ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

# WP4 Review Meeting
# Task 4 - Verification of the tools and processes

supported by:

Federal Ministry of Education and Research

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

INVESTISSEMENTS D'AVENIR

Région de Bruxelles-Capitale

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN

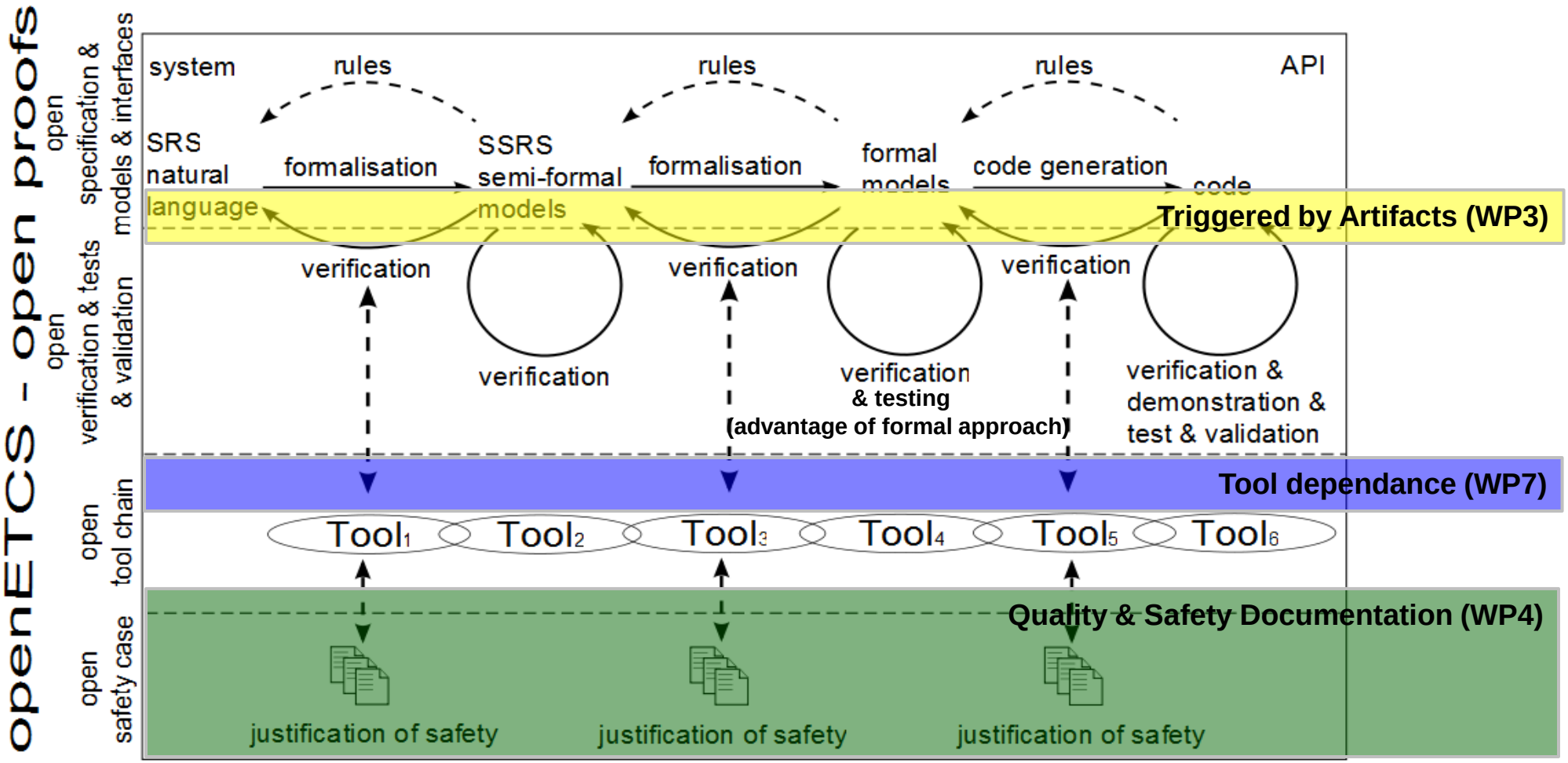

openETCS@ITEA2 Project

Jan Welte, TU-BS


München, 14.01.2014

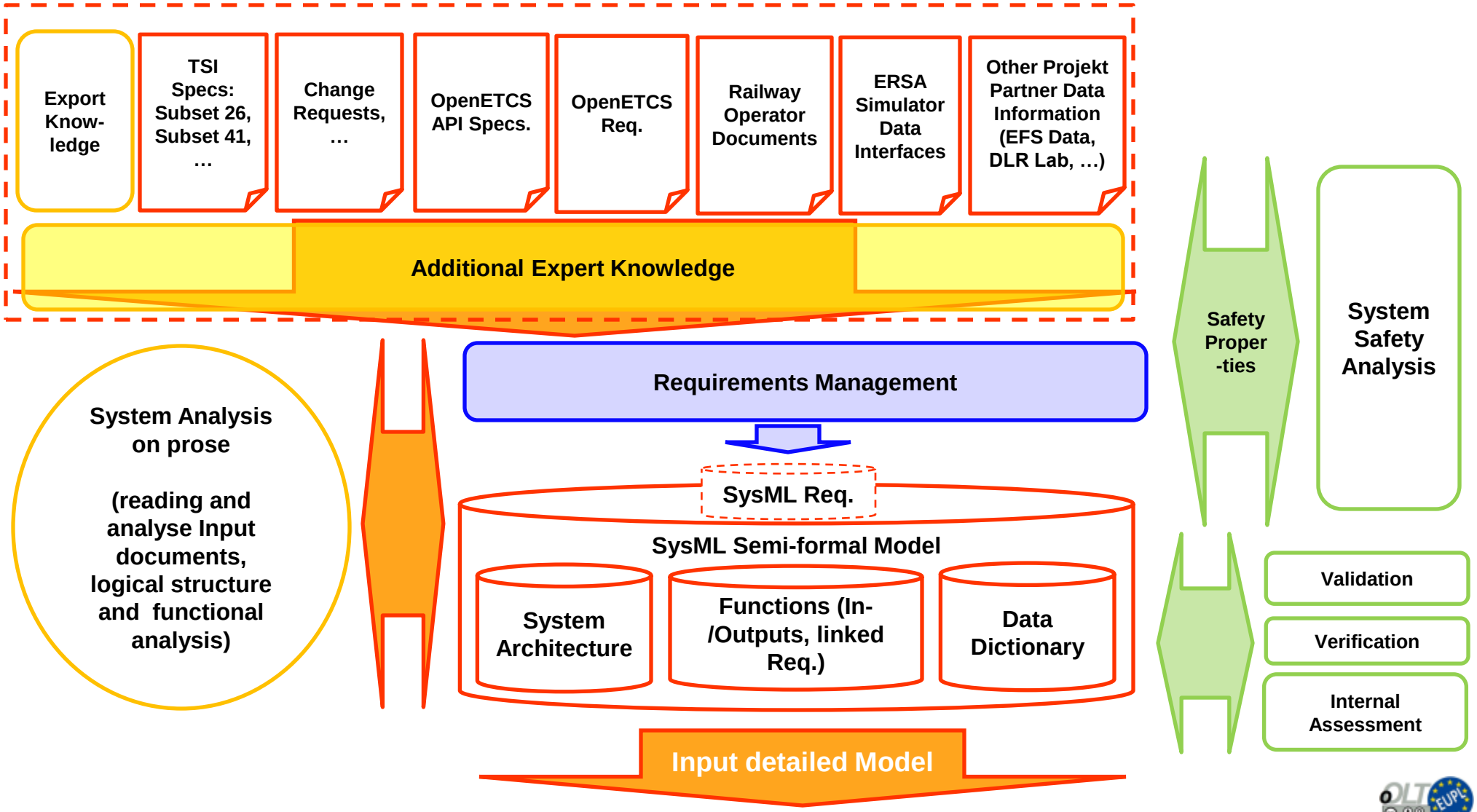
# Process and Tool Verification

## Two Major User Interfaces & Early Model-Based Testing



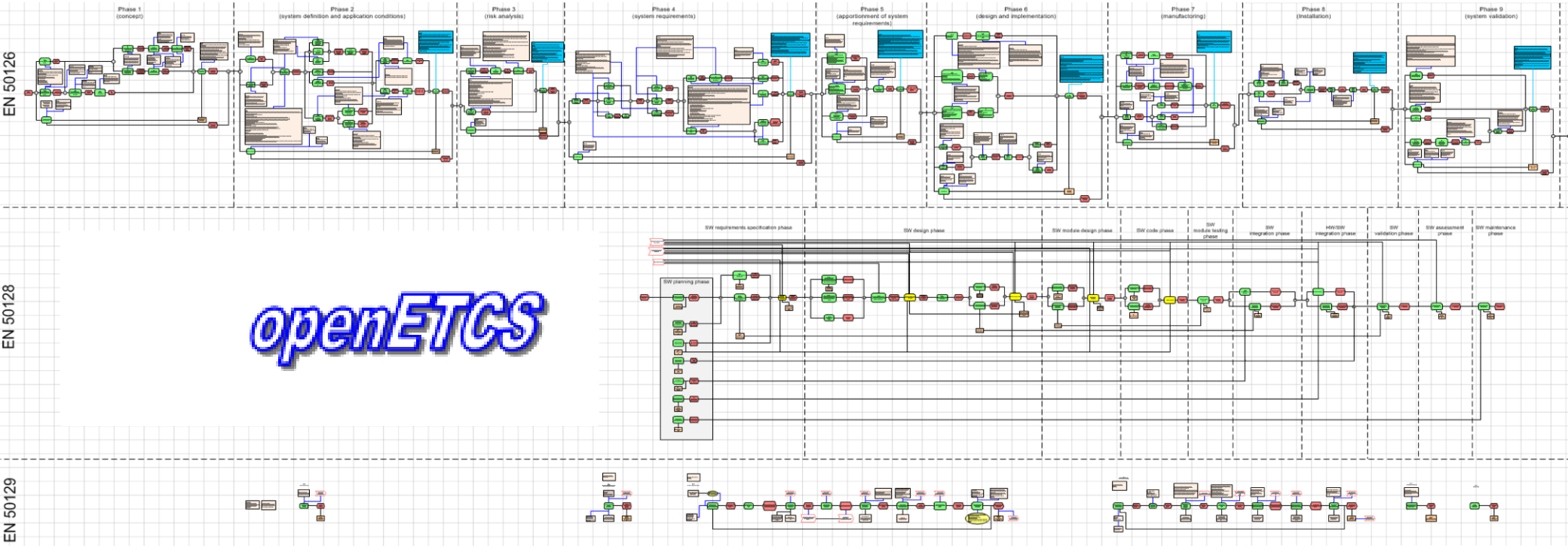
