

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 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

This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.



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 Process 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.

Disclaimer: This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE ("CCPL" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS LICENSE OR COPYRIGHT LAW IS PROHIBITED.

BY EXERCISING ANY RIGHTS TO THE WORK PROVIDED HERE, YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS LICENSE. TO THE EXTENT THIS LICENSE MAY BE CONSIDERED TO BE A CONTRACT, THE LICENSOR GRANTS YOU THE RIGHTS CONTAINED HERE IN CONSIDERATION OF YOUR ACCEPTANCE OF SUCH TERMS AND CONDITIONS.

<http://creativecommons.org/licenses/by-sa/3.0/>

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 Compliance of project deliverables with QAP	vi
0.5 Quality Log and Traceability	vi
V&V Activities Assessment	vii
0.6 V&V Plan	vii
0.7 Compliance of project deliverables with V&V Plan	vii
0.8 V&V log and traceability for Model	vii
0.9 V&V log and traceability for Code	vii
Safety Activities Assessment	viii
0.10 Safety Evaluation Criteria	viii
0.11 Safety Requirements Traceability	viii
0.12 Semi-Formal and Formal Models	viii
Internal assessment activities planing	ix
Conclusion	x

Introduction

The role of the Assessor is to perform an assessment of the software developed during the project OpenETCS. An assessment is a Process 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 "Jeco-system" or "JCo-Competition").

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 software development activities, from the very beginning of the project to the end of it

0.3 Quality Assurance Plan - QAP

Quality Assurance Plan Configuration Management Plan Competencies Matrix Review Process
Project Development Process

0.4 Compliance of project deliverables with QAP

0.5 Quality Log and Traceability

V&V Activities Assessment

0.6 V&V Plan

0.7 Compliance of project deliverables with V&V Plan

0.8 V&V log and traceability for Model

0.9 V&V log and traceability for Code

Safety Activities Assessment

0.10 Safety Evaluation Criteria

0.11 Safety Requirements Traceability

0.12 Semi-Formal and Formal Models

Internal assessment activities planing

Conclusion