openETCS/WP4/D4.5

ITEA2 Project
Call 6 11025
2012 – 2015

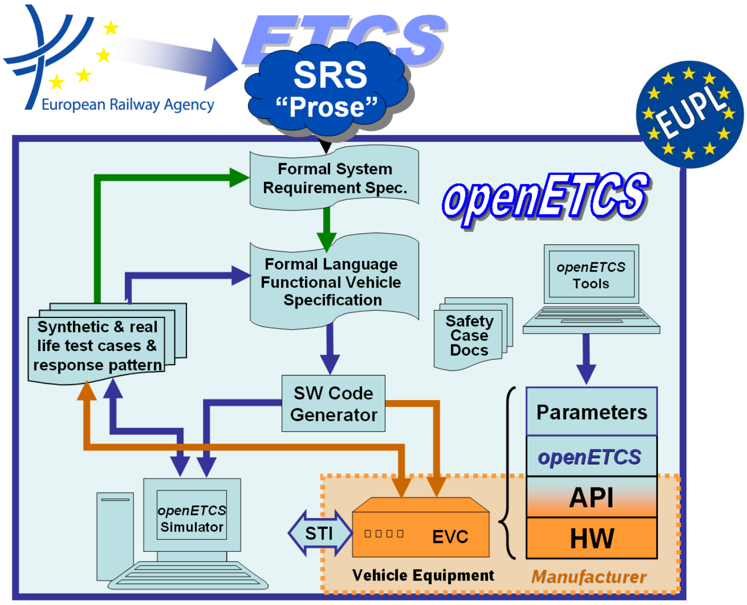
Work-Package 4: "V&V Strategy"

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

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 **?** 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.¨

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 **?** 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.

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.

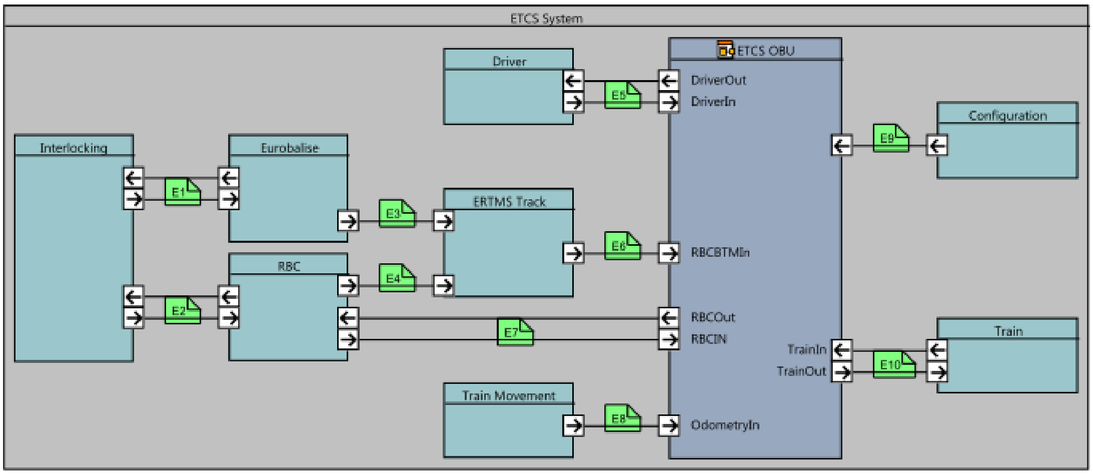


Figure 1: Top level architecture view of the ETCS OBU

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 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.