# Development Process and Toolchain

## Interfaces with early design phase



# EN 5012x Development Process

## Standard provides overall process structure



# Safety Case

## Transparency of the Safety Argumentation

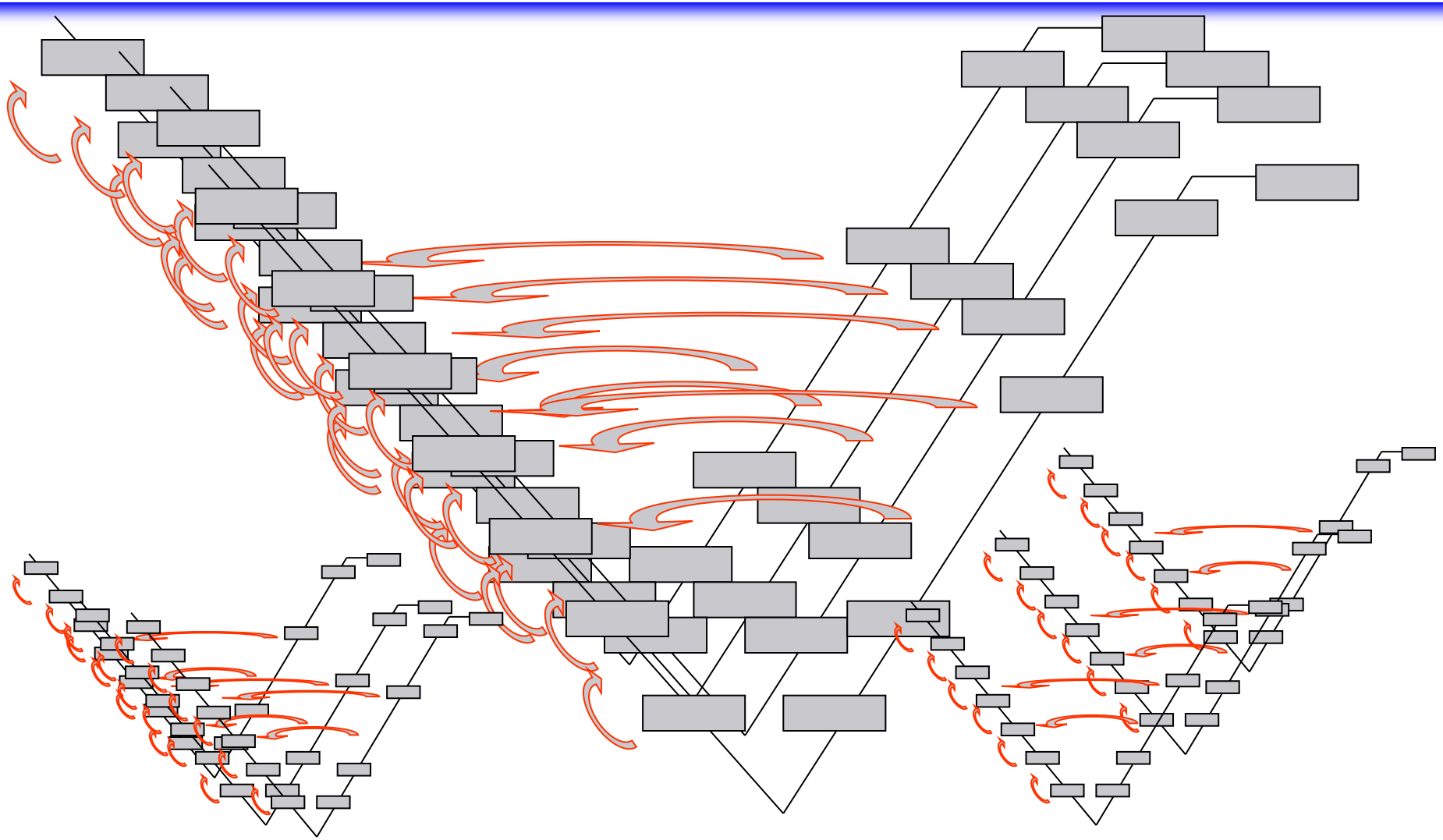
**A safety case is "the documented demonstration that the product complies with the specified safety requirements." [EN 50129]**

