openETCS/WP4/D4.5

ITEA2 Project
Call 6 11025
2012 – 2015

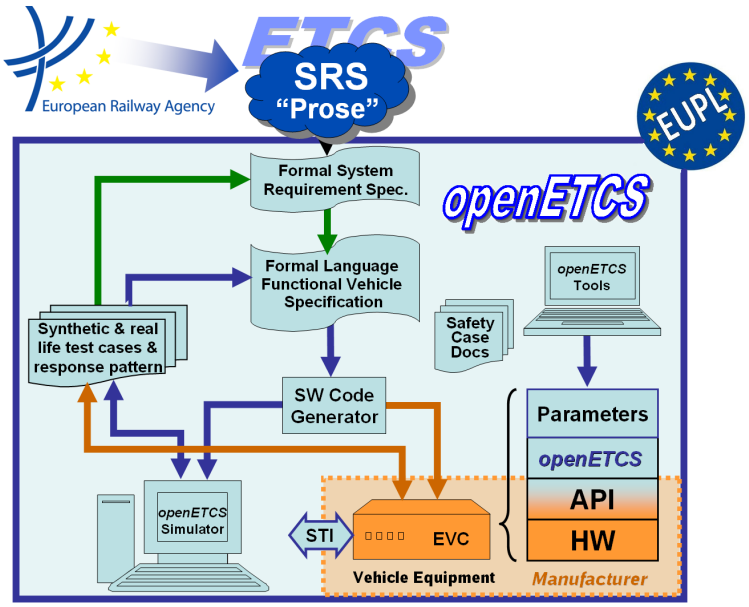
Work-Package 4: "V&V Strategy"

openETCS D4.5: Draft Assessment Report

Independent Assessment according to the standard EN 50128:2011

Frédérique Vallée and Norbert Schäfer

December 2015



Funded by:

Federal Ministry of Education and Research
Région de Bruxelles-Capitale
GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

openETCS

This page is intentionally left blank

Work-Package 4: "V&V Strategy" **openETCS/WP4/D4.5**
December 2015

openETCS D4.5: Draft Assessment Report

Independent Assessment according to the standard EN 50128:2011

Document approbation

Lead author:	Technical assessor:	Quality assessor:	Project lead:
location / date	location / date	location / date	location / date
signature Frédérique Vallée (All4tec)	signature Norbert Schäfer (AEbt)	signature Marc Behrens (DLR)	signature Klaus-Rüdiger Hase (DB Netz)

Frédérique Vallée

All4tec
Immeuble Odyssée Bâtiment E
2-12, rue du Chemin des femmes
91 300 MASSY
France

Norbert Schäfer

AEbt Angewandte Eisenbahntechnik GmbH
Adam-Klein-Str. 26
90429 Nürnberg
Germany

final version

Prepared for openETCS@ITEA2 Project

Abstract: The Assessment Report describes the Assessmentresults in the frame of V&V activities in the openETCS [2] project. According to the CENELEC EN50128:2011 [1] standard, 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 as to whether the software is fit for its intended purpose.¨

Modification History

Version	Section	Modification / Description	Author
0.1	all	template of 1st version	Abdelnasir Mohamed
0.2	all	entering assessment result of ADD document	Frédérique Vallée
0.3	all	conversion to LaTeX	Marc Behrens

Table of Contents

List of Tables

1 Information about the Contract

1.1 Customer\ Organization\ Authority

The customer of the assessment is the OpenETCS project represented by the project leader:

Klaus Rüdiger Hase
Project Leader openETCS
DB Netz AG
Völckerstrasse 5
80939 München, GERMANY

1.2 Assessor\Contractor

Frédérique Vallée

All4tec
Immeuble Odyssée Bâtiment E
2-12, rue du Chemin des femmes
91 300 MASSY
France

Norbert Schäfer

AEbt Angewandte Eisenbahntechnik GmbH
Adam-Klein-Str. 26
90429 Nürnberg
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

The openETCS organization consists of the openETCS consortium [2] as being initiated by the ITEA2 labelled project [3].

The Assessment is performed on the generic, vendor independent openETCS Software. Normally an Assessment for SW and SW development process is done after getting an order from a specific manufacturer\Producer, in this case the customer of the Assessment is the openETCS Consortium itself.

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

ETCS	European Train Control System
ERA	European Railway Agency
EVC	European Vital Computer
FMEA	Failure Mode Effect Analysis
SIL	Safety Integrity Level
SRS	System Requirement Specification
V&V	Verification & Validation

Table 1. Assessment Glossary

2.2 Referenced standards, guidelines and directives

• References from the openETCS template

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

Table 2. Referenced Documents

3 Introduction

3.1 Initial situation

The openETCS project has the goal to develop a semi-formal followed by a strictly formal OBU model realizing functionalities of the UNISIG SRS-SUBSET-026, baseline 3, required for running on the ETCS level 2 of the Utrecht-Amsterdam track. The purpose of this formal model is to increase and spread consistent understanding of the subset, where it can be used as an artifact for testing, analyzing, verification and validation and also for further development purposes by industrial actors. This shall be achieved within a framework that is based on an open source concept. The ETCS On Board Unit EVC software model depicted in Figure 1 will be the focus of the software assessment according to the EN 50128:2011.

