ITEA2 Project
Call 6 11025
2012 – 2015

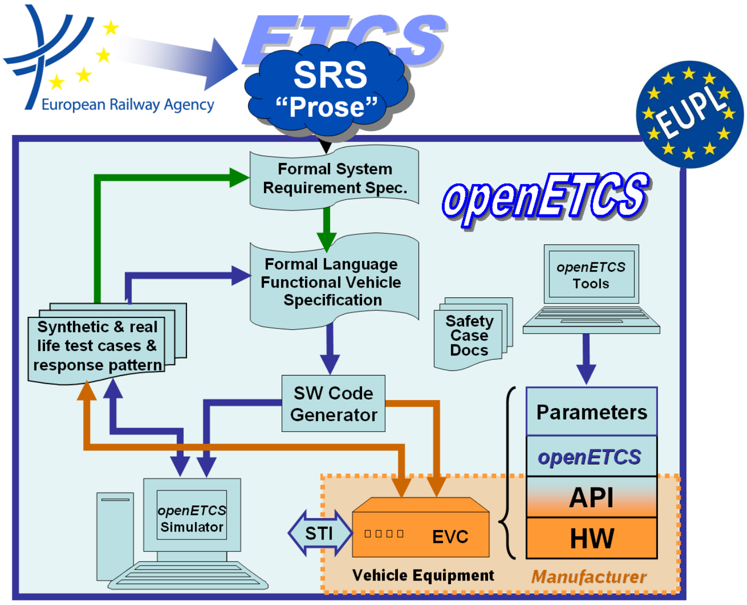
Work-Package 4: “Validation & Verification Strategy”

openETCS Safety case for tool chain and processes

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

Jan Welte and Raphaël Faudou

November 2015



Funded by:

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

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	signature	signature	signature
Jan Welte]	Abdelnasir Mohamed	Veronique Gontier	Klaus-Rüdiger Hase
(TU Braunschweig)	(AEbt)	(All4Tec)	(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

Raphaël Faudou

Samares Engineering on behalf of ENSEEIHT

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.

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 traceability for safety argumentation - introducing basic concept - main findings (limitations)

Requirement traceability activity consists in ensuring that all product engineering artifacts (including verification means) can be traced to an originating stakeholder requirement either directly (direct link) or through other requirements derived from stakeholder requirements. It means creating links but also manage their status (created, confirmed...) and potentially their deletion.

Concerning OpenETCS, there are several needs for traceability but main ones concern definition of links between SRS-Subset 26 requirements and two models:

- OpenETCS architecture SysML model (System, subsystem, SW functions), edited with SCADE System tool
- OpenETCS OBU formal executable software model (SW architecture, SW functions, detailed design), edited with SCADE Suite tool

Figure 1 illustrates all required traceability links needed to achieve current design verification and highlights main priority (arrows with largest size).

OpenETCS tool chain currently supports ability to create links between:

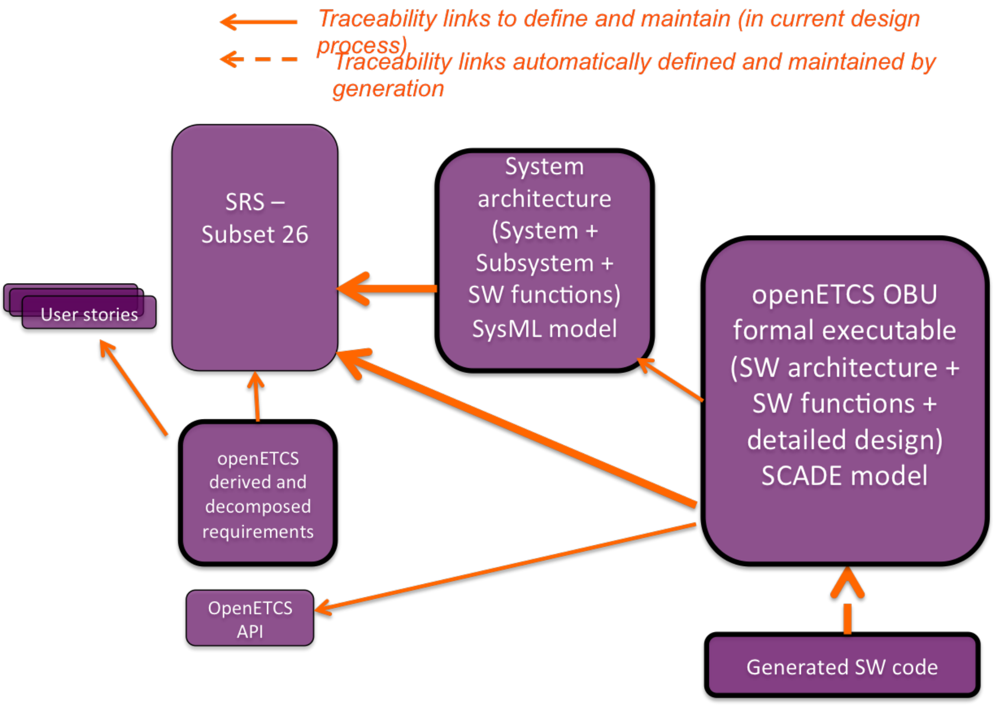

Traceability links to define and maintain (in current design process)
Traceability links automatically defined and maintained by generation
SRS – Subset 26
User stories
System architecture (System + Subsystem + SW functions) SysML model
openETCS OBU formal executable (SW architecture + SW functions + detailed design) SCADE model
openETCS derived and decomposed requirements
OpenETCS API
Generated SW code