**"The safety case is a line of argumentation, not just a collection of facts."[Odd Nordland, SINTEF]**

**A safety case is "A *structured argument*, supported by a *body of evidence* that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment." [UK Defense Standard]**

# Safety Case

## High Complexity of different argumentations



# Goal Structuring Notation

## Modeling the argumentation structure

| Element | Description |
|---|---|
| Goal | A goal is a requirement, target or constraint to be met by the system. The term goal hierarchy refers to the collection of goals produced by the hierarchical decomposition of goals into sub-goals. |
| Strategy | A goal (or set of goals) can be solved by a strategy, which breaks a goal into a number of sub-goals. The satisfactory solution of the sub-goals then entails the solution of the original goals. A strategy can be regarded as a rule to be invoked in the solution of goals. |
| Solution | Some goals may be solved directly by what we term solutions, rather than by decomposition into sub-goals. This is where the high level argument links to and uses the supporting evidence. Solutions will be individual pieces of analysis, evidence, results of audit reports, or references to design material including models. In fact we are not restrictive at all of the form that solutions can take. |
| Justification J | Strategies often need some justification for their use. It may be that the strategy is laid down in some standard followed by the developers: it may be common practice; or it may be a more elaborate argument as to the validity of the use of the strategy. Alternatively a justification may call upon evidence from analysis of the model or be a structured proof. |
| Assumption A | Any assumption on which the strategy or goal is being put forward as a solution to the parent goal. |
| Context | Additional contextual information to a goal, a strategy or any other element can be couched in a context element. |

# Goal Structuring Notation

Modeling the argumentation structure

a) **GSN is suitable to clarify the chain of arguments**

b) **The arguments focus on the essentials.**

c) **The GSN thus reduces the overhead**

d) **It improves the overview**

e) **Facilitate the maintenance of durable Safety's case, since it gives a good summary.**

f) **If the security argument is well known and standardized, even larger development projects carried out in parallel.**