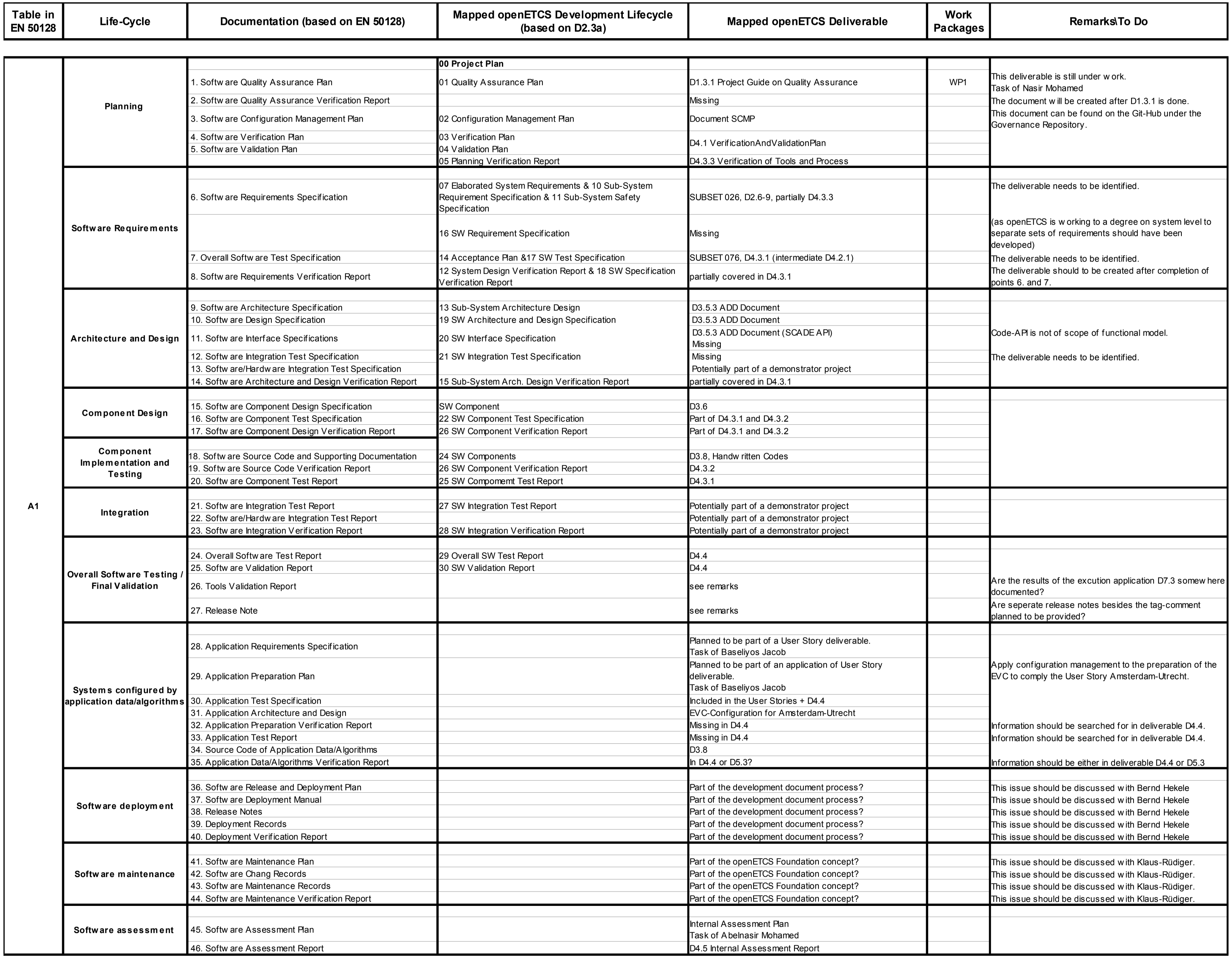


Table in EN 50128	Life-Cycle	Documentation (based on EN 50128)	Mapped openETCS Development Lifecycle (based on D2.3a)	Mapped openETCS Deliverable	Work Packages	Remarks\To Do
A1	Planning		**00 Project Plan**			
		1. Softw are Quality Assurance Plan	01 Quality Assurance Plan	D1.3.1 Project Guide on Quality Assurance	WP1	This deliverable is still under w ork. Task of Nasir Mohamed
		2. Softw are Quality Assurance Verification Report		Missing		The document w ill be created after D1.3.1 is done.
		3. Softw are Configuration Management Plan	02 Configuration Management Plan	Document SCMP		This document can be found on the Git-Hub under the Governance Repository.
		4. Softw are Verification Plan	03 Verification Plan	D4.1 VerificationAndValidationPlan		
		5. Softw are Validation Plan	04 Validation Plan			
			05 Planning Verification Report	D4.3.3 Verification of Tools and Process		
	Software Requirements	6. Softw are Requirements Specification	07 Elaborated System Requirements & 10 Sub-System Requirement Specification & 11 Sub-System Safety Specification	SUBSET 026, D2.6-9, partially D4.3.3		The deliverable needs to be identified.
			16 SW Requirement Specification	Missing		(as openETCS is w orking to a degree on system level to separate sets of requirements should have been developed)
		7. Overall Softw are Test Specification	14 Acceptance Plan &17 SW Test Specification	SUBSET 076, D4.3.1 (intermediate D4.2.1)		The deliverable needs to be identified.
		8. Softw are Requirements Verification Report	12 System Design Verification Report & 18 SW Specification Verification Report	partially covered in D4.3.1		The deliverable should to be created after completion of points 6. and 7.
	Architecture and Design	9. Softw are Architecture Specification	13 Sub-System Architecture Design	D3.5.3 ADD Document		
		10. Softw are Design Specification	19 SW Architecture and Design Specification	D3.5.3 ADD Document		
		11. Softw are Interface Specifications	20 SW Interface Specification	D3.5.3 ADD Document (SCADE API) Missing		Code-API is not of scope of functional model.
		12. Softw are Integration Test Specification	21 SW Integration Test Specification	Missing		The deliverable needs to be identified.
		13. Softw are/Hardw are Integration Test Specification		Potentially part of a demonstrator project		
		14. Softw are Architecture and Design Verification Report	15 Sub-System Arch. Design Verification Report	partially covered in D4.3.1		
	Component Design	15. Softw are Component Design Specification	SW Component	D3.6		
		16. Softw are Component Test Specification	22 SW Component Test Specification	Part of D4.3.1 and D4.3.2		
		17. Softw are Component Design Verification Report	26 SW Component Verification Report	Part of D4.3.1 and D4.3.2		
	Component Implementation and Testing	18. Softw are Source Code and Supporting Documentation	24 SW Components	D3.8, Handw ritten Codes		
		19. Softw are Source Code Verification Report	26 SW Component Verification Report	D4.3.2		
		20. Softw are Component Test Report	25 SW Compomemt Test Report	D4.3.1		
