OETCS/WP4/D4.2aV01

openETCS

ITEA2 Project
Call 6 11025
2012 – 2015

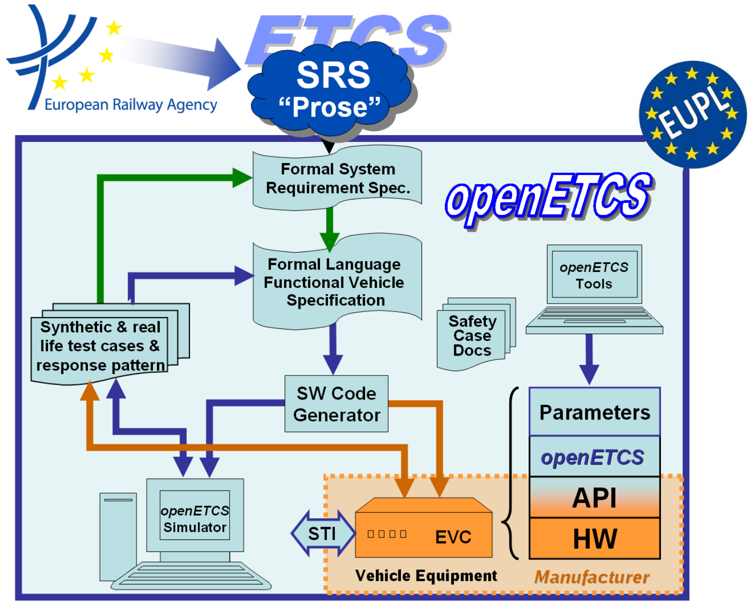
Work-Package 4: “Validation & Verification Strategy”

openETCS Safety Plan

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

Jan Welte

October 2013



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/D4.2aV01
October 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: The safety plan presents an overview about the main safety activities performed during the OpenETCS development process. Thereby, a consistent safety guideline is shown, which combines the functional safety analysis for the system and subsystems from which safety properties will be derived with verification and validation techniques to ensure the overall quality during the design of all safety related parts of the system. Overall, the safety plan will guarantee that the safety design activities required in D2.6 are covered and all safety requirements are fulfilled.

Table of Contents

Figures and Tables

Figures

Tables

Document Control

Document information	
Work Package	WP4
Deliverable ID or doc. ref.	D4.2
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	October 2013
Approved by	–	–	

Document evolution			
00.01	01/10/2013	Jan Welte	Document creation
Version	Date	Author(s)	Justification
0.10	28/01/2014	Jan Welte	Extended Introduction

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 the environment from hazards coming 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. The standards for 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.

1.1 Purpose

The safety plan is part of the overall safety process which is "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 in a proper way the EN 50129 requires a safety management which is consistent process for RAMS presented in the EN 50126.

The purpose of the safety plan is to show in details how the safety requirements will be implemented over the development process. To do this the plan has to present the management structure, all related activities and documentations over the life-cycle, as well as the approval mile-stones and review requirements. As the product life-cycle is an ongoing process and, specifically in a project like openETCS, iterative changes are taking place, the safety plan has to be updated to assess the respective safety effects. Thereby, the safety plan will also include the plan for the safety case, which itself is the final assessment document to demonstrate the actual product compliance with all specified safety requirements which have been implemented according to the safety plan.

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 mayor parts of a train control system like ETCS include functionalities which shall guarantee that the overall railway system does not get in a hazardous situation.

Since the openETCS project does not produce a specific train borne on-board unit the openETCS safety plan, will not cover all specific software and hardware aspects. The focus is mainly on the EVC kernel functionality and only partially on further real time and hardware/software integration aspects. However, this safety plan shall at least cover the safety process needed to ensure that the openETCS software development can be extended to become the functional basis for a complete on-board unit development.

1.2 Document Structure

As the openETCS software development process and the respective tool chain a used in an iterative process this version of the safety plan is also only one iteration step. As the design selectivities and the use of tools proceed further more details concerning the hazard identification methods, safety verification and validation principals and their corresponding result documentation will be added to this document. So far the version 1.0 of the safety plan will only cover the overall safety process and it general activities as well as the safety management activities which will create the safety plan as the final documentation document. Details are only presented for the hazard identification and evaluation method, as well as for the argumentation structure management method. All detailed activities concerning verification and validation of different safety requirements are closely connected to the V&V plan and all activities described there.