g) **Contains implicitly the structure of the project schedule.**

# Goal Structuring Notation

## Example for OpenETCS

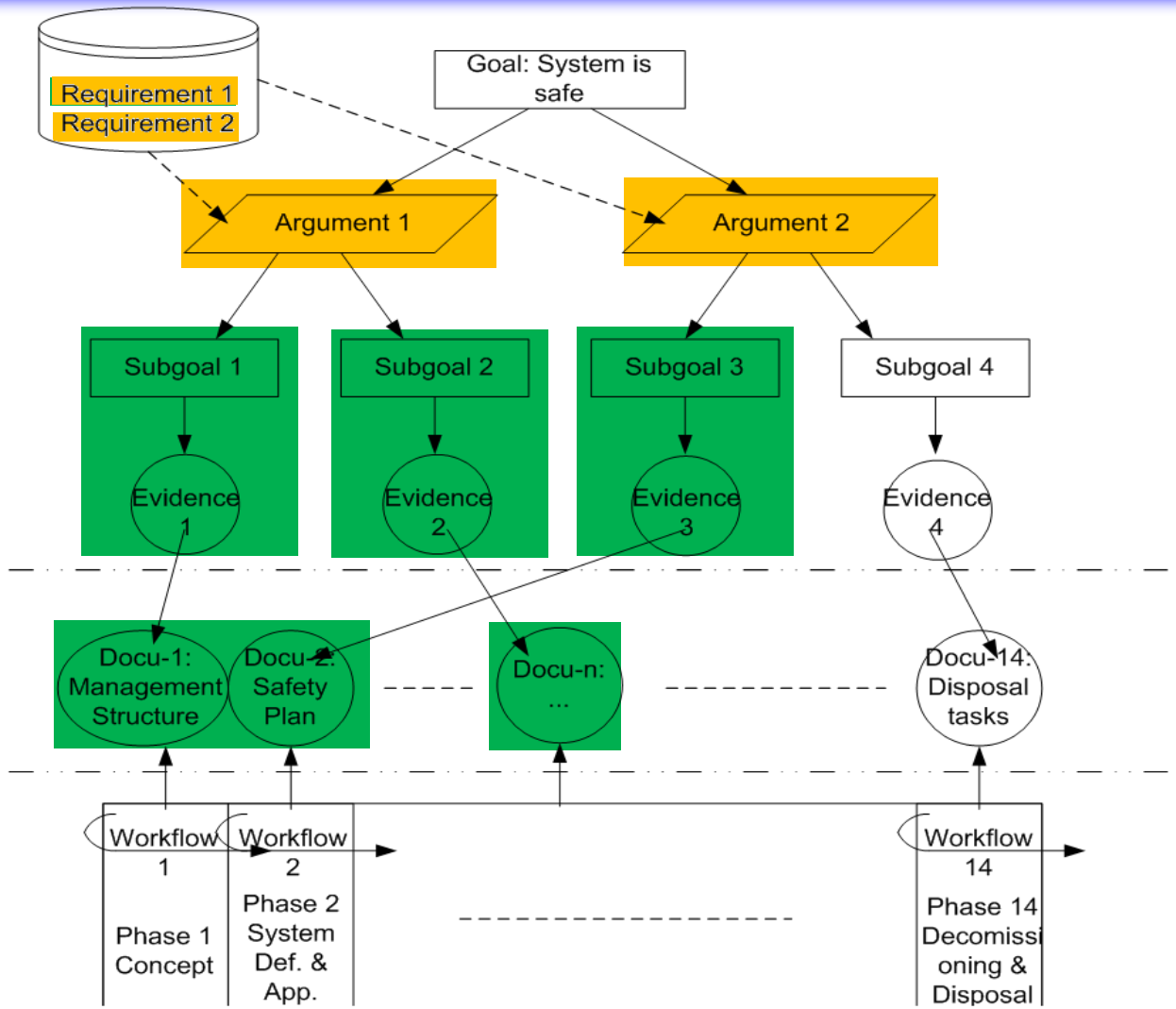
**Overall System Goals („Goal Structure“)**