	Integration	21. Softw are Integration Test Report	27 SW Integration Test Report	Potentially part of a demonstrator project		
		22. Softw are/Hardw are Integration Test Report		Potentially part of a demonstrator project		
		23. Softw are Integration Verification Report	28 SW Integration Verification Report	Potentially part of a demonstrator project		
	Overall Software Testing / Final Validation	24. Overall Softw are Test Report	29 Overall SW Test Report	D4.4		
		25. Softw are Validation Report	30 SW Validation Report	D4.4		
		26. Tools Validation Report		see remarks		Are the results of the excution application D7.3 somew here documented?
		27. Release Note		see remarks		Are seperate release notes besides the tag-comment planned to be provided?
	Systems configured by application data/algorithms	28. Application Requirements Specification		Planned to be part of a User Story deliverable. Task of Baseliyos Jacob		
		29. Application Preparation Plan		Planned to be part of an application of User Story deliverable. Task of Baseliyos Jacob		Apply configuration management to the preparation of the EVC to comply the User Story Amsterdam-Utrecht.
		30. Application Test Specification		Included in the User Stories + D4.4		
		31. Application Architecture and Design		EVC-Configuration for Amsterdam-Utrecht		
		32. Application Preparation Verification Report		Missing in D4.4		Information should be searched for in deliverable D4.4.
		33. Application Test Report		Missing in D4.4		Information should be searched for in deliverable D4.4.
		34. Source Code of Application Data/Algorithms		D3.8		
		35. Application Data/Algorithms Verification Report		In D4.4 or D5.3?		Information should be either in deliverable D4.4 or D5.3
	Software deployment	36. Softw are Release and Deployment Plan		Part of the development document process?		This issue should be discussed w ith Bernd Hekele
		37. Softw are Deployment Manual		Part of the development document process?		This issue should be discussed w ith Bernd Hekele
		38. Release Notes		Part of the development document process?		This issue should be discussed w ith Bernd Hekele
		39. Deployment Records		Part of the development document process?		This issue should be discussed w ith Bernd Hekele
		40. Deployment Verification Report		Part of the development document process?		This issue should be discussed w ith Bernd Hekele
	Software maintenance	41. Softw are Maintenance Plan		Part of the openETCS Foundation concept?		This issue should be discussed w ith Klaus-Rüdiger.
		42. Softw are Chang Records		Part of the openETCS Foundation concept?		This issue should be discussed w ith Klaus-Rüdiger.
		43. Softw are Maintenance Records		Part of the openETCS Foundation concept?		This issue should be discussed w ith Klaus-Rüdiger.
		44. Softw are Maintenance Verification Report		Part of the openETCS Foundation concept?		This issue should be discussed w ith Klaus-Rüdiger.
	Software assessment	45. Softw are Assessment Plan		Internal Assessment Plan Task of Abelnasir Mohamed		
		46. Softw are Assessment Report		D4.5 Internal Assessment Report		

Figure 1. Mapping of openETCS Documents to the CENELEC Lifecycle