As safety is a term which is used in different context and therefore interpreted differently depending on the used reference system, the following section 1.3 presents the principal concept and terminology on which the following safety process is founded [**?**]. These section shall present and clarify the underlying understanding of safety as it in standards EN 50126, EN 50128 and EN 50129 for railway system development. Thereby, it is important to state more precisely the relation between quality and safety for software as this is the core aspect for the openETCS development.

1.3 Background Information

In the context of railway system development the EN 5012X and the ISO 900X standards are closely connected. Respectively, the terms safety and quality and related terms as reliability, maintainability, availability, usability and security are often used together. For example the EN 50129 names evidence of quality and safety management as conditions for a safety acceptance. The following sections shall give a common definition for all this aspects, which are required in a CENELEC confirm development process.

1.3.1 Quality

The ISO 9000 defines quality as "degree to which a set of inherent characteristics fulfills requirements" [**?**], which clearly shows a more objective view as the EN 50129, which defines quality as "a user perception of the attributes of a product" [**?**]. As for system development the given requirements always present the objective against which the system has to be measured this definition is consistent with the definition of verification and validation as it is presented in the EN 50128 and the openETCS V&V plan.

Depending on the respective field of application specific standards further specify the characteristics which shall be taken in account to establish quality. The EN 50126 as primary standard for railway applications gives RAMS as the major contributor for the quality of service.

1.3.2 RAMS

1.3.3 Software Quality

1.3.4 Safety

1.3.5 Probabilistic Safety Concept

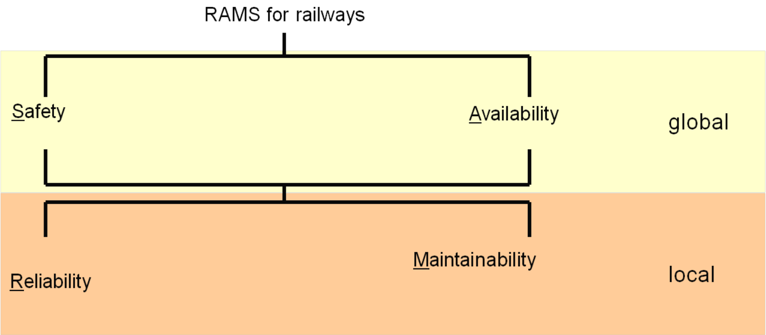


Figure 1. RAMS for Railway elements and their relations [?]

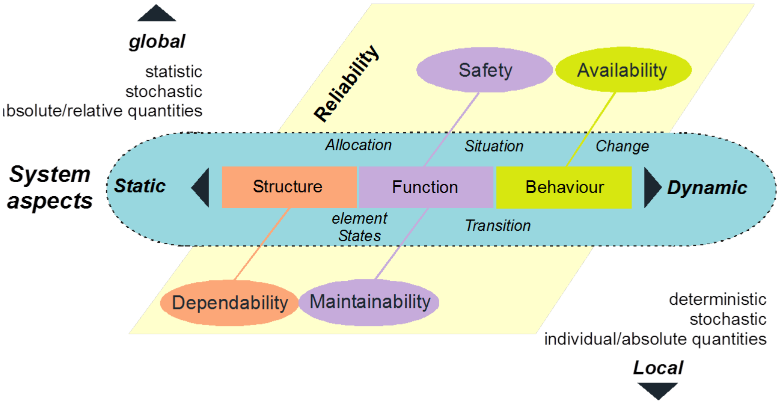


Figure 2. Systems Characteristics and their relations to RAMS in Railways [?]

Risk

The EN50128 standard defines safety as the “freedom from unacceptable levels of risk of harm to people" [?], which shows that the safety approach required by the CENELEC standards is risk-based. As the risk is defined as the “combination of the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm" [?] this approach is based on a probabilistic understanding of event occurrence. The overall relations between all these safety-related terms used to define the safety properties, characteristics and quantities are outlined by the Risk-Genesis-Model of Schnieder, which is shown in the following figure 3.

