will be performed at precise time

Project Quality Assessment

This chapter details what are the main features to be checked regarding the quality insurance regarding the whole Open ETCS activities, from the very beginning of the project to the end of it. The Safety Criteria are defined in the document D2.2 appendix B3, and these criteria will be checked during the Internal Assessment review. The main points to be assessed are:

- The Quality Assurance Plan completeness
- The Project Deliverables compliance with QAP
- The Management and Responsibilities management

0.3 Quality Assurance Plan - QAP

The purpose of the QA Plan is to define the processes, methods and tools that will be used to develop the OpenETCS project meeting ITEA requirements, following Open Source principles and practices and applying the SCRUM Methodology. Besides, two of the project outcomes, the OpenETCS software, the OpenETCS Tool Chain, will have to comply with CENELEC requirements.

The following parts of the QAP will be precisely checked by the assessor, whether they belong to the QAP document or to another document.

- Open ETCS development process. This process describes the whole documentation to be issued in the framework of Open ETCS project, and the connexions between the project inputs, the project outcomes, and the work packages and tasks identified in the project. The coherency between the IO documents and informations identified in the development process and the related document content will be checked.
- Open ETCS tool development process. This process has to be described as precisely as the Quality Assurance related to the OBU EVC Software development activity. The same verifications and assessments activities will be performed on this process than on the software development process.
- Configuration Management Plan. The
- Review Process
- Project Development Process

0.4 Project Deliverables compliance with QAP

The Safety Criteria are defined in the document D2.2, and these criteria will be checked during the Internal Assessment review. The main points to be assessed for the project deliverables are:

- the documentation compliance for Software Safety Integrity Level 4. This includes a functional and interface description of the system, the application conditions, the configuration or architecture of the system, the hazards to be controlled, the safety integrity requirements, the SIL allocation to Software and Hardware, and the timing constraints.

- the Requirements for tools class T1, T2 and T3. Tools have been identified so far for each category (text editor, requirements support, configuration support tool for T1, static code analysers, model checkers, model based testing tools, simulators for T2, and compilers or code generation tools for T3), and all proof of compliance with the CENELEC standard and justification for use will be check within internal assessment activities.

0.5 The Management and Responsibilities management

The Quality Assurance in Open ETCS has to claim the proof that all people involved in project has the sufficient skills and competencies to fulfill their responsibilities. All these competencies have to be gathered and tracked whether in the QAP or in a separate quality related document that has to be identified in the QAP. According to the CENELEC EN50128, the 10 software development key roles to be identified are:

- the Requirements Manager,
- the Designer,
- the Implementer,
- the Tester,
- the Verifier,
- the Integrator,
- the Validator,
- the Project Manager,
- the Configuration Manager.

The information needed in Quality Assurance documentation is:

- The Actual Competencies Matrix of each committer in the project, linked to the work packages and the tasks they are involved in.
- The Needed Competencies Matrix for each task, document and project outcomes. Each people contribution as to be as detailed as possible (at least the contribution to a precise task or outcome).
- From the gab identified between the both actual competencies matrix and required competencies matrix, a Training plan has to be set up for all the commiters of the Open ETCS project. This plan will have to track all the identified needs, and then the solutions chosen in order to harmonize the competencies needs and the committers skills (training session, re-organization,

0.6 Quality Log and Traceability

In the framework of Asessment activities, all discrepancies related to Quality Assurance whatever the level considered, will be gathered in a table called the Quality Log. This log will be used by the Assessor as a list of possible or required improvements, to be used as a road map in order to get rid of all quality assurance concerns or discrepancies identified during the whole project life cycle. The Quality Log table will encompass the following information:

- Number of the log row
- Document/ Outcome concerned and precise discrepancy localization
- Document/ Outcome version
- Date
- Discrepancy description by assessor, and comments (assessor, author or else)
- Action planned to fix (commonly defined by at least the document author and the assessor)
- Action Deadline
- Status of the log (fixed, under investigation...)

V&V Activities Assessment

This chapter details what are the main features to be checked regarding the V&V activities regarding the whole Open ETCS software development activities, from the very beginning of the project to the end of it. The Quality Criteria regarding V&V activities are defined in the document D2.2 appendix B4, and these criteria will be checked during the Internal Assessment review. The main points to be assessed are:

- V&V Plan
- Verification & Validation activities for Model
- Verification & Validation activities for Primary Toolchain
- Verification & Validation activities for Code
- Safety

0.7 V&V Plan

The purpose of the V&V Plan is to define, describe and plan the verification and validation activities in the project openETCS. As the goals of the project include the selection, adaption and construction of methods and tools for a FLOSS development in addition to performing actual development steps, the V&V plan will deal separately with these two aspects. The Verification Plan for the model should describe the selection of verification strategies and techniques to be applied to the Open ETCS for Testing the Open ETCS Semi-Formal Model and Formal Model. The set of techniques, the definition of the process for test creation, test coverage and completeness, and roles in the testing team will be assessed in the same way than for the Quality Assurance Aspects. The Verification Plan for the tool is based on the same principle than for the Model Assessment, but related to the tool or the whole toolchain. The Assessment will focus on quality assurance and traceability of the verification.

The Validation Plan aims to give a frame to Validation activities to be performed within OpenETCS project. It aims at determining whether the developed tool fits the user needs, in particular with respect to safety and quality relatively to the environment it will be run it.

0.8 Verification and Testing Activities

The First aspect is related to the Verification activities. The Assessment for Verification will mainly concern the following points:

- Test Specifications. The Test Specifications will have to fulfill the CENELEC requirements regarding the tests objectives, the precise content of the test in terms of environment handling, data and expected results. Their coherency with the test policy will be checked and assessed.
- Test Reports. The test report will have to report as precisely as possible the information related to the test performance. The tests results are compared with the expected results defined during the test specification, failures have to be recorded, described and then investigated. The test environment such as Tester names and test conditions have to be clearly described as well.

0.9 Validation Activities

The second aspect is related to the Validation Activities. The Assessment for Validation will mainly concern the following points:

- The creation of a Validation Plan in order to give a frame

0.10 V&V log and traceability for Model

The V&V activities can be split in testing activities and verification activities. The testing activities aim at verifying the Model behavior and performances against the corresponding system and software specification, in order to achieve the capability, maintainability, portability, functionality, reliability and usability objectives for the OBU EVC Kernel Software Model. For each test, a Test Specification has to be issued and will have to fulfill the CENELEC requirements regarding the tests objectives, the precise content of the test in terms of environment handling, data and expected results. Their coherency with the test policy will be checked and assessed. At the end of the test, a test report is then created. The coherency between the Test specification and the Test

0.11 V&V log and traceability for Code

Safety Activities Assessment

0.12 Safety Evaluation Criteria

0.13 Safety Requirements Traceability

0.14 Semi-Formal and Formal Models

Internal assessment activities planing

Conclusion