ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

WP4 – 1st Workshop on Safety Assessment
OpenETCS Safety Activities

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

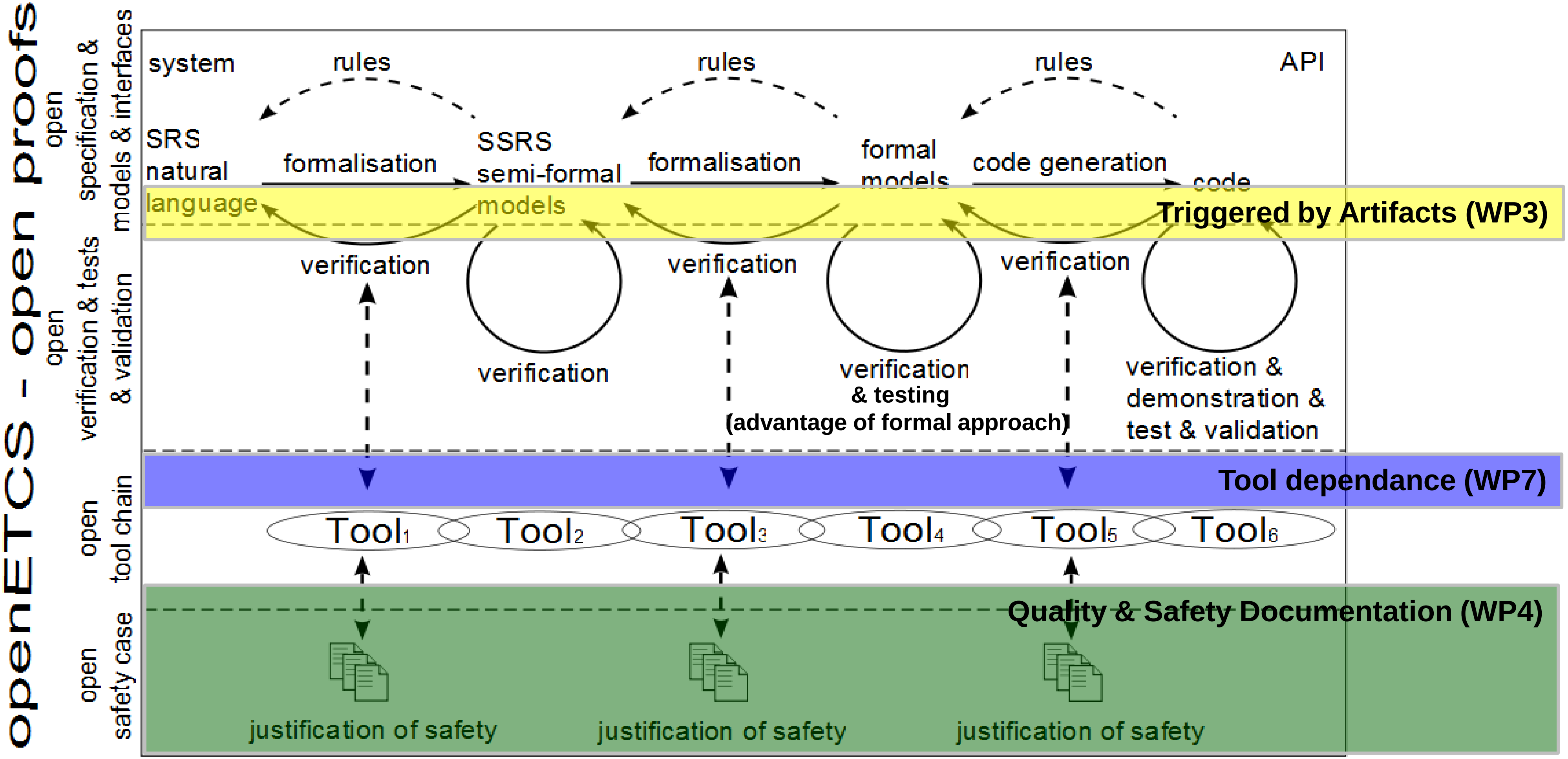
openETCS@ITEA2 Project

Jan Welte, TU-BS

Nürnber, 18.02.2014

Process and Tool Verification

Two Major User Interfaces & Early Model-Based Testing



openETCS - open proofs

open specification & models & interfaces

open verification & tests & validation

open tool chain

open safety case

system

rules

rules

rules

API

SRS natural language

formalisation

SSRS semi-formal models

formalisation

formal models

code generation

code

Triggered by Artifacts (WP3)

verification

verification

verification

verification

verification & testing (advantage of formal approach)

verification & demonstration & test & validation

Tool dependance (WP7)

