OETCS/WP4/D4.2-Draft

openETCS

ITEA2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

**ITEA2 Project**
**Call 6 11025**
**2012 – 2015**

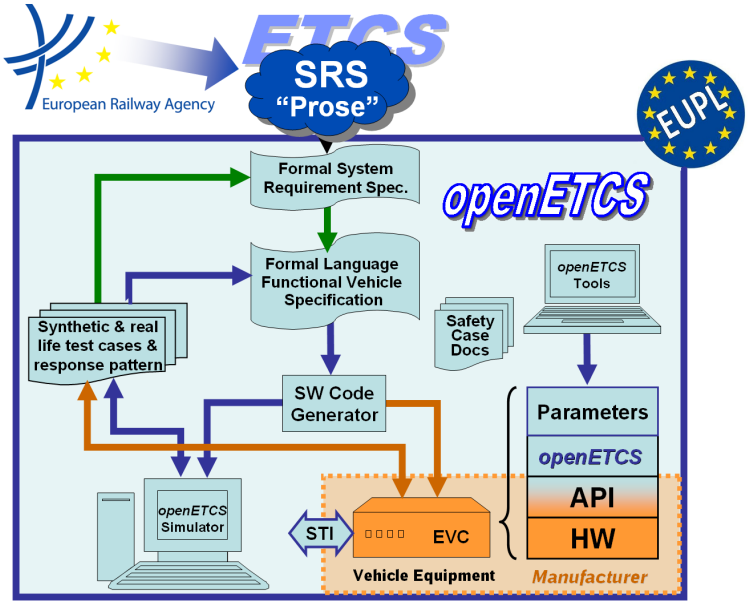
Work-Package 4: “Verification and Validation”

# Preliminary safety Evaluation Criteria

**Latex Document Draft**

Jan Welte

May 2013
Revised May 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: “Verification and Validation”**

**OETCS/WP4/D4.2-Draft**
**May 2013**
**Revised May 2013**

# Preliminary safety Evaluation Criteria

**Latex Document Draft**

Jan Welte

Technische Universität Braunschweig
Institute for Traffic Safety and Automation Engineering
Langer Kamp 8
38118 Braunschweig
Germany

Output for secoundary tool evaluation

Prepared for openETCS@ITEA2 Project

**Abstract:** This document presents an overview of the safety related evaluation criteria used within the openETCS document structure and based on this derives evaluation criteria for the choice of suitable tools and methods for all safety activities which have to be performed during the openETCS development process. These criteria are based on the safety activities required in D2.6 and the general concept for an openETCS safety process.

# Table of Contents

# Figures and Tables

## Figures



## Tables

# 1 Safety Process

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 characteristics and the properties are demonstrated by the Risk-Genesis-Model of Schnieder, which is shown in the following figure 1.

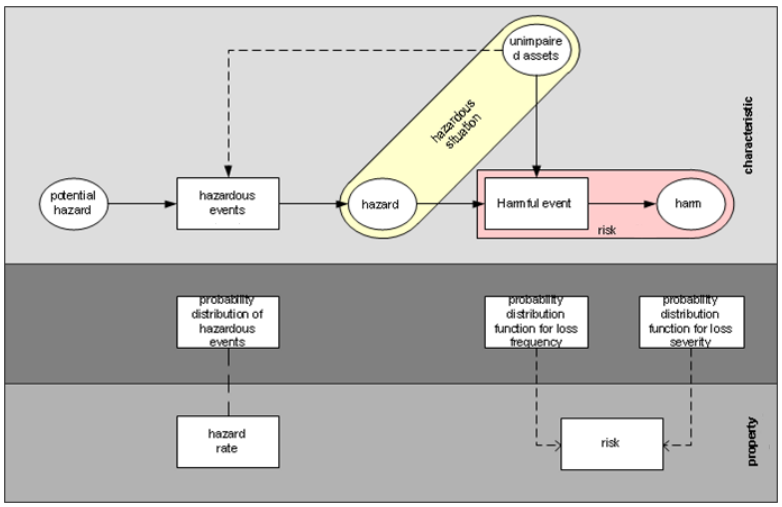



**Figure 1. Risk-Genesis-Model showing the relations between the safety-related terms [? ]**

This demonstrates that the first step is to define the system characteristics of a system identifying the harms and their lated hazardous situations. This has to be performed during a system hazard analysis. Afterwards the specific properties of this characteristics have to be defined by assessing the risk concerning the identified hazards. Based on this work safety integrity levels can be determined for all safety functionalities which are then allocated during the design to certain safety-related systems. As this work is closely related to all design decisions, it has to be specified for all abstraction levels during the system design. This leads to safety requirements which have to be implemented in the software design and verified, as well as validated specifically on system level.

Respectively the EN50126 describes the safety 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 by different safety activities.

## 1.1 Safety artifacts

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

- System Concept
- 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 process has to create artifacts to demonstrated that all safety and quality-related requirements included in the system design. Respectivly the following artifacts are created during the safety 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.

### 1.2 Safety activities

The safety activities set-up or evolve the safety artifacts in relation to the different design artifacts. Respectively, every activity has certain input and output artifacts as defined in table 1:

Overall the safety 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.

