Independent Assessment

according to the standard EN 50128:2011

Table of contents

1 Information about the Contract

1.1 Customer\ Organization\ Authority

o OpenETCS project

1.2 Assessor\Contractor

Frédérique Vallée
All4tec
Immeuble Odyssée Bâtiment E
2-12 Rue du Chemin des femmes
91300 MASSY
FRANCE

Norbert Schäfer
AEbt Angewandte Eisenbahntechnik GmbH
Adam-Klein-Straße 26
90429 Nuremberg
Germany
Accredited assessor according to EN 17020

Contact:

Norbert Schäfer	Norbert.Schaefer@aebt.de +49 911 520992 - 13
Frédérique Vallée	Frederique.Vallee@all4tec.net +33 (0)1 78 85 81 43

1.3 About the contract

Suggestion:

- Description of the openETCS organization
- Mention that:

o the openETCS SW is vendor independent (Normally an Assessment for SW and SW development process is done after getting an order from a specific manufacturer\Producer)

o the Safety Integrity Level of the developed SW is SIL4 and therefore an expert assessment is to be prepared in accordance with EN 50128:2011 for SIL 4

- Frédérique Vallée (All4tec) and Norbert Schäfer (AEbt) have been tasked with the independent expert assessment of the software and of the software development process of the openETCS.

2 General

2.1 Glossary\List of Abbreviations

- Glossary from the openETCS template
- Additional Abbreviations for the Assessment

2.2 Referenced standards, guidelines and directives

- References from the openETCS template

Document	Date
Example: EN 50128 Railway applications - Communications, signaling and processing systems - Software for railway control and protection systems	2011

3 Introduction

3.1 Initial situation

- In this subchapter a briefed description of the openETCS as a system should be presented.

o Hier a top level of the system architecture can be shown (Figure 2 of the ADD document)

o Mention that the ETCS OBU (marked within the red dashed area) is the highest level taken into consideration for the Assessment

3.2 Scope of the assessment

- openETCS deliverables
- openETCS Kernel
- openETCS SW and the SW development (including openETCS Tool-Chain?)

- Suggestion:

o Hier the second level of the system architecture can be shown (Figure 4 of the ADD document) distinguishing between the ETCS OBU and the ETCS kernel.

3.3 Contents of the assessment and issues of concern

The purpose of this assessment is to answer the following questions relating to software development:

1. What measures have been taken to satisfy EN 50128?
2. Are the measures taken for satisfying EN 50128 SIL 4 sufficient?

3.4 Assessment conditions and exceptions

- What are the exceptions here? (I.e. HW-Integration is out of scope)
  - A grooming is needed here.

3.5 Documents for the software life cycle and software creation

- Table of the mapped deliverables to CENELEC EN50128 life-cycle should be included here.
  - It shall be mentioned:

o The following documents, which describe the software creation process, have been made available to the expert assessor.

4 Expert assessment

4.1 Process

4.1.1 Assessment process

- The openETCS documents from the development process should be made available to the assessor. All documents should be submitted and needs to be reviewed for content and form by the assessor as well as reflected and evaluated in the project life cycle and CENELEC standard EN 50128. The results should continually be relayed to the responsible entities within the WPs.
  - Due to the agile workflow in the openETCS project this assessment process should be done iteratively.

4.1.2 Review of Planning Documents

- The planning documents for quality assurance (software quality assurance plan, software verification plan, software validation plan, software coding standards, software configuration management plan and software maintenance plan) should be reviewed for changes. Also the deliverables should be reviewed for plausibility and compliance with standards.
  - The unresolved issues of the deliverables review shall be discussed.
  - Measures shall be defined.
  - A review report needs to be created

4.1.3 Initial Assessment

- Here a brief description of the start date of the Assessment process as it is described in the Assessment Plan.

4.2 Sections assessed

- Here the assessed sections of the life-cycle of the SW development EN 50128 should be presented.
  - Suggestion:

o Table with sections of the SW life-cycle and a column with Yes/No Statement

5 Answers to Questions

Here a brief description to this chapter (three aspects of Assessment see. AssPlan)

5.1 Project Quality Assessment

5.1.1 Goals, conformity and SIL [EN 50128 Section 4] PQ

Goal: allocating the safety related system functions to openETCS SW, as well as SW APIs shall be identified in the system documentation. Also the SW-SIL shall be specified here.

Assessment:

5.1.2 Personnel and responsibility [EN 50128 section 5.1 and 5.2] PQ

Goal: Ensure that all the staff members are accountable for the software, are organized, competent and capable of exercising this responsibility.

