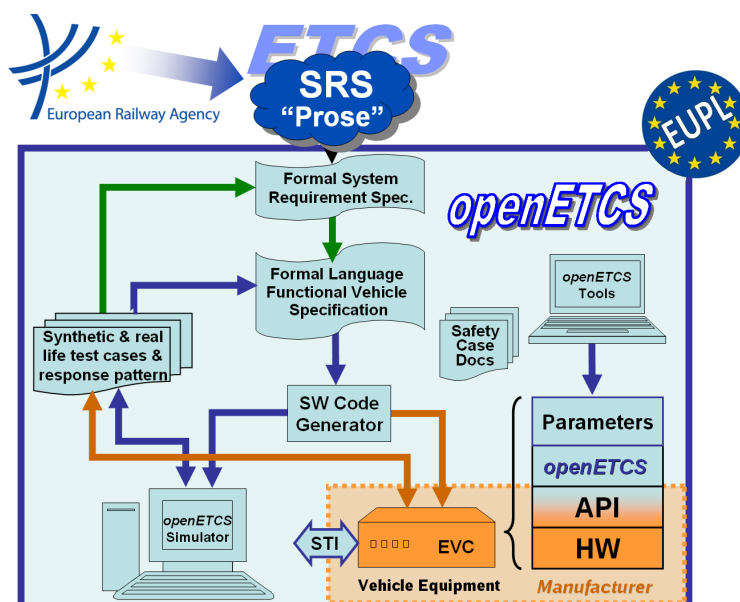OETCS/WP4/D4.4aV01

openETCS

Work-Package 4: "Validation & Verification Strategy"

openETCS Safety Plan

Guideline for the safety related activities in an openETCS Onboard Unit development

Jan Welte   June 2013

This page is intentionally left blank

Work-Package 4: "Validation & Verification Strategy"   **OETCS/WP4/D4.4aV01**
                                                               June 2013

openETCS Safety Plan
Guideline for the safety related activities in an openETCS Onboard Unit development

Jan Welte

Technische Universität Braunschweig
Institute for Traffic Safety and Automation Engineering
Langer Kamp 8
38106 Braunschweig, Germany
eMail: openetcs@iva.ing.tu-bs.de
WebSite: www.iva.ing.tu-bs.de

Output Document

Prepared for   openETCS@ITEA2 Project

Abstract:

Table of Contents

Figures and Tables

Figures

Tables

Document information	
Work Package	WP4
Deliverable ID or doc. ref.	D4.4
Document title	openETCS Safety Plan
Document version	00.01
Document authors (org.)	Jan Welte (Tu-BS)

Review information	
Last version reviewed	–
Main reviewers	–

Approbation			
	Name	Role	Date
Written by	Jan Welte	WP4-T4.4 Task Leader	June 2013
Approved by	–	–	

Document evolution			
00.01	12/06/2013	Jan Welte	Document creation
Version	Date	Author(s)	Justification
–	–	–	–

Introduction

0.1 Purpose

Safety Strategy

0.2   Activities for VnV Level 1

The VnV Level 1 activities try to implement the overall safety strategy on parts of the benchmark modelling results to establish details for artifact relations, traceability between different artifacts and tool use. Therefore the following benchmark models are used as exemplary design artifacts:

- SysML model Papyrus by CEA and All4tec

- Fraunhofer

- Scade model by Siemens

0.2.1   Hazardous Events

Based on the

a. KERNEL-6 Manage communication session failure - Related to model of Subset 26 §3.5.3 Establishing a communication session

b. KERNEL-9 Speed calculation underestimates train speed (or KERNEL-25 Incorrect traction/braking model (Acceleration only)) - Related to model of Subset 26 §3.13 Braking curves

c. KERNEL-19 Failure of train trip supervision in OS, LS and FS - Related to model of Subset 26 §5.9 Procedure On-Sight

References

[1] Leslie Lamport, *LaTeX: A Document Preparation System*. Addison Wesley, Massachusetts, 2nd Edition, 1994.