Tool1 Tool2 Tool3 Tool4 Tool5 Tool6

Quality & Safety Documentation (WP4)

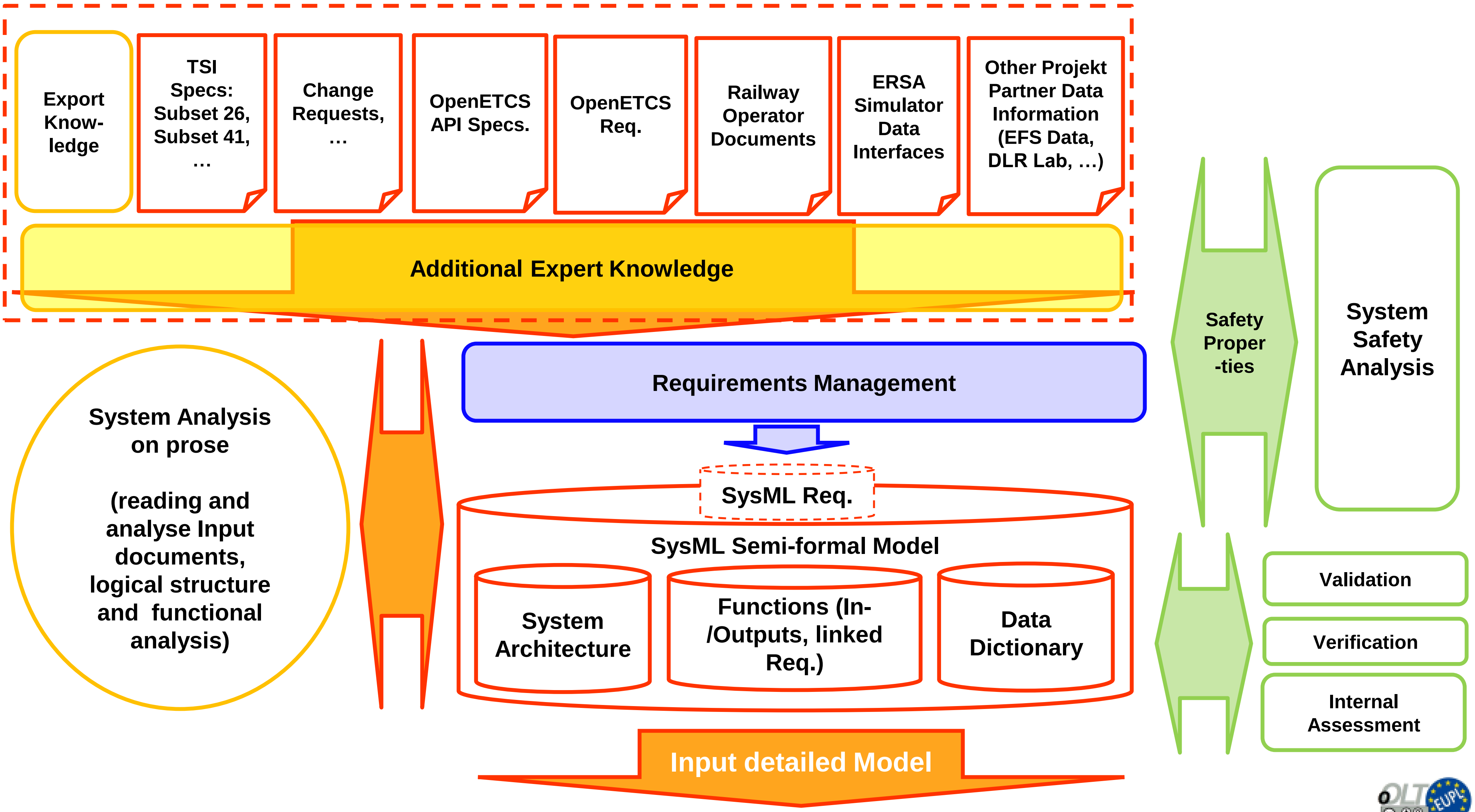
justification of safety

justification of safety

justification of safety

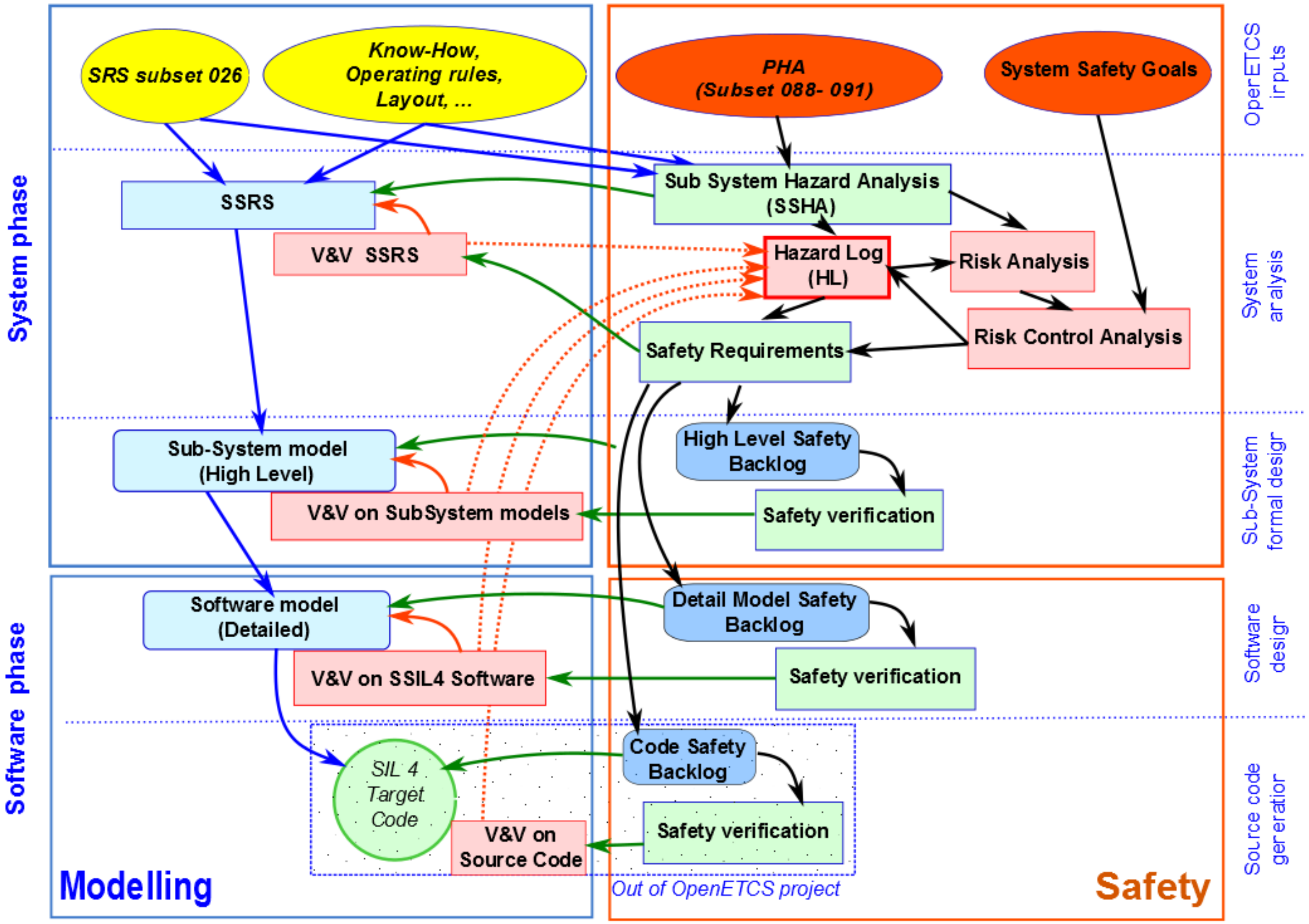
Development Process and Toolchain

Interfaces with early design phase


Export Know-ledge
TSI Specs: Subset 26, Subset 41, …
Change Requests, …
OpenETCS API Specs.
OpenETCS Req.
Railway Operator Documents
ERSA Simulator Data Interfaces
Other Projekt Partner Data Information (EFS Data, DLR Lab, …)
Additional Expert Knowledge
Safety Proper-ties
System Safety Analysis
System Analysis on prose
(reading and analyse Input documents, logical structure and functional analysis)
Requirements Management
SysML Req.
SysML Semi-formal Model
System Architecture
Functions (In-/Outputs, linked Req.)
Data Dictionary
Validation
Verification
Internal Assessment
Input detailed Model