**Structured argument**

**Body of evidence**

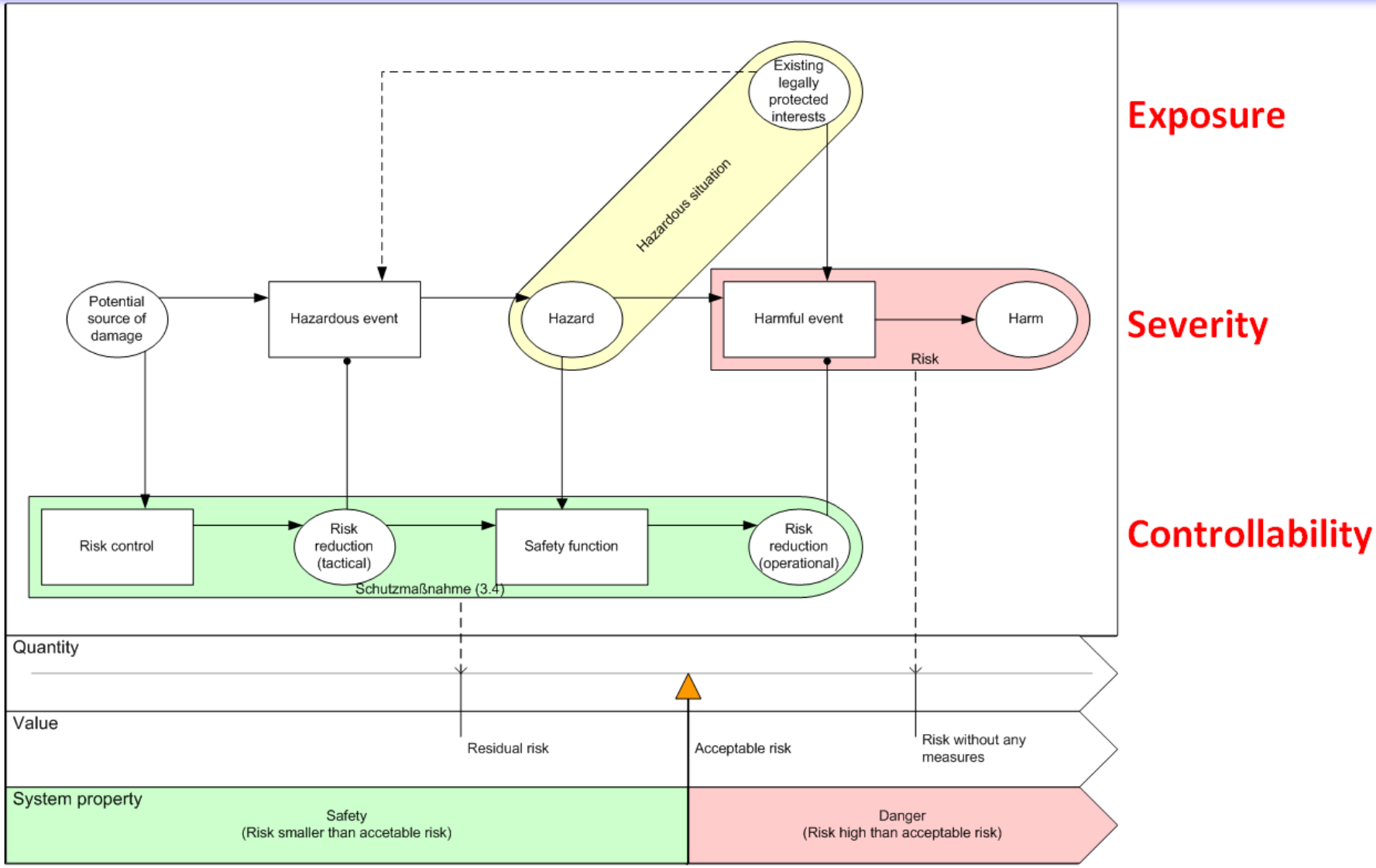
**Database of Documents**

**Document Management System (Github)**



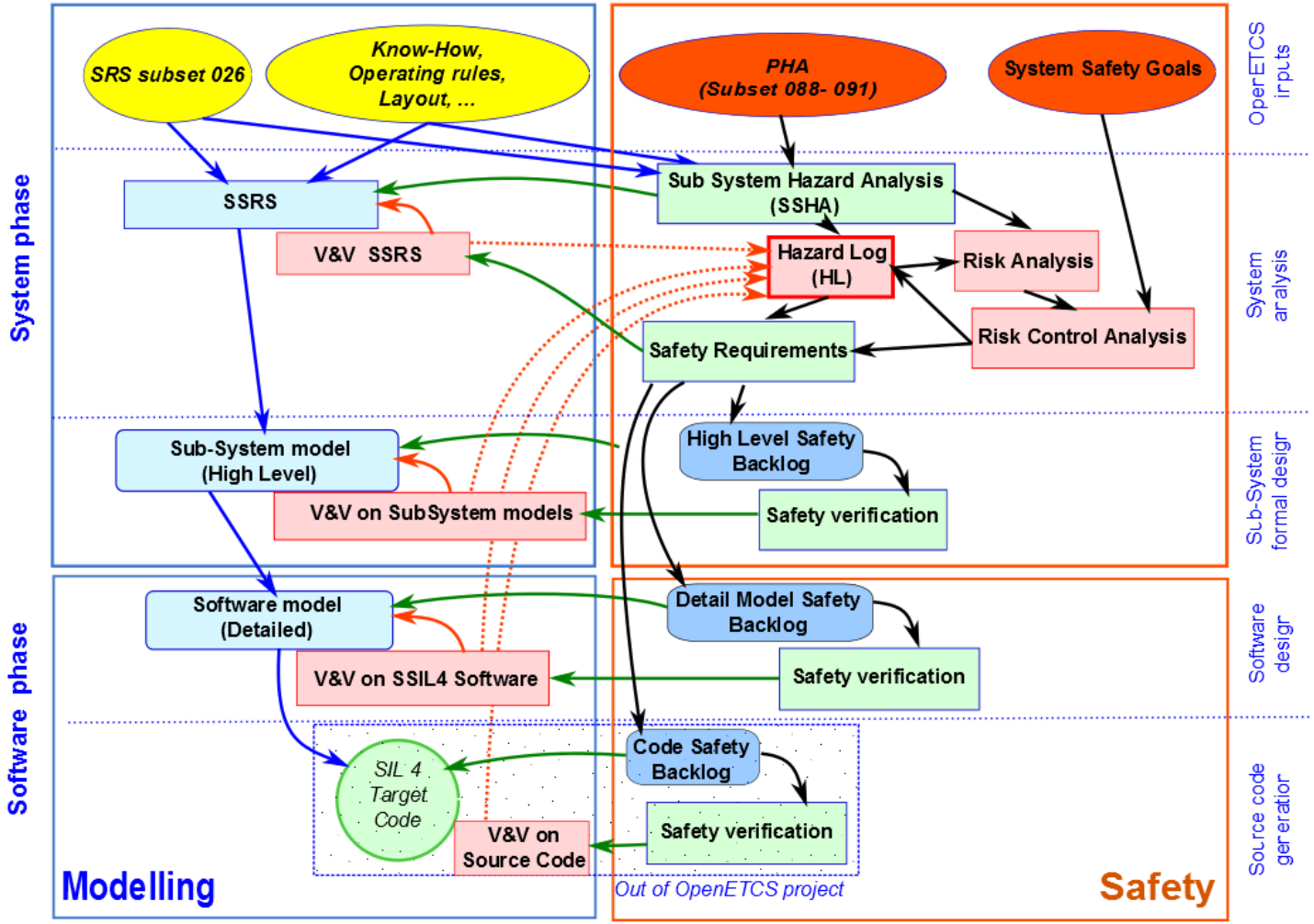
# Safety

## Risk-Genesis-Model



# Safety Process Structure

## Overview for OpenETCS



# Safety Process

VnV Level 1 Safety work

**Objectives:**

- implement parts of the safety strategy on existing benchmark models
- establish details for artifact relations and traceability

**Main focus:**

- hazard identification
- Determination of resulting requirements

# Safety Process

## VnV Level 1 Safety – hazard identification

Identification is lead by the **Core Hazard**

*Exceedance of the safe speed / distance as advised to ETCS*

Maximum rate of occurrence for the core hazard (THR for ETCS) has been defined to

$$2.0 * 10^{-9}\ hour^{-1}\ train^{-1}$$

Based on

| | |
|---|---|
| *SUBSET 91* | *Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 (Baseline 3)* |
| *SUBSET 88* | *ETCS Application Levels 1 & 2 - Safety Analysis* |

# Safety Process

## VnV Level 1 Safety – Proof of Concept for MoRC

### List of Hazardous Events

- 34 events assigned to the kernel resulting in the core hazard are listed in SUBSET 91 Annex A

### Proof of Concept

### (by Systerel, AEBT and All4Tec)

- Based on Hazard KERNEL-6
- Hazard Analysis for benchmark model on MoRC
- Derived Safety Criteria based on a FMEA for the subsystem

| Event Id. | Event Description | Corresponding performance requirement in SUBSET-041 |
|---|---|---|
| KERNEL-1 | Balise linking consistency checking failure | In case the message is received but the linking is not consistent:<br>5.2.1.1: Delay between receiving of a balise message and applying the emergency brake |
| KERNEL-2 | Balise group message consistency checking 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 | |
| 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 com- |

# Safety Process

## VnV Level 1 Safety – Results

### Specific for the Proof of Concept

- FMEA has been successfully done on the SysML model of MoRC
- 18 Safety Criteria have been defined
- Traceabilty has been established to SUBSET 26
- Results can be found at *https://github.com/openETCS/validation/blob/master/VnVUserStories/VnVUserStorySysterel/04-Results/a-SafetyAnalysis/safety_analyse_MoRC_4A.doc*