Figure 1. OpenETCS traceability chains for current design with highlight on main priorities

- SRS Subset 026 .ReqIF requirements and additional requirements => through ProR integrated tool,
- SysML architecture model and SRS Subset 026 .ReqIF requirements through ReqCycle integrated tool

Note: it is also possible to create links between SCADE Model and SRS Subset 026 .ReqIF requirements through SCADE Suite RM Gateway and ReqTify traceability product but it is not an open solution and it requires additional licenses. Therefore that approach was used only by a few partners and was not considered as conclusive. There are pending investigations to provide alternate open solutions to support edition of those traceability links.

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

Table 1. List of ETCS Kernel Hazardous Events

Event Id.	Event Description	Corresponding performance requirement in Subset-041	OpenETCS allocation
KERNEL-1	Balise linking consistency checking failure	In case the message is received but the linking is not consistent: 5.2.1.1: Delay between receiving of a balise message and applying the emergency brake KERNEL-2	
KERNEL-2	Balise group message consistency check-ing failure	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake	
KERNEL-3	Failure of radio message correctness check		
KERNEL-4	Radio sequencing checking failure		

Continues on next page

Event Id.	Event Description	Corresponding performance requirement in Subset-041	OpenETCS allocation
KERNEL-5	Radio link supervision function failure		
KERNEL-6	Manage communication session failure		
KERNEL-7	Incorrect LRBG		
KERNEL-8	Emergency Message Acknowledgement Failure		
KERNEL-9	Speed calculation underestimates train speed	5.3.1.2: Accuracy of speed known on-board, in ceiling speed monitoring, release speed monitoring and in target speed monitoring in case the compen-sation of the speed measurement in-accuracy is inhibited	
KERNEL-10	Functional failure of standstill detection		
KERNEL-11	Incorrect traction/braking model (e.g. brake use restrictions)		
KERNEL-12	Failure of standstill supervision		
KERNEL-13	Failure of backward distance monitoring		
KERNEL-14	Failure of reverse movement protection		
KERNEL-15	Incorrect cab status (TIU failure)		
KERNEL-16	Incorrect train status TIU sleeping/cab status		
KERNEL-17	Wrong Acceptance of MA		
KERNEL-18	Failure to manage RBC/RBC		
KERNEL-19	Failure of train trip supervision in OS, LS and FS	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake 5.2.1.13: Delay between passing an EOA/LOA and applying the emergen-cy brake	

Continues on next page

Event Id.	Event Description	Corresponding performance requirement in Subset-041	OpenETCS allocation
KERNEL-20	Failure of train trip supervision, shunting and SR	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake	
KERNEL-21	Incorrect supervision of stop in SR	5.2.1.1: Delay between receiving of a balise message and applying the emergency brake	
KERNEL-22	Incorrect current EoA	5.2.1.6: Delay between receiving of an emergency message and applying the reaction on-board	
KERNEL-23	Incorrect train position / train data sent from on-board to trackside	5.3.1.3: Age of position measurement for position report to trackside 5.3.2.1: Safe clock drift	
KERNEL-24	Failure of message acknowledgement		
KERNEL-25	Incorrect traction/braking model (Accelera-tion only)		
KERNEL-26	Deleted		
KERNEL-27	Incorrect System Data (e.g. current level)		
KERNEL-28	Incorrect confidence interval		
KERNEL-29	Failure to shorten MA		
KERNEL-30	Incorrect shortening of MA		
KERNEL-31	Deleted		
KERNEL 32	Failure of loop message consistency check-ing		
KERNEL-33	Wrong processing of MA information	5.2.1.3: Delay between receiving of a balise message and reporting the resulting change of status on-board (5.2.1.4: Delay between receiving of a MA via radio and the update of EOA on-board). Note: Whether 5.2.1.4 is safety related must be evaluated in the specific application's hazard analysis, see further section 5.3.	

Continues on next page

Event Id.	Event Description	Corresponding performance requirement in Subset-041	OpenETCS allocation
KERNEL-34	Incorrect supervision of MA time-outs (sec-tions and overlaps)	5.2.1.3: Delay between receiving of a balise message and reporting the resulting change of status on-board (5.2.1.4: Delay between receiving of a MA via radio and the update of EOA on-board). Note: Whether 5.2.1.4 is safety related must be evaluated in the specific application's hazard analysis, see further section 5.3.	

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 ...