OETCS/WP4/D4.3.3V0.0

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

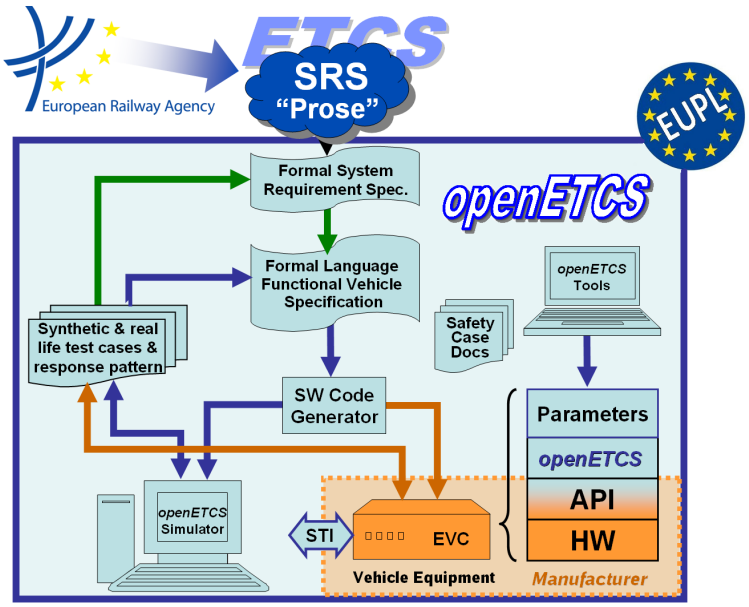
Work-Package 4: “Validation & Verification Strategy”

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 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

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 applied by the openETCS development process and its supporting toolchain. Thereby, the it is shown how the overall openETCS development process principals presented in D2.3 and additional document can be applied for a CENELEC confirm SIL 4 development, if the interfaces to the system development are complemented accordingly. For the generic safety argumentation it is shown hw the model design addresses the ETCS system hazards for the OBU Kernel.

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

During system development the system limits and components have to be established before the necessary steps can be taken to ensure that the system behavior is not unsafe. In this context safety is understood as protecting humans from harm resulting from the system as distinguished from security which covers protecting the system itself from hazards coming from the outside. Respectively, safety and security are comparative terms which have to be specified in context of the system for which they shall be proven. With respect to the definition of safety used in the EN 50128 hazards are only taken in account with respect to direct harm to humans, not to the environment overall, as it is considered in the context of different systems. The standards for railway system development like EN 50126, EN 50128 and EN 50129 provide only guidelines how safety for a system shall be determined and assured by providing certain management principles and methods for the respective system development. As the openETCS project is related to a number of different system definitions like the overall railway system, the on-board unit, the kernel software and the development tool chain different safety aspects have to be taken in consideration. Only a small number of these can actually be determined in the openETCS context alone. Respectively, this document and all considerations concerning safety in openETCS are focusing on the principal functional safety of the openETCS on-board kernel software and it resulting principals which have to be applied if the software model and code shall be used in a specific context.

1.1 Purpose

The hazard and risk analysis activities are part of the overall safety process which is defined in the EN 50129 as "the series of procedures that are followed to enable all safety requirements of a product to be identified and met". To ensure that the safety process is implemented and followed in a proper way during the development the EN 50129 requires a safety management. The management has to present and control all related activities and documentation over the life-cycle taking into account the approval mile-stones and review requirements. As the product life-cycle is an ongoing process and iterative changes are taking place, the management system has to ensure that the respective safety effects of every change is considered. The openETCS project does not cover the full development of an ETCS on-board unit, the safety related activities in WP 4 do not cover all required parts of an EN 50129 compliant safety process and management. Hence, the purpose of this document is to present the basic concepts for hazard and risk analysis and safety case development evaluated and derived during the first iteration of WP 4. As openETCS constitutes a research project planning and responsibilities can not be derived and confined as it would be expected in a pure development project. Respectively, this document is not intended to document all required roles, documents and responsibilities as it would be required for safety documentation according to EN 50126 and EN 50129. This report only intends to present concepts and principals which would fit the needs for openETCS and how these have to be applied up to this point in the project.

