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
openETCS D4.5: Draft Assessment Report
Independent Assessment according to the standard EN 50128:2011

Document approbation

<table>
<thead>
<tr>
<th>Lead author:</th>
<th>Technical assessor:</th>
<th>Quality assessor:</th>
<th>Project lead:</th>
</tr>
</thead>
<tbody>
<tr>
<td>location / date</td>
<td>location / date</td>
<td>location / date</td>
<td>location / date</td>
</tr>
<tr>
<td>signature</td>
<td>signature</td>
<td>signature</td>
<td>signature</td>
</tr>
<tr>
<td>Frédérique Vallée</td>
<td>Norbert Schäfer</td>
<td>Marc Behrens</td>
<td>Klaus-Rüdiger Hase</td>
</tr>
<tr>
<td>(All4tec)</td>
<td>(AEbt)</td>
<td>(DLR)</td>
<td>(DB Netz)</td>
</tr>
</tbody>
</table>

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

This work is licensed under the "openETCS Open License Terms" (oOLT).
Abstract: The Assessment Report describes the Assessment results in the frame of V&V activities in the openETCS project. According to the CENELEC EN50128:2011 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."

Disclaimer: This work is licensed under the "openETCS Open License Terms" (oOLT) dual Licensing: European Union Public Licence (EUPL v.1.1+) AND Creative Commons Attribution-ShareAlike 3.0 – (cc by-sa 3.0)

THE WORK IS PROVIDED UNDER openETCS OPEN LICENSE TERMS (oOLT) WHICH IS A DUAL LICENSE AGREEMENT INCLUDING THE TERMS OF THE EUROPEAN UNION PUBLIC LICENSE (VERSION 1.1 OR ANY LATER VERSION) AND THE TERMS OF THE CREATIVE COMMONS PUBLIC LICENSE ("CCPL"). THE WORK IS PROTECTED BY COPYRIGHT AND/OR OTHER APPLICABLE LAW. ANY USE OF THE WORK OTHER THAN AS AUTHORIZED UNDER THIS OLT 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/

This work is licensed under the "openETCS Open License Terms" (oOLT).
# Modification History

<table>
<thead>
<tr>
<th>Version</th>
<th>Section</th>
<th>Modification / Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>all</td>
<td>template of 1st version</td>
<td>Abdelnasir Mohamed</td>
</tr>
<tr>
<td>0.2</td>
<td>all</td>
<td>entering assessment result of ADD document</td>
<td>Frédérique Vallée</td>
</tr>
<tr>
<td>0.3</td>
<td>all</td>
<td>conversion to LaTeX</td>
<td>Marc Behrens</td>
</tr>
</tbody>
</table>
Table of Contents

Modification History................................................................. 3
1 Information about the Contract.............................................. 6
   1.1 Customer/ Organization/ Authority................................. 6
   1.2 Assessor/ Contractor.................................................. 6
   1.3 About the contract..................................................... 7
2 General..................................................................................... 9
   2.1 Glossary/ List of Abbreviations..................................... 9
   2.2 Referenced standards, guidelines and directives............. 9
List of Tables

Table 1. Assessment Glossary ................................................................. 9
Table 2. Referenced Documents ............................................................ 9
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 Odyssee 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

This work is licensed under the "openETCS Open License Terms" (oOLT).
1.3 About the contract

The openETCS organization consists of the openETCS consortium as being initiated by the ITEA2 labelled project.

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.
This work is licensed under the "openETCS Open License Terms" (oOLT).
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

<table>
<thead>
<tr>
<th>Document</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>EN 50128 Railway applications - Communications, signaling and processing systems</td>
<td>2011</td>
</tr>
</tbody>
</table>

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 affect 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 ESTEREL Technology 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.
<table>
<thead>
<tr>
<th>OpenETCS Deliverable</th>
<th>Remarks/To Do</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Planning</td>
</tr>
<tr>
<td>00 Project Plan</td>
<td>... of the EVC to comply the User Story Amsterdam-Utrecht.</td>
</tr>
<tr>
<td>Internal Assessment Plan</td>
<td>Task of Abelnasir Mohamed</td>
</tr>
<tr>
<td>Task of Baseliyos Jacob</td>
<td>Planned to be part of a User Story deliverable.</td>
</tr>
<tr>
<td>see remarks</td>
<td>see remarks</td>
</tr>
<tr>
<td>D4.4</td>
<td>Potentially part of a demonstrator project</td>
</tr>
<tr>
<td>D4.3.1</td>
<td>D4.3.2</td>
</tr>
<tr>
<td>Potentially part of D4.3.1 and D4.3.2</td>
<td></td>
</tr>
<tr>
<td>D3.6</td>
<td>Partially covered in D4.3.1</td>
</tr>
<tr>
<td>D3.5.3</td>
<td>ADD Document (SCADE API)</td>
</tr>
<tr>
<td>SUBSET 076, D4.3.1 (intermediate D4.2.1)</td>
<td>Missing</td>
</tr>
<tr>
<td>D4.3.3 Verification of Tools and Process</td>
<td>Missing</td>
</tr>
<tr>
<td>D1.3.1 Project Guide on Quality Assurance</td>
<td>Missing</td>
</tr>
<tr>
<td>D4.1 VerificationAndValidationPlan</td>
<td></td>
</tr>
</tbody>
</table>