openETCS/WP4/D4.x

openETCS
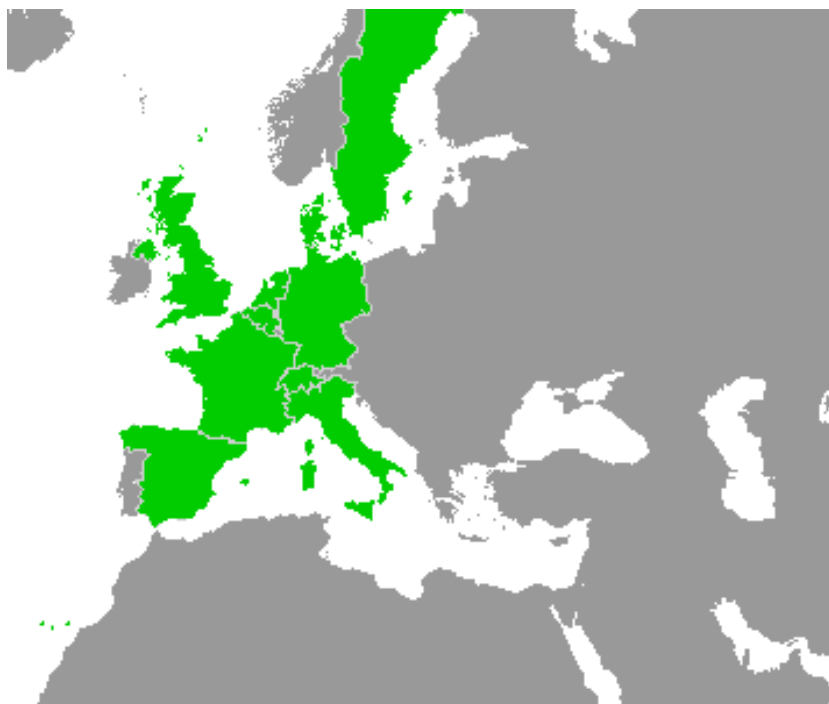
Work-Package 4: "V&V Strategy"

openETCS D4.x: OpenETCS Suggestion Assessor tasks

Set of Suggestions regarding Assessor's activities during Open ETCS Software development

Anne-Catherine Vie (All4tec), Cyril Cornu (All4tec) and Merlin Pokam (AEbt)

February 2013

openETCS D4.x: OpenETCS Suggestion Assessor tasks

Set of Suggestions regarding Assessor's activities during Open ETCS Software development

Anne-Catherine Vie (All4tec), Cyril Cornu (All4tec) and Merlin Pokam (AEbt)

AEbt Angewandte Eisenbahntechnik GmbH
Adam-Klein-Straße 26
90429 Nürnberg
Germany

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

Preliminary Report

Prepared for   ITEA2 openETCS consortium
Europa

Abstract: This note is a set of suggestions regarding the Assessor tasks. These tasks shall be performed during the software development process of the project OpenETCS.

Table of Contents

Role of the Assessor

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. Safety assessment is focused on but not limited to the safety properties of a system.˙. The last sentence explains the fact that the safety properties of the software to be developed are a major concern of the assessment, but the overall quality and process aspects of the software development are totally concerned as well by assessment activities.

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 is not part of project stakeholders and is totally independent from the project teams (The project considered here is not the Open ETCS project, but the Software development. Therefore, a company part of the whole Open ETCS project, but not involved in the software development, could provide an assessor, at the moment he respects the both previous conditions).

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 iin the project scope.

The assessor roles are described in the CENELEC EN50128 standard in following paragraphs: §6.4.4.8, §6.4.4.9, §6.4.4.10, §6.4.4.11, §6.4.4.12, §6.4.4.13, §6.4.4.14 and §6.4.4.15.

Assessor Tasks in the development process

The Assessor shall write a Software Assessment Plan. It is like an assessment process which is linked to the software development process. More precisely, he shall explain the tasks needed to assess the software of the project OpenETCS.

Note: The Verifier shall write a Software Assessment Verification Report, as required in the standard EN50128, to verify in the first time that the Software Assessment Plan meets the general requirements for readability and traceability.

During the software development, he shall evaluate the software verification and validation activities. We propose that the Assessor intervenes at least seven times during the software development process (this is equivalent to one time at least by Work Product).

Note: the numbers of WPs are not given in the chronological order, e.g. WP1 is performed during all the development process and WP5 occurs before the end of WP4.

During WP1: Project Management.

The Assessor is able to assess:

- The Quality Assurance
- The capability of the Project Manager and the quality of his deliverables

The Assessor shall assess the Software Quality Plan. We propose that he gives a formal approval of this document.

During WP2: Requirements for Open Proof.

The Assessor is able to assess:

- The System requirements specification, including:
    - functions and interfaces;
    - application conditions;
    - configuration or architecture of the system;
    - hazards to be controlled;
    - safety integrity requirements;
    - apportionment of requirements and allocation of SIL to software and hardware;
    - timing constraints
- The software requirements specification,
- The software architecture and design specification,
- The software component specification,
- The personnel key roles, responsibilities and competence,

- The Quality Assurance

Nevertheless, he shall assess the implementation of both activities and deliverables of WP 2.

During WP3: Modeling of (part of) ETCS specification.

The Assessor shall evaluate the software implementation respectively the software modeling. Furthermore, he is able to assess:

- A part of the lifecycle and the documentation,
- The Quality Assurance,
- The personnel roles and responsibilities and competence.

The Assessor shall assess the implementation of both activities and deliverables of WP 3.

During WP4: Validation & Verification Strategy.

The Assessor shall assess:

- the Software Verification Plan and the Software Validation Plan,
- the Quality Assurance.

We propose that he gives a formal approval on these documents. He shall mainly evaluate the verification activities and the implementation of both activities and deliverables of the WP 4.

During WP5: Demonstrator.

The Assessor shall assess the specific openETCS software. Indeed, before the beginning of the validation activity (WP4), the Assessor shall assess the Software Integration Test Report to give or not the approval for software validation. This point is the Validation first step (the previous steps are related to the verification).

During WP6: Dissemination, Exploitation and Standardization.

The Assessor shall verify that the software maintenance plan is written and compliant with the software safety integrity level (SIL4).

During WP7: Language, ToolChain and Opensource Ecosystem.

The Assessor shall assess the developed tool chain according to Tool class T3 of EN 50128:2011. The other tools (T2) have to be assessed as well, but the effort is liter regarding the T3 assessment effort.

At the end of the software development process, the Assessor shall perform a final assessment. Indeed, he shall evaluate that the lifecycle processes and products resulting are such that the software is of the defined software safety integrity level and fits for its intended application. All the steps of assessment performed during the software development process shall be gathered in the Software Assessment Report. This report could be updated all along the process.

Note: the Software Assessment Verification Report permit to verify the internal consistency of the Software Assessment Report.

Conclusion

This note is also a preliminary document which can be used **to elaborate the Software Assessment Plan**, as required by the standard EN 50128:2011.

It can be also used to perform an âĂIJinternalâĂİ assessment (within the WP4 for instance) during the software development.