As the movement characteristics of a train set specific limits in which a driver alone is able to avoid derailment or any kind of collisions, railway signaling and protection systems have been developed to ensure safe train movements. Respectively, the major parts of a train control system like ETCS includes functionalities which shall guarantee that the overall railway system does not get in a hazardous situation. Correspondingly, this document illustrates the concepts for hazard

and risk analysis which has been defined during the first WP 4 iteration to identify hazards or allocate them from the overall system analysis if they are related to the openETCS software. In addition the resulting risk for these hazards has to be evaluated to deduce specific safety requirements which have to be considered during the development process to reduce the risk. The results of the first proof of concept activities performed during this iteration are presented in section **??**.

As the openETCS project does not produce an implemented train borne on-board system, the openETCS documents will not cover all specific software and hardware aspects which the EN 50129 requires for a sufficient safety case. Respectively, the openETCS results cannot be used without further work to demonstrate that a derived product using the openETCS kernel is compliant with all specified safety requirements. On this grounds during the first WP 4 iteration a model-based concept has been derive how the openETCS contributions have to be presented to at least serve as a basis for an on-board unit safety case. Therefore, all documents shall be related to a generic safety case for an EVC using the openETCS software development.

1.2 Document Structure

As the openETCS software development process and the respective tool chain are used in an iterative process this document only presents the current state of the openETCS safety related activities for the first WP 4 iteration. Chapter 1 gives an introduction to the overall document providing the basic document information and listing all reference standards and openETCS deliverables. Additionally, section 1.6 provides an introduction concerning the context of quality and safety as it is understood in this document.

As the hazard and risk analysis and all safety case activities are directly related to the overall development process, chapter 3 introduces the general steps of the openETCS development process and its interface to safety activities. In the following chapter 4 the concept for hazard and risk analysis during the openETCS development is presented. The fundamental safety principals for ETCS, which are the starting point for all openETCS specific activities, are described in section **??**. The derived plan how hazard and risk analysis may be performed for the openETCS software development is specified in section **??** and evaluated in a first proof of concept work performed during the first WP 4 iteration. Chapter **??** describes the plan to collect and establish the safety case related documentation for the openETCS development. While section **??** states the principal requirements for the overall safety case activities, section **??** presents the model-based approach planed for openETCS and the supporting tools, which shall be applied.

1.3 Document Evolution

This document is based on the results of the first iteration work of WP 4 and shall present the overall concept for hazard and risk analysis methods applied during the openETCS development. All resulting changes and additional safety activities have to be maintained and documented according to the overall safety process in following iteration and will be documented in the respective following deliverables.

The openETCS development plan presented in chapter 3 is based on the current version of the Quality Assurance Plan and WP 2 deliverables D2.3 and D2.4. As the development methods and processes are still evolving this document has to be adopted accordingly. Concrete methods to verify and validate safety relevant properties derived from the hazard control methods described in this document, will be specified in the Verification and Validation plan. Also the tools used to support those activities will be detailed in this plan.