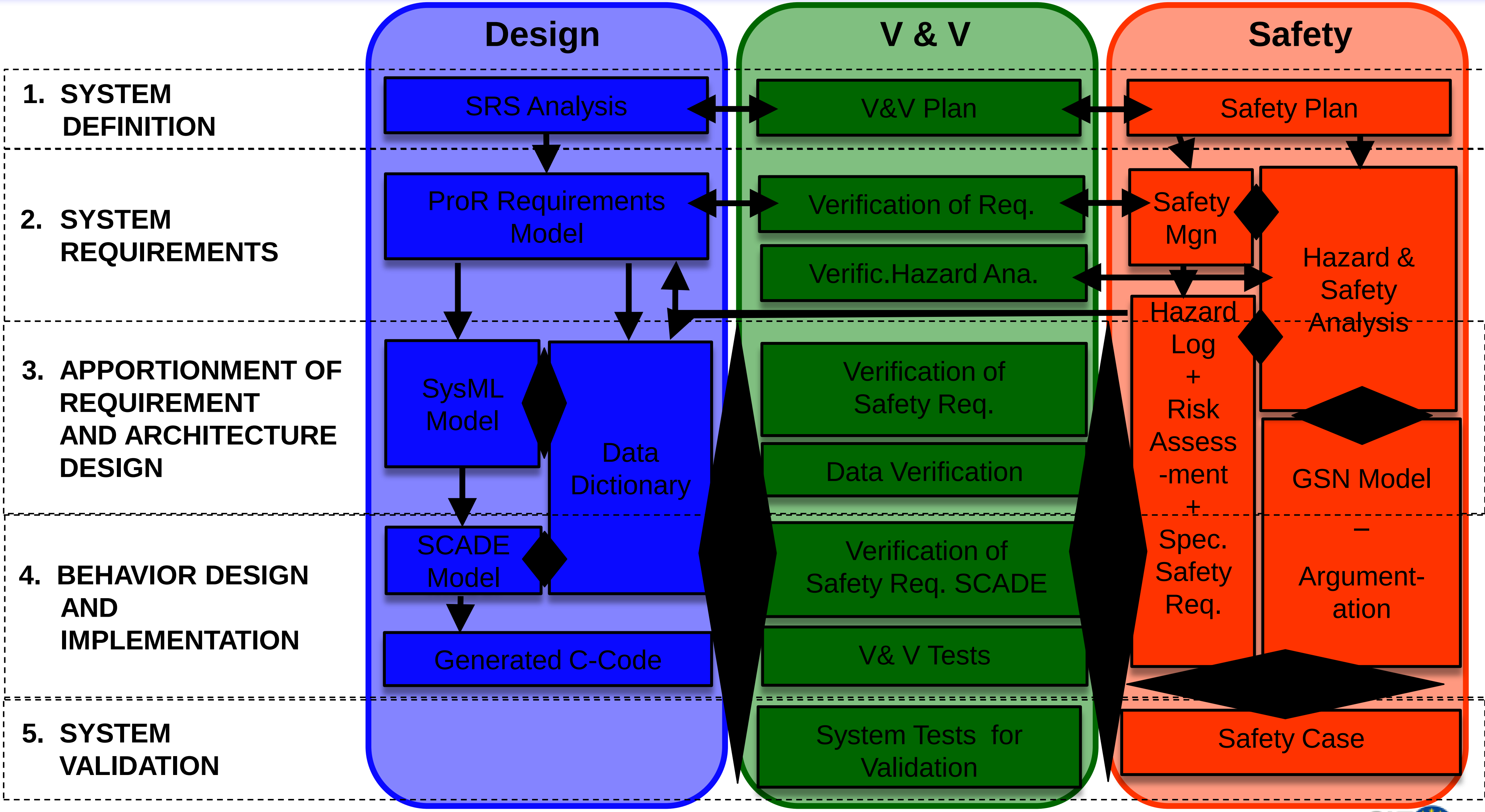
Safety Process Structure

Overview for OpenETCS



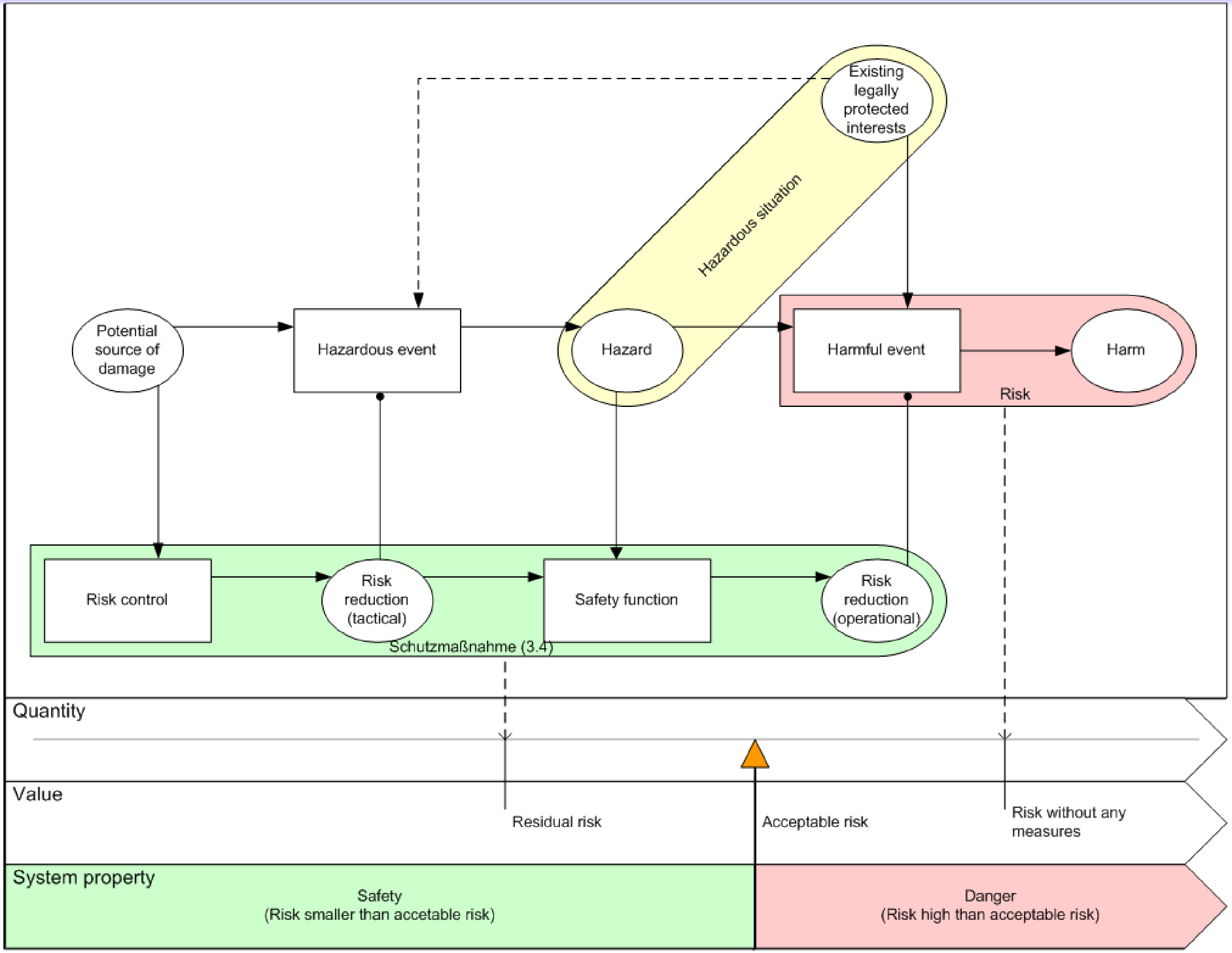
Safety Process Structure

Overview Artifacts



Safety

Risk-Genesis-Model


Existing legally protected interests