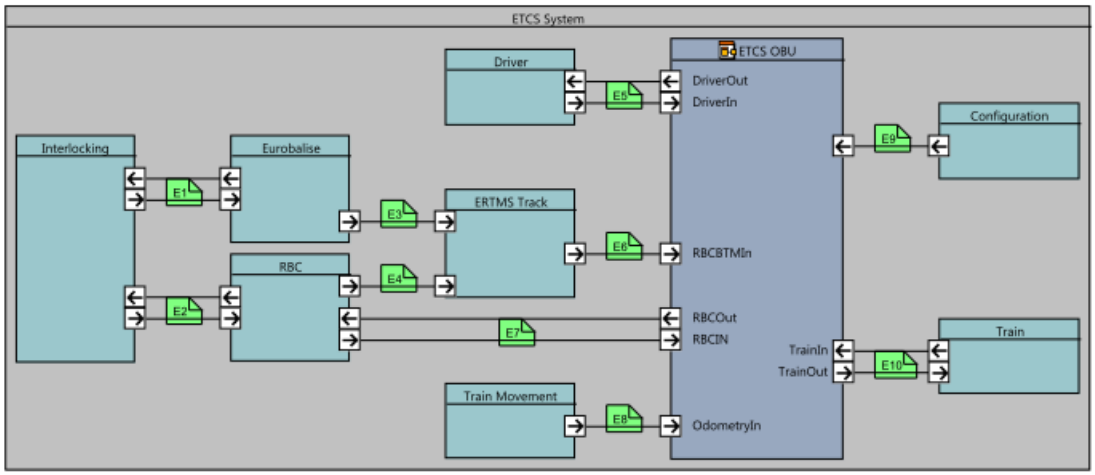


Figure 1: Top level architecture view of the ETCS OBU

3.2 Scope of the assessment

The scope of the assessment will cover three main categories of the openETCS software development. These are:

- Project and Software Quality assurance
- Verification & Validation and
- Safety

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. Does the agile development methodology applied in this project affects these measures taken for satisfying EN 50128?

3.4 Assessment conditions and exceptions

It should be noted:
– The ETCS OBU software model has been developed with the closed source SCADE Suite of the company Systerel and the code generated is SIL4 certified. Hence only the deliverables of the openETCS Tool chain will have the scope of the assessment.
– HW-Integration is out of the scope of the assessment

3.5 Documents for the software life cycle and software creation

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

Mapping_openETCS_Deliverables_To_EN50128-2011Docs

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:

- 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.
We have examined the document D1.3.1 "*Project Quality Assurance Plan*".
ASS512.1

The openETCS organization consists of seven work packages (WP1 to WP7) where each WP has its own WP-Leader and team members who shall fulfill the roles and their independency required in the EN 50128:2011. The following image shows the minimum requirements for the independence of the assessor as well as that between the members of the project team.

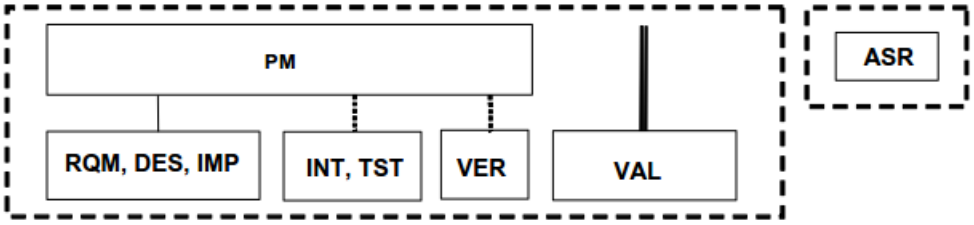


Figure 2: Preferred organizational structure for SIL 4 SW-Development
WP-Leader 1 (WPL1) is the project manager of the whole project. For the actual development three WPLs have an equivalent role to that of a project manager depicted in Figure 1. Other roles are distributed within the different WPs depending on their tasks and goals.

EN 50128:2011 Role	Person	WP (Entity)
Project manager of all WPs	Mr. Dr. Hase (DB)	WP1
WPLs as Project manager	Mr. Cochetti (Alstom)	WP3
	Mr. Behrens (DLR)	WP4
	Mr. Deutsch (ERSA)	WP5
	Mr. Jastram (Formal Mind)	WP7

Table 1 Work package Leaders as project manager

Assessment:
For the targeted SIL4 the roles were chosen appropriately within the openETCS organization. There are seven WPLs where the WPL1 is also the leader of all WPLs. The Assessors have examined the independencies of the roles within the openETCS organization and came to following conclusions:

– Although the validator belongs organizationally to WP4 he is an independent entity in the openETCS project and does not underlie the WPL1, WPL3, WPL5 nor WPL7.
– The verifiers are not the same persons as the entities integrator, Tester, requirements manager, designer nor implementer
– The independency of the rest of the entities are guaranteed according to Figure 1.
Due to the fact that every project partner is EN ISO 90001 certified in addition to the many technical discussions the assessors had held with the WPLs or the many attended openETCS Scrum meetings the assessors can confirm the competences of the WPLs and their team, which are listed in the competence matrix in the QAP.
The training and qualification of the project participants is also sufficient for the tasks to be implemented. For example a SCADE Suite training is held for all partners using the SCADE Suite software tool in 2014.
This requirement is fulfilled.