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

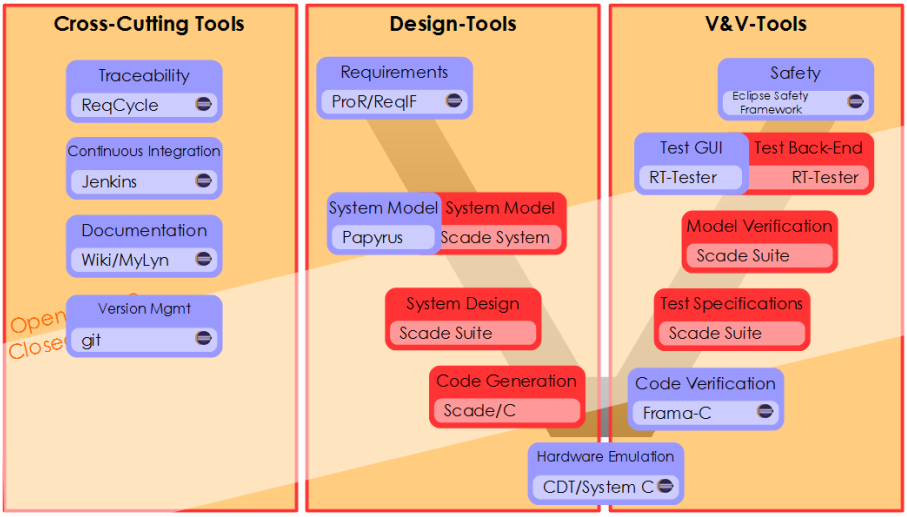


Figure 1. Core openETCS Toolchain

2.2 Tool Qualification

Table 1. OpenETCS toolchain and categorisation

Tool	Support Activity	Tool Class	Justification
Papyrus Editor	Definition of the model architecture	T1	
Papyrus SysML checker	Check SysML conformity of the model	T2	
SCADE Editor	Low-level modeling and code generation	T1	
SCADE Code Generator	Code generation	T3	
ProR	Requirements management	T1	
Bitwalker	Generation of data structures for modelling	T3	
Git	Versioning & Traceability	T1	

Continues on next page

Tool	Support Activity	Tool Class	Justification
RT Tester	Model-based testing	T2	
CPN Tools	Model checking and test case generation	T2	

tool are coming from D7.3 table 1

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 2 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:

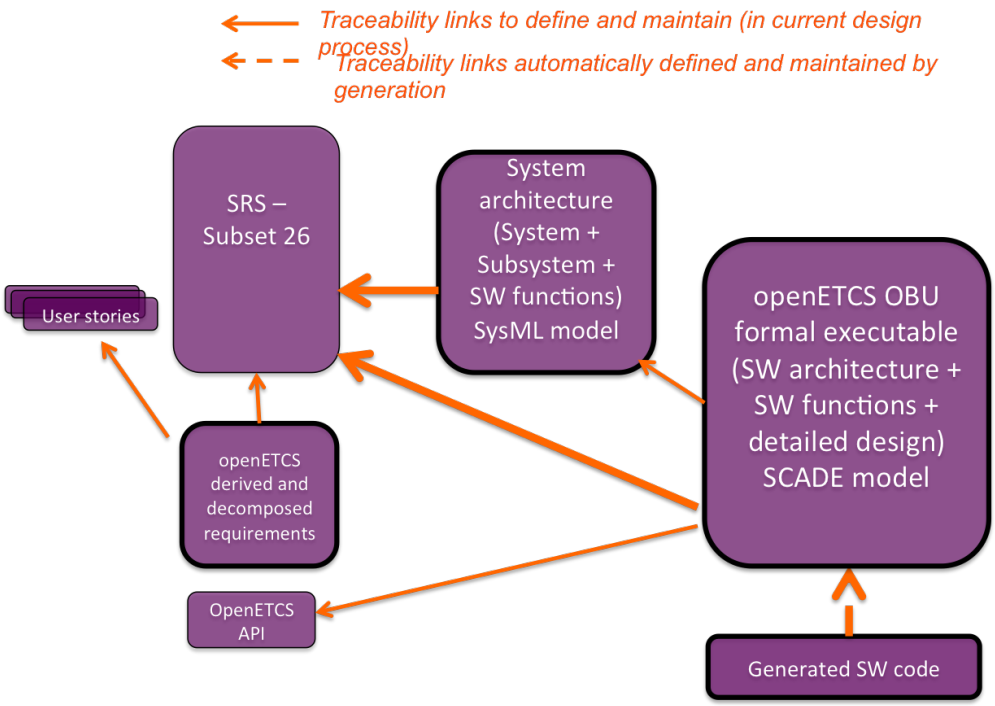


Figure 2. OpenETCS traceability chains for current design with highlight on main priorities