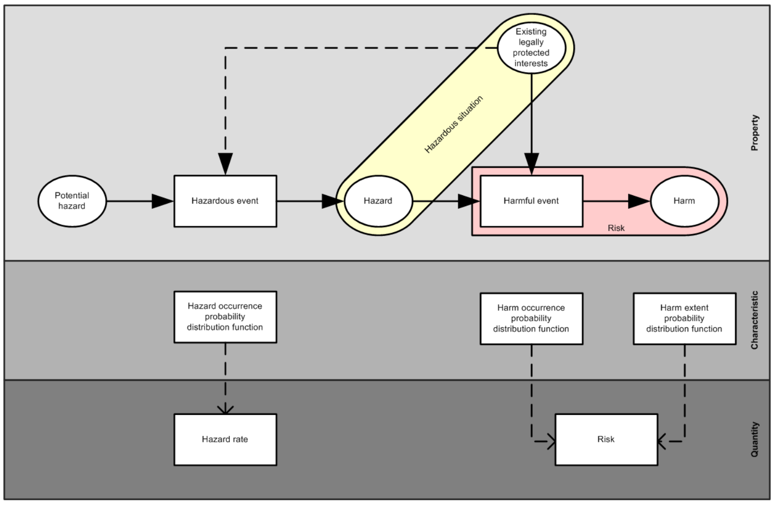

Existing legally protected interests
Hazardous situation
Property
Potential hazard
Hazardous event
Hazard
Harmful event
Harm
Risk
Hazard occurrence probability distribution function
Harm occurrence probability distribution function
Harm extent probability distribution function
Characteristic
Hazard rate
Risk
Quantity

Figure 3. Risk-Genesis-Model showing the relations between the safety-related terms [?]

it This demonstrates that the first step is to define the system properties, specifically identifying the harms and their related hazardous situations. This has to be performed during a system hazard analysis. Afterwards the respective properties have to be determined by assessing the risk concerning the identified hazards. Based on this work safety integrity levels can be assigned to all system functionalities which are then allocated during the design to certain parts of the operational equipment. As this work is closely related to all design decisions, it has to be done iteratively for all abstraction levels during the system design.

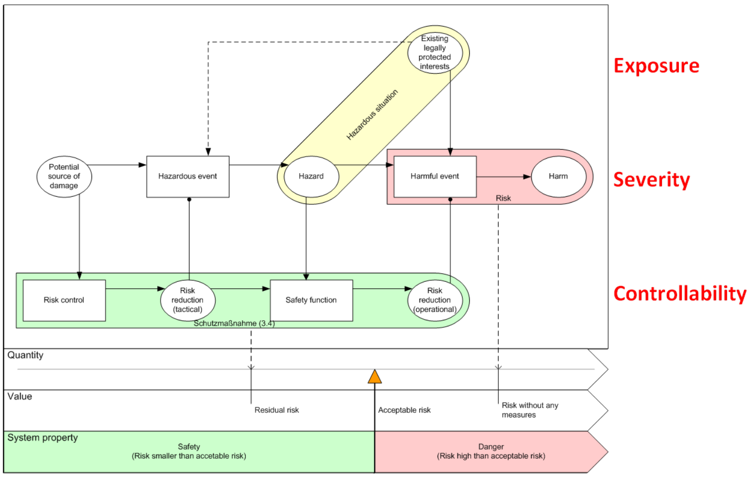


Figure 4. Risk control process [?]

Safety Integrity Level

The safety integrity level represented the acceptable risk for every part of the system. The risk control process as it is presented in figure 4 is then performed to ensure that the safety integrity levels are reach by every part of the system.

Since software itself does not fails in the way technical equipment does the specific software safety integrity level represent a qualitative measure with respect to the required degree of correctness for the software functionality than a qualitative value for the likelihood of failing. To reach the needed degree of correctness for the software various design, verification and validation methods are required corresponding to the assigned software safety integrity level. This process leads to safety requirements which have to be implemented in the software design as well as verified and validated. Respectively the EN50126 describes the safety design process as a series of safety tasks for each life cycle phase. This task are related to a number of safety artifacts which are created, used and adapted over time through the different safety design activities.

Addition topics shall be proposed by every participant. Section will be managed by Jan Welte

1.3.6 Safety Case

1.3.7 Safety Glossary

Added via the glossary documentation process for openETCS

2 Document Evolution

The safety plan will be further specified with the progress of the design process. This specifically reference to the refinement of safety properties on different modeling levels and their corresponding verification and validation methods. All resulting changes and additional safety activities have to be maintained according to the EN 50128.