### 3.3. FMEA

| #¤ | Function¤ | Failure·mode¤ | Effect¤ | Hazard¤ | Detectability¤ | SIL¤ | Safety·Criteria¤ | Comment¤ |
|---|---|---|---|---|---|---|---|---|
| 1¤ | register·mobile·terminal¤ | Absence¤ | The·Mobile·Terminal·is·not·registered·to·the·radio·network.·Communication·with·trackside·equipment·is·not·possible.¤ | yes¤ | Detectable¤ | SIL-4¤ | REQ_FMEA_ID_001¶ The·Mobile·Terminal·shall·be·safely·registered·to·a·Radio·Network.¶ ¤ | ¤ |
| 2¤ | | Loss¤ | The·Mobile·Terminal·is·not·registered·to·the·radio·network.·Communication·with·trackside·equipment·is·not·possible.¤ | yes¤ | Detectable¤ | SIL-4¤ | REQ_FMEA_ID_002¶ The·driver·shall·be·safely·informed·of·the·state·of·the·radio·communication·(resulting·of·the·different·steps:·registration·of·the·Mobile·Terminal·to·the·Radio·Network,·establishment·of·the·communication,·end·of·communication).¶ ¤ | ¤ |
| 3¤ | | Inadvertent¤ | The·Mobile·Terminal·changes·form·a·radio·network·to· | yes¤ | Detectable¤ | SIL-4¤ | REQ_FMEA_ID_003¶ If·a·communication·through·a·Radio· | ¤ |

### 5. SAFETY CRITERIA

*REQ_FMEA_ID_001*

The Mobile Terminal shall be safely registered to a Radio Network.

*REQ_FMEA_ID_002*

The driver shall be safely informed of the state of the radio communication (resulting of the different steps: registration of the Mobile Terminal to the Radio Network, establishment of the communication, end of communication).

*REQ_FMEA_ID_003*

If a communication through a Radio Network is active, registration of the associated Mobile Terminal to another Radio Network mustn't be performed.

*REQ_FMEA_ID_004*

A safety protocol shall be used to performed communication between Mobile Terminal and Radio Network.

*REQ_FMEA_ID_005*

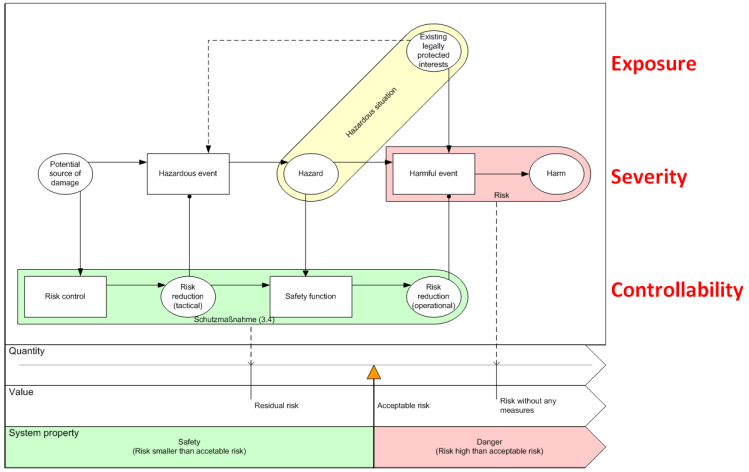
If a communication with trackside equipment is active, set-up of safe radio connection with another trackside equipment mustn't be performed. Exception in case of handover with RBC.

# Safety Process

## VnV Level 1 Safety – Results overall safety process

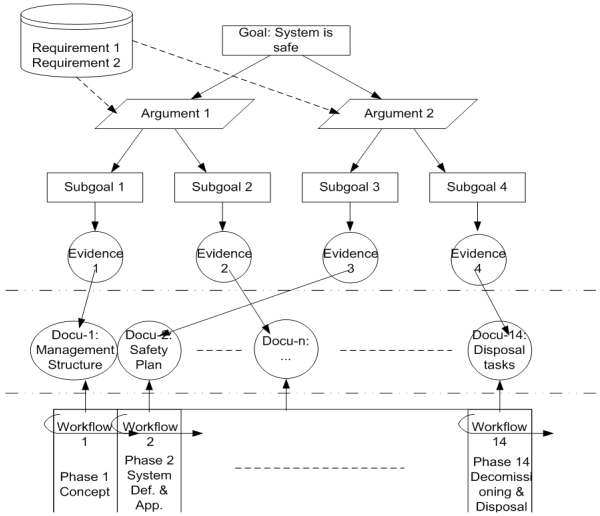
### Overall results

- Definition of generic safety process
- Proposed process for hazard analysis and safety criteria definition is suitable for openETCS design process
- Certain level of architecture and data information are needed for the safety analysis




### Open Points

- Intergration of safety requirements in the design process
- Proof of Concept for tool safety analysis
- Integration of safety tools in the tool chain



# Questions or Discussion

Technische Universität Braunschweig

Institut für Verkehrssicherheit und Automatisierungstechnik iVA

Prof. Dr.-Ing. Dr. h.c. mult. E. Schnieder

**Task 4.4 Verification of the tools and processes**

Jan Welte

TU Braunschweig

Institute for Traffic Safety and Automation Engineering
welte@iva.ing.tu-bs.de