OETCS/WP4/D4.3.3V0.0

ITEA2 Project
Call 6 11025
2012 – 2015

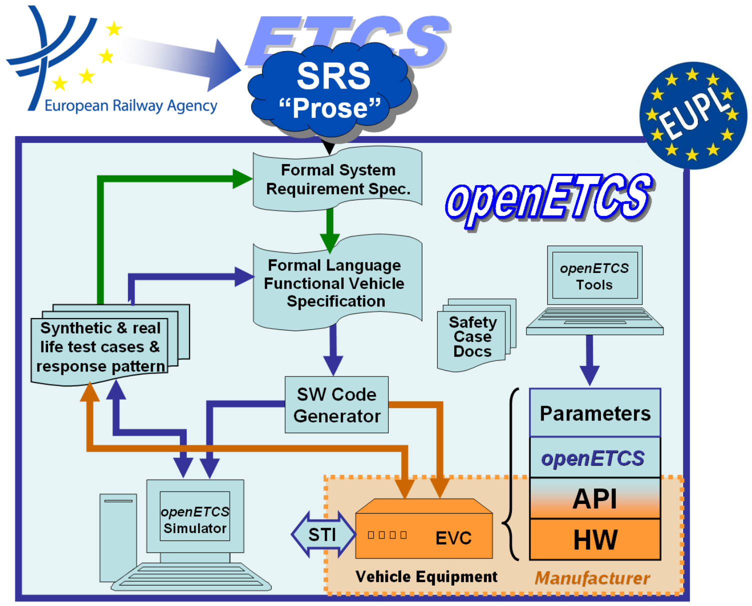
Work-Package 4: “Validation & Verification Strategy”

openETCS Safety case for tool chain and processes

Process and Toolchain verification for the openETCS on-board unit software development

Jan Welte

November 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: “Validation & Verification Strategy”

OETCS/WP4/D4.3.3V0.0
November 2015

openETCS Safety case for tool chain and processes

Process and Toolchain verification for the openETCS on-board unit software development

Document approbation

Lead author:	Technical assessor:	Quality assessor:	Project lead:
location / date	location / date	location / date	location / date
signature Jan Welte] (TU Braunschweig)	signature Abdelnasir Mohamed (AEbt)	signature Veronique Gontier (All4Tec)	signature Klaus-Rüdiger Hase (DB Netz)

Jan Welte

Technische Universität Braunschweig
Institute for Traffic Safety and Automation Engineering
Hermann-Blenk-Str. 42
38108 Braunschweig, Germany
eMail: openetcs@iva.ing.tu-bs.de
WebSite: www.iva.ing.tu-bs.de

Output Document

Prepared for openETCS@ITEA2 Project

Abstract: This document addresses the general quality and safety assurance concept implemented and used by the openETCS development process and its respective toolchain.

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)

Table of Contents

Figures and Tables

Figures

Tables

Document Control

Document information	
Work Package	WP4
Deliverable ID	D 4.3.3
Document title	Process and Toolchain verification for the openETCS on-board unit software development
Document version	0.1
Document authors (org.)	Jan Welte (TU-BS)

Review information	
Last version reviewed	
Main reviewers (org.)	

Approbation			
	Name	Role	Date
Written by	Jan Welte	WP4-T4.4 Task Leader	November 2015
Approved by	–	–	

Document evolution			
Version	Date	Author(s)	Justification
0.1	18/10/2013	Jan Welte	Document creation

1 Introduction

..

1.1 Purpose

...

1.2 Document Structure

...

1.3 Document Evolution

...

1.4 Reference Documents

This document essentially refers to the following standards, ETCS specification documents and openETCS project documents.

- **ISO 9000** — 12/2005 — *Quality management*
- **ISO 9001** — 12/2008 — *Quality management systems — Requirements*
- **ISO 25010** — 03/2011 — *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*
- **CENELEC EN 50126-1** — 01/2000 — *Railways applications — The specification and demonstration of Reliability, Availability, Maintenability and Safety (RAMS) — Part 1: Basic requirements and generic process*
- **CENELEC EN 50128** — 10/2011 — *Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems*
- **CENELEC EN 50129** — 05/2003 — *Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling*
- **CCS TSI** — *CCS TSI for HS and CR transeuropean rail has been adopted by a Commission Decision 2012/88/EU on the 25th January 2012*
- **SUBSET-026** 3.3.0 — *System Requirement Specification*
- **SUBSET-091** 3.2.0 — *Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2*
- **SUBSET-088** 2.3.0 — *ETCS Application Levels 1 & 2 - Safety Analysis*
- **OpenETCS FPP** — *Project Outline Full Project Proposal Annex OpenETCS* – v2.2
- **OpenETCS D2.2** – Report on CENELEC standard

- **OpenETCS D2.3** – Definition of the overall process for the formal description of ETCS and the rail system it works in
- **OpenETCS D2.4** – Definition of the methods used to perform the formal description

1.5 Glossary

ACedit	Assurance Case Editor
ARM	Argumentation Metamodel
ETCS	European Train Control System
ERA	European Railway Agency
FMEA	Failure Mode Effect Analysis
GSN	Goal Structured Notation
MoRC	Management of Radio Communication
RAMS	Reliability, Availability, Maintainability and Safety
SIL	Safety Integrity Level
SRS	System Requirement Specification
THR	Tolerable Hazard Rate
V&V	Verification & Validation

1.6 Background Information

If specific information are needed the can be place here. (D4.2.3 shall not be repeated)

2 Tool Chain

2.1 overview

by Jan Welte

2.2 Tool Qualification

by Michael Jastram (or other expert from WP7)

broad overview of the toolchain and the status of qualification (generall information can be placed in section Overview) - which tools have to be qualified - which tools are qualified? (in which way) - how should qualification be address for tools with pending qualification

2.3 SCADE

by Jan Welte and Marc Behrens

- use of SCADE for quality assurance - limitations of SCADE - addressing safety issues and properties in SCADE (potential specific aspects in openETCS deviation from the usual use of SCADE)

2.4 Safety Architect

by FrederiqueVallee (or Francois Revest)

- use of Safety Architect in openETCS (maybe addressing relation to Eclipse Safety Framework) - function in development process - inputs and outputs - results (in general, and specific for openETCS)

3 OpenETCS Development

3.1 overview

by Jan Welte

Short overview of current work.

- Main principals to ensure consistency

- Mainly collecting findings

- allocate the tools to the process steps used/ qualified

3.2 Compatibility to CENELEC standards

by Mohamed Abdelnasir

- overview results relation to EN 50126/50128 lifecycle - reasons for deviations - additional findings

3.3 Traceability

by @janwelte @raphaelfaudou

- addressing specific position of traceabilty for safety argumentation - introducing basic concept - main findings (limitations)

4 Generic OpenETCS Safety Case

4.1 System/ Sub-System Definition

by Jan Welte

- general information concerning openETCs system and sub-system structure - potential applications for artifacts

4.2 Quality Management

by Mohamed Abdelnasir

- basic concept for quality management in openETCS - missing aspects in quality management - main finding to address additional measures to complete quality management

4.3 Safety Management

by Jan Welte

- basic concept for safety management in openETCS - missing aspects in safety management - main finding to address additional measures to complete safety management

4.4 Functional/Technical Safety

by Jan Welte

- addressing general system safety properties and allocation to functional structure - listing needed integration properties for "safe" use of software model (specifically interface assumptions)

by Francois Revest

- addressing concrete findings from safety propagation analysis - additional measures applicable to tackle open points

5 Conclusion

This document presents the final results ...