V01, T0+16: First version of the plan.

V02, T0+17: First revision, based on the openETCS development process and the preliminary SSRS results. Also the first iteration of V&V activities will be considered. (D4.2.3)

V03, T0+25: Second revision, based on the internal reports of modeling and V&V activities. (D4.3.3)

V04, T0+36: Final version as part of the final V&V report (D4.4)

The first version of the plan is based on the available information of the design process. This is not yet very detailed as also the description in Chapter **??** of this report shows. In particular, the nature of the SSRS is yet to be defined precisely, and the architecture description including the HW/SW partitioning needs to be revised.

Concrete plans of activities are thus still to be made, and methods and tools to be applied will have to be selected. Only the first phase of V&V activities is described in Sec. **??**.

3 General ETCS Safety Principals

This section shall present as short description of all safety principals used for the overall safety strategy.

3.1 Overall Safety

This section shall present as short description for the overall safety strategy.

3.2 Functional Safety

This section shall present the applied openETCS safety strategy.

4 OpenETCS Safety Process

4.1 Safety-related Activities

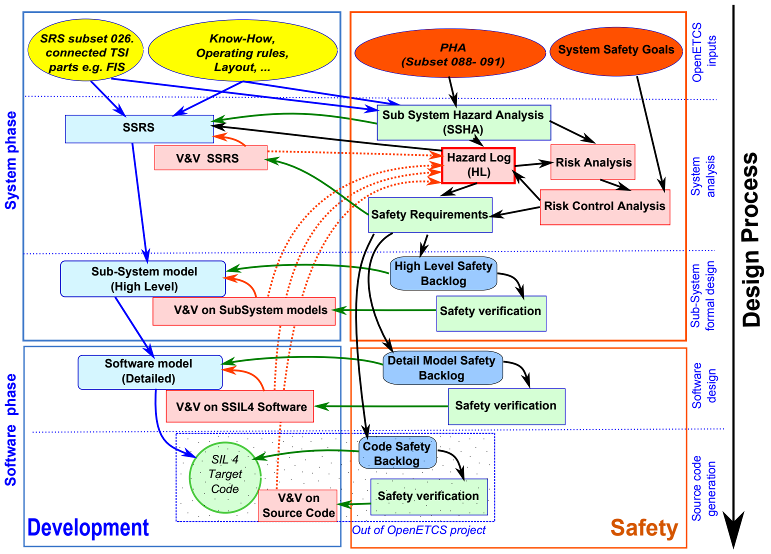


Figure 5. Overall safety process

Process description has to be updated with the latest work. Cooperation between Cyril, Merlin and Jan

4.1.1 OpenETCS safety design process

The presented CENELEC standard safety artifacts and activities are always related to the overall system development. Since the openETCS development process just describes the development of the on-board unit software for ETCS additional system informations are needed for the openETCS safety design process. These are mainly the following two parts of the CCS TSI:

- UNISIG SUBSET-026 System Requirements Specification (Version 3.3.0)
- UNISIG SUBSET-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2 (Version 3.2.0)

In relation to SUBSET-91 further documents should be considered:

- Part of TSI Annex A
  - SUBSET-036
  - SUBSET-037
  - SUBSET-040
  - SUBSET-041
  - SUBSET-098

- Not part of TSI Annex A
    - SUBSET-039
    - SUBSET-078
    - SUBSET-079
    - SUBSET-080
    - SUBSET-081
    - SUBSET-088

From these documents the Preliminary Hazard Analysis and the System Safety Goals have to be derived which are needed as the starting point for the openETCS safety design process. Based on these information a subsystem hazard and risk analysis for the openETCS scope can be performed which set-up the openETCS hazard log. Based on these results the openETCS safety requirements will be specified, which are then further developed to functional requirements. During the development these requirements are adopted if necessary for the different abstraction levels from the high level model down to the source code. This is done using corresponding safety backlogs, which are the reference for the safety requirement verification. Altogether the source code has to be validated against all safety requirements to demonstrated, that software faults can not cause any harm. The safety case has to present all needed documentation.

The main task of the openETCS safety design process and the interactions with the design process are shown in figure 6.