- 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

Since the openETCS project as a research does not have the objective to conduct all steps needed for a vital on-board unit development, the resulting safety case will be generic in many parts only giving the requirements and basic safety strategies, but lacking the actual evidence. However, the overall safety argumentation has to be set up to meet SIL 4 requirements. Therefore the safety case has to show that the methods chosen in the openETCS development process satisfy the EN 50128 quality requirements and which documents have to be created during the process to obtain the required evidence. Basis for this work will be the Quality Assurance Plan as this document builds the basis for all quality management activities.

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

As detailed in chapter 4 the overall safety argumentation has to demonstrate that during the development process the higher-level safety requirements have been addressed and that accordingly the on-board software satisfies the safety level. The safety case has to specify traces from high-level hazardous events to all subsystem requirements allocated to the openETCS software architecture and their verification and validation. Therefore, the safety case has to present evidence that the chosen methods are sufficient to demonstrate compliance to the requirements and that these methods are applied in a consistent process to ensure that all safety requirements are respected and validated.

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

Based on the ETCS reference architecture SUBSET-91 defines the role of ETCS as a train protection system the following way:

"To provide the Driver with information to allow him to drive the train safely and to enforce respect of this information, to the extent advised to ETCS."

Respectively, the Core Hazard for the ETCS reference architecture is defined as the following in SUBSET-91:

"Exceedance of the safe speed or distance as advised to ETCS."

Based on the role of ETCS and its respective SIL 4 quantification the maximum allowed rate of occurrence (Tolerable hazard rate) of the ETCS Core Hazard for ETCS on-board is

$$1.0 \times 10^{-9} hour^{-1} train^{-1}.$$

The same value is specified for the corresponding track-side.

Adapted form the ETCS system safety analysis presented in SUBSET-88 the Annex A of SUBSET-91 presents the List of Hazardous Events inside ETCS that might cause the ETCS Core Hazard to occur, either alone or in combination with other failures. These are the events not eliminated by the operational analysis. 34 of these hazardous events are allocated to the Kernel, which make them the basis for the on-board software hazard and risk analysis.

Table 2. 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		
KERNEL-5	Radio link supervision function failure		
KERNEL-6	Manage communication session failure		
KERNEL-7	Incorrect LRBG		

Continues on next page

Event Id.	Event Description	Corresponding performance requirement in Subset-041	OpenETCS allocation
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.	

The main evidence for this part will be provided during verification steps, tracing identified hazards and risk control measures and in case where it is possible also validation results showing that the system is not behaving in an unsafe way. Mainly, it shall be demonstrated that all required risk control measures are taken into account in the actual model and/or code. Thereby, it has to be stated which artifacts have to be provided by which role during the development process and which content can be reused for overall safety argumentation in an implementation.

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 basic concept for the main safety related activities in the openETCS development as they have been determined during the first verification and validation iteration level of WP 4. As these have been done in respect to a still evolving development methodology and tool chain, the overall process as to be detailed and adopted as the project continues.

In general the verification and validation activities have to ensure that the safety principal apportioned to the on-board functionality are satisfied. Hence, the main objective for the openETCS safety case as presented in chapter **??** is to provide the fundamental quality and safety principles for the openETCS development as these have to be completed by adopters of the openETCS results for their assessment. Therefore, the general safety argumentation and the concrete evidence shall be clear distinguished to ease applicability and support discussions with different legal authorities.

Overall the main methodology for the hazard and risk analysis as well as the safety case work has been defined during the first level iteration but these concepts have to be further refined over the next iterations with the evolving development process.