5.1.3 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 5.1.4 Software quality assurance [EN 50128 section 6.5]* PQ

(*): other EN 5018 parts to be examined here = *sections 7.3.4.25 to 7.3.4.27 related to coding standards.*
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

(*): other EN 5018 parts to be examined here = section 7.3.4.33 (software component test specification) and sections 7.3.4.29 to 7.3.4.40 (software integration and software/hardware integration specifications)
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

(*): other EN 5018 parts to be examined here = sections 7.3.4.41 to 7.3.4.43 (software architecture and design verification).

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 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.
We have examined the document: D3.5.3 “openETCS Architecture and Design Specification”.
Notice that the section 7.3 of EN 50128 covers not only architecture, interface and design specifications but also test specification for software component test, software integration and software/hardware integration. These elements are not covered by D3.5.3. So section 7.3.4.33 and sections 7.3.4.29 to 7.3.4.40 have been transferred to & 5.2.1 of this document. For the same reason, sections 7.3.4.41 to 7.3.4.43 dealing with verification have been transferred to & 5.2.2 of this document, and sections 7.3.4.25 to 7.3.4.27 related to coding standards have been transferred to & 5.1.4 of this document.

ASS534.1

Considering the safety aspects we have some doubt about the robustness of the proposed design. Theoretically the following fields “Behaviour when value is at boundary / Behaviour for values out of valid range / Behaviour when value is erroneous, absent or unwanted”, given for all inputs should explain which safety mechanisms have been implemented and how they work . Numerous remarks can be done on these fields:

• Sometimes the behavior in case of “erroneous data” is considered as identical to the behavior in case of “data at the boundary” which is not acceptable (see for example 5.2.2.1.3 ActualOdometry; 5.2.2.1.11 inSupervisingRbcId . . .).

• Sometimes the behavior in case of “erroneous data” could result in a hazard but no safety mechanism is proposed (see for example 5.2.2.1.13 q_nvlocacc; 5.3.2.1.2 Status_MA_FS_SR_OS_LS_SH_from_MA_L2_Management; 5.3.2.1.8 statusValid_Position_from_Position_Calculation . . .).

• A majority of these fields indicates “n/a” and that seems very curious for a SIL4 software. These n/a should be justified (For example, the input “5.9.2.1.19 SafetyCriticalFailure” is considered has having no effect when it is absent or erroneous which is very curious considering the name of the data).

ASS534.2

Requirement 7.3.4.5 of the EN 50128 is: “The Software Architecture Specification shall identify, **analyse and detail the significance** of all hardware/software interactions”. This requirement is not fulfilled.

ASS534.3

Requirement 7.3.4.6 b) of the EN 50128 is: “Software components shall be clearly identified and **independently versioned inside the configuration management system**”. This requirement is not fulfilled.

ASS534.4

The following EN 50128 requirements are not fulfilled:

• 7.3.4.10 The Software Architecture Specification shall **describe the strategy for the software development** to the extent required by the software safety integrity level.

• 7.3.4.11 **Measures for handling faults** shall be included in the Software Architecture Specification in order to achieve the balance between the fault avoidance and fault handling strategies.

ASS534.5

The Software Interface Specification (see requirements 7.3.4.18 and 7.3.4.19 of EN 50128) is missing. The description of interface data given in D3.5.3 is incomplete [a) pre/post conditions; f) allocated memory, f) and h) synchronization mechanisms are missing].

ASS534.6
The description given in the software design part does address neither the main algorithms and sequencing or concurrency aspects, nor the error reporting mechanisms (see f) and g) of requirement 7.3.4.23 of EN 50128 and b3) and b4) of requirement 7.3.4.28 of EN 50128.

Assessment:
Design Specification is incomplete (Scrum process) but numerous requirements of the CENELEC standard are not fulfilled and will not be if the content of the document is not modified.
Notwithstanding these previous remarks, a major remark is that safety aspects are not well addressed in this design.

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

6 Summary

7 Tasks, recommendations and notes

This sections describes the recommendations for a follow-up assessment when incorporating openETCS results.

8 Finalization

Nuremberg,

Expert assessor
Norbert Schäfer

Massy,

Expert assessor
Frédérique Vallée

References

[1] Comité Européen de Normalisation Electrotechnique. Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, EN 50128. *EUROPEAN STANDARD*, 2011.

[2] openETCS Consortium. European Train Control System (ETCS) Open Proofs - Open Source. *Project Home Page*, 2015. `http://openetcs.org`.

[3] openETCS Consortium. Open Proofs Methodology for the European Train Control Onboard System. *ITEA2 Project Page*, 2015. `https://itea3.org/project/openetcs.html`.