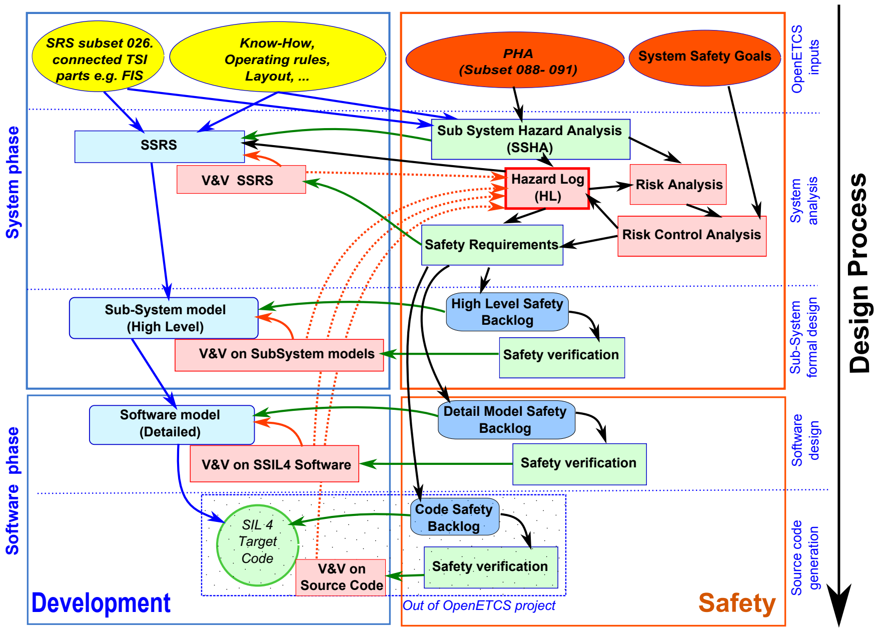


Figure 6. OpenETCS Safety Design Process

The openETCS safety design process will be specified more detailed in the safety plan. Correspondingly, the main safety artifacts and safety design activities which have to be handled during the openETCS safety design process are shown in table 1 and 2.

The safety design process and the resulting documentation constitute the main documents for the system approval, as it is required by European and national law to do everything reasonable expectable to prevent harm. Accordingly the CENELEC standards build the common technical

Table 1. Main openETCS safety design process artifacts

Abbreviation	Safety Artifact	Degree of Formalisation
Safety Req	Safety Requirements: list of all requirements which have to be respected during the system development to reach the safety goals	Informal/ Semi-Formal / Formal
HL	Hazard Log: List of identified hazards and its associated risk classification as well as information concerning the risk control	Informal
SP	Safety Plan: Document which specifies all activities, resources and events to ensure that the source code will satisfy all relevant safety requirements	Informal
SC	Safety Case: Documentation which demonstrates that the used development process and the resulting source code fulfil all safety requirements	Informal
CSB	Code Safety Backlog: list of requirements/ properties to be implemented inside the dM derived from the HL (and the dMSB)	Semi-Formal/ Strictly-Formal
dMSB	Detailed Model Safety Backlog: list of requirements/ properties to be implemented inside the dM derived from the HL (and the hLSB)	Semi-Formal/ Strictly-Formal
hLSB	High Level Safety Backlog: list of requirements/ properties to be implemented inside the hM derived from the HL	Informal/ Semi-Formal

rules for the development process. The Common Safety Methods present a concept based on the EN50126 how the risk evaluation and management has to be performed.

Therefore the main references concerning the safety design process are the CENELEC standards, mainly the EN50126 on how the safety aspects have to be handled as part of the RAMS management over the development process. The overall risk evaluation concept is also defined at this point. The specific concerning the safety case preparations are defined in the EN50129 including the Safety Integrity Level concept.

Therefore the overall safety management process has to be followed during the openETCS project, as far as it is concerning the scope of openETCS. Therefore the following table 3 presents a first list of relevant requirements:

4.1.2 Safety artifacts

Process description has to be updated with the latest work. Cooperation between Cyril, Merlin and Jan

Since all safety design activities are based on the system development activities all system design artifacts are part of the safety design process. Therefore, the following design artifacts of the CENELEC standard development process build the basis for all safety artifacts:

- System Concept

Table 2. Main openETCS safety design process activities

Safety Design Activity	Input Artifact(s)	Output Artifact(s)
Establish Safety Plan	QA-Plan + Project documentation (FPP, . . .)	Safety Plan
Preliminary Hazard Analysis (PHA)	Mainly SUBSET-91(+SUBSET-88)	Safety Goals + Safety Acceptance Criteria + PHA report
Sub-System Hazard and Risk Analysis (SSHA)	Safety Goals and Acceptance Criteria + SSRS + additional design and architecture specification + additional user constraints	Hazard Log (incl. Hazards and Safety Functions)
Specification of Sub-System Safety Requirements	SUBSET-26 + SUBSET-91 + Hazard Log	Safety Requirement Specifications
Update Hazard Log and corresponding Sub-System Safety Requirements	Verification Reports + Test Cases	Hazard Log + Sub-System Safety Requirements
Specify model specific Requirements	SSRS + Safety Requirement Specification	Safety Plan + Model Backlogs
Verify Safety Requirements	Models + Safety Requirements + Model Backlogs	Verification Report + Verification report
Validate Safety Requirements	Source Code + Safety Requirements	Validation Report + Validation report
Establish Safety Case	V and V Plan + Safety Plan + all requirements and specifications + V and V Reports	Safety Case

Table 3. CENELEC Safety Process Requirements

Standard	Section	Titel
EN 50126	4	Railway RAMS
EN 50126	6	RAMS lifecycle
EN 50128	Table A.3	Software Error Effect Analysis
EN 50129	5.3	Evidence of safety management
EN 50129	Annex A	Safety Integrity Levels
EN 50129	Annex B	Detailed technical requirements

- System Requirements Specification
- Software Requirement Specification
- Software Architecture Specification
- Software Design Specification
- Software Module Design Specification
- Software Source Code

The main safety artifacts are those which are set-up to build the reference for the safety-related aspect during the system development, which are continuously evolved during the design phases. Correspondingly the safety design process has to create artifacts to demonstrated that all safety and quality-related requirements included in the system design. Respectively the following artifacts are created during the safety design process:

- System Safety Plan
- Software Quality Assurance Plan
- Hazard Log
- System Safety Requirement Specification
- Safety Case

This artifacts have to be managed over the development process. Since all safety requirement have to be verified and validated there is likewise a close to all Test and Validation Reports.

4.1.3 Safety design activities

Process description has to be updated with the latest work. Cooperation between Cyril, Merlin and Jan

The safety design activities set-up or evolve the safety artifacts in relation to the different design artifacts. The following safety design activities are required according to the EN 50128:

- Preliminary Hazard Analysis
- Establish Safety Plan
- System Hazard and Risk Analysis
- Risk Assessment
- Specification of System Safety Requirements
- Define Safety Related Functional Requirements
- Specify Sub-System and Component Safety requirements
- Implement Safety Plan

- Verify System, Sub-System and Component Safety requirements
- Validate System Safety Requirements
- Establish Safety Case

Overall the safety design activities have to be performed in close relation to the overall verification and validation activities as these have to verify and validate all safety requirements and their results become part of the safety plan.

4.1.4 Safety Activities—User Sories

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

4.1.4.1 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

4.1.5 Important mile-stones

4.2 Safety Management

4.3 Safety design process supporting tools

Supporting software tools are needed to handle the safety artifacts and to some degree to more efficiently perform the safety design activities. As some safety artifacts like the safety requirement specifications and the safety backlogs are closely related to design artifacts the same tools can be used. Especially all requirements should be handled by one tool to ensure full traceability and provide one main interface for the verification and validation activities.

Depending on the methods used for hazard and risk analysis appropriate tools are needed to perform the analysis, collect the hazards and associated risks in the hazard log and to evaluated possible risk control measures. Thereby, traceability has to be guaranteed between all activities.

Since the safety plan and safety case provide the basis for the safety approval the tools used to generated these artifacts should help to generate a consistent argumentation and efficiently collect the data needed to provide evidence. Respectively, interfaces to manage documents and automatically generate reports would be helpful functionalities.

4.4 Safety Interfaces

Clear description of the interfaces to the process providing inputs for safety and using the Safety results. Specific describing the applied iterations.

4.4.1 Specific Interfaces to the Design Process

4.4.2 Interface to Quality Management

4.4.3 Interface to Verification

4.4.4 Interface to Validation

4.5 Safety Documentation

Short description for the needed documentation

5 Conclusion

References