### 1.3 OpenETCS safety 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 process.

### 1.4 Tools for safety activities

## 2 Evaluation Criteria

### 2.1 Safety artifacts

Abbreviation Verification Categorization Degree of Formalisation C Code: used for the executable model Strictly-Formal 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 dM

**Table 1. Safety Activities and their inputs and outputs**

| Safety Activity | Input Artifact(s) | Output Artifact(s) |
|---|---|---|
| Preliminary Hazard Analysis | System Concept | Safety Plan |
| System Hazard and Safety Risk Analysis | System Concept and Description | Hazard Log |
| Risk Assessment | System Concept and Description + Hazard Log | Hazard Log |
| Specification of System Safety Requirements | System Requirements Specification + Hazard Log | System Safety Requirement Specifications |
| Define Safety Acceptance Criteria | Hazard Log | Safety Plan |
| Define Safety Related Functional Requirements | System Safety Requirement Specifications | System Requirements Specification |
| Specify Sub-System and Component Safety requirements | System Requirements Specification + System Safety Requirement Specification | System Safety Plan + System Requirements Specification + System Safety Requirement Specification |
| Implement Safety Plan | Safety Plan | Hazard Log + Safety Case |
| Validate System Safety Requirements | System Safety Requirements | Safety Case |

Detailed Model: model used for code generation 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 HL Hazard Log: List of identified hazards and its associated risk classification as well as information concerning the risk control Informal hLSB High Level Safety Backlog: list of requirements/ properties to be implemented inside the hM derived from the HL Informal/ Semi-Formal hM "Higher Model: model derived from srsM or another hM and used as an input for dM or another level of hM" Semi-Formal/ Strictly-Formal SSHA Subsystem Hazard Analysis: Safety Analysis of the openETCS subsystem and ist interfaces defined in the SSRS Informal/ Semi-Formal Subset-026 Subset 26 version 3.3.0 of the Control Command and Signalling Technical Specification of Interoperability of the trans-European rail system Informal Subset-088 Subset-088 version 2.3.0 ETCS Application Levels 1 and 2 - Safety Analysis Informal/ Semi-Formal Subset-091 Subset-091 version 3.2.0 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2 Informal PHA Preliminary Hazard Analysis of the System, which is mainly delivered based on subset-88 and subset-91 Informal Safety Goals General Safety Goal defined for the System mainly related to the accepted level of risk Informal/ Semi-Formal/Formal 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

## 2.2 Safety activities

Abbreviation System Level Activies Degree of formalisation PHA + subset-26->SSHA Hazard Analysis of the Sub System mainly to identify relevant hazards Informal -> Informal/Semi-formal SSHA->HL Identifying all relevant risks in the subsystem and determining their risk and possible control activities Informal -> Informal/Semi-formal HL->SafetyReq Deriving

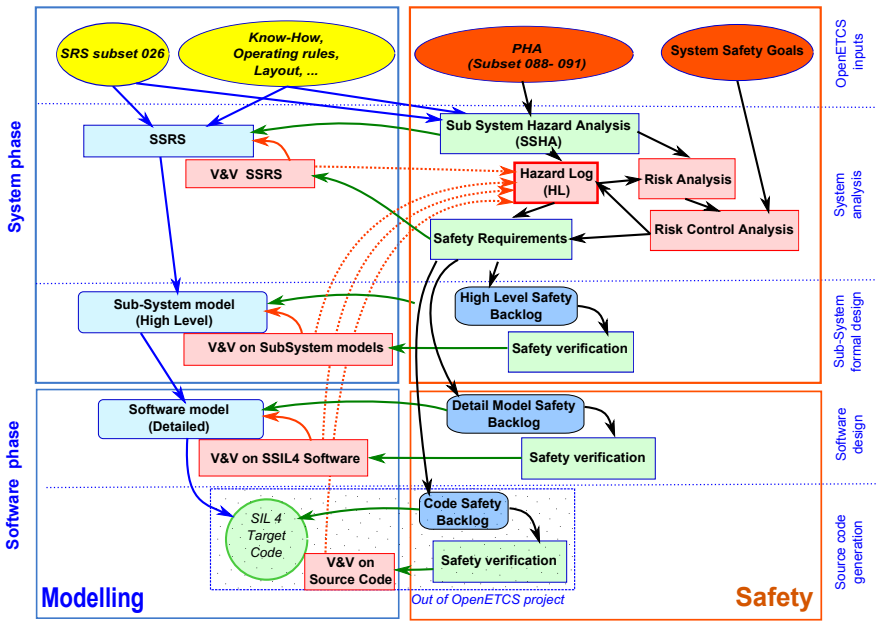



**Figure 2. OpenETCS Safety Process**

safety requirements for the subsystem based on all relevant hazards and their associated risk controls Informal/Semi-formal -> Informal/Semi-formal SafetyReq->hLSB Transformation of all relevant requirements to the level of abstraction of the high level model Informal/Semi-formal -> Informal/Semi-formal SafetyReq->dMSB Transformation of all relevant requirements to the level of abstraction of the detailed Software model Informal/Semi-formal -> Semi-formal/Strictly-Formal SafeReq->CSB Transformation of all relevant requirements to the source code abstraction level Informal/Semi-formal -> Strictly-Formal hM/dM/C->HL Continuous hazard identification during the modelling and model analysis Informal/Semi-formal -> Informal/Semi-formal

Abbreviation Verification Activities Degree of formalisation hM->Safety Req/hLSB 1. Verification of the higher model against the high level safety requirements Informal -> Semi-formal/ Strictly-Formal dM->Safety Req/dMSB 2. Verification of the detailed model against the detail safety requirements Semi-formal/ Strictly-Formal -> Semi-formal/ Strictly-Formal C->Safety Req/CSB 3. Verification of code against the code safety requirements Semi-formal/ Strictly-Formal -> Strictly-Formal

Abbreviation Validation Activities Degree of formalisation C->HL 1. Validation of the implemented system against all identified hazards and their associated risk Semi-formal/ Strictly-Formal -> Semi-Formal/ Informal

### 2.3 Tools for safety activities

## References