Assessment:

5.1.3 Life cycle and documentation [EN 50128 section 5.3] PQ

Goal: Organization of the software development into set phases and activities as well as registration of all the information used for the software throughout the entire life cycle of the software.

Assessment:

5.1.4 Software quality assurance [EN 50128 section 6.5] PQ

Goal: Identification, monitoring and controlling of all technical and management activities that are necessary in order to ensure that the software attains the required quality. This is necessary to guarantee the required qualitative defense against systematic faults and to ensure that an audit can be set up to make it possible to efficiently take verification and validation measures.

Assessment:

The description of the process of configuration management (above list) is not described in enough detail and is to be improved.

5.1.5 Changes and change management [EN 50128 sect. 6.6] PQ

Goal: Ensure that the software functions as required and that the software safety requirement and reliability is retained upon modification of the software.

Assessment:

5.2 V&V Assessment

5.2.1 Software test [EN 50128 sect. 6.1] V&V

The goal of the software test is to check the behavior or performance of the software.

Assessment:

5.2.2 Software verification [EN 50128 sect. 6.2] V&V

The goal of the software verification is the investigation and evaluation based on demonstrating that the results of a certain development phase are sufficient.

Assessment:

5.2.3 Software validation [EN 50128 sect. 6.3] V&V

The goal of the software validation is to demonstrate that the processes and output variables of the software comply with the set SIL, satisfy the software requirements and are suitable for the intended application. The main validation activities consist of analysis and/or testing and evaluation of the safety criticality of all the faults and deficiencies.

Assessment:

5.2.4 Software implementation and test (EN 50128 sect. 7.5) V&V

Goal: Creation of software that is analyzable, testable, verifiable and repairable. This phase also covers component tests.

Assessment:

5.2.5 Software integration (EN 50128 sect. 7.6) V&V

Goal: Execution of the software integration and software/hardware integration. Demonstration that the software and the hardware properly work together to perform their intended functions.

Assessment:

5.3 Safety Activities Assessment

5.3.1 Software assessment [EN 50128 sect. 6.4] SA

Goal: Evaluation of the process of the life cycle and the products arising from it allow the conclusion that the software exhibits the set SIL 1 to 4 and is suitable for it intended use.

Assessment:

5.3.2 Supporting tools and languages [EN 50128 sect. 6.7] SA

Goal: Software tools must be appropriately selected for the software development process, the tools should be able to work together, the use of tools in classes T2 and T3 must be justified and for T3 proof of suitability must be present.

Assessment:

5.3.3 Software requirement (EN 50128 sect. 7.2) SA

Goal: Description of a complete set of requirements for the software that satisfies all the system and safety requirements and provides an extensive set of documents for each later phase.

Assessment:

5.3.4 Software architecture and design (EN 50128 sect. 7.3) SA

Goal: Development of a software architecture. Identify and evaluate what the interaction between hardware and software means for safety. Selection of a design process. Design of the software of a defined SIL. Ensure that the resulting system and its software can easily be tested from the outset.

Assessment:

5.3.5 Software components design (EN 50128 sect. 7.4) SA

Goal: development of a software component design and software component test specifications, with which the requirements of the software design specifications are satisfied to the extent required by the SIL.

Assessment:

5.3.6 Overall software test [EN 50128 sect. 7.7] SA

Analysis and test of the integrated SW and HW in order to ensure accordance with the software requirement specifications, especially the functional and safety aspects as per the SIL.

Assessment:

5.3.7 Application data or algorithms – systems configured by application data or algorithms [EN 50128 sect. 8] SA

Assessment:

5.3.8 Deployment of the software [EN 50128 sect. 9.1] SA

Goal: Ensure that the software works as intended, adheres to the required SIL and reliability when it is deployed in the final environment of application

Assessment:

5.3.9 Maintenance of the software [EN 50128 sect. 9.2] PQ or SA

Goal: Verification that the software functions as required and the obligatory SIL and reliability are maintained if corrections, extensions or adjustments are performed on the software.

Assessment:

5.4 Answer to the question: Are the measures taken for satisfying EN 50128 SIL 4 sufficient?

Answer to the above question

5.5 OTHER Question?

- E.g.: Agile development in openETCS and its conformity to the EN 50128
  - ....

6 Summary

7 Tasks, recommendations and notes

- Should this section be described in a new deliverable "**Recommendation for the Assessment**"?

8 Finalization

Nuremberg, xx.xx.2015

Expert assessor
Norbert Schäfer

Expert assessor
Frédérique Vallée