Hazardous situation
Potential source of damage
Hazardous event
Hazard
Harmful event
Harm
Risk
Risk control
Risk reduction (tactical)
Safety function
Risk reduction (operational)
Schutzmaßnahme (3.4)
Quantity
Value
Residual risk
Acceptable risk
Risk without any measures
System property
Safety (Risk smaller than accetable risk)
Danger (Risk high than acceptable risk)

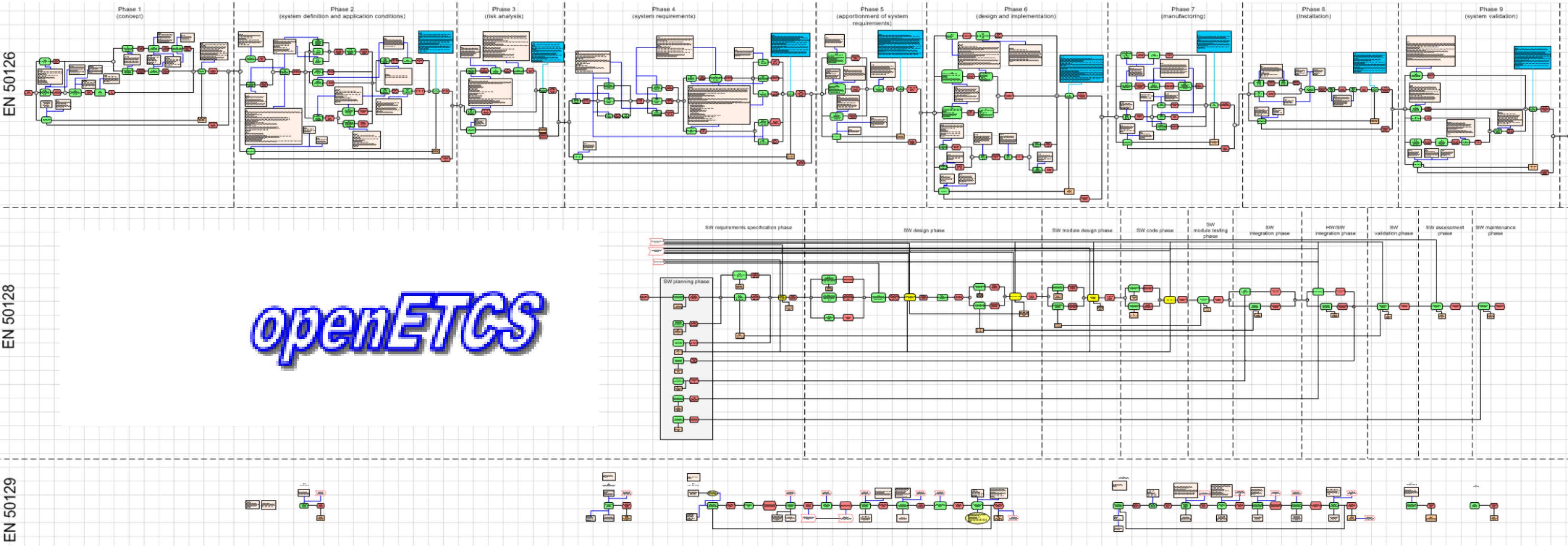
Exposure

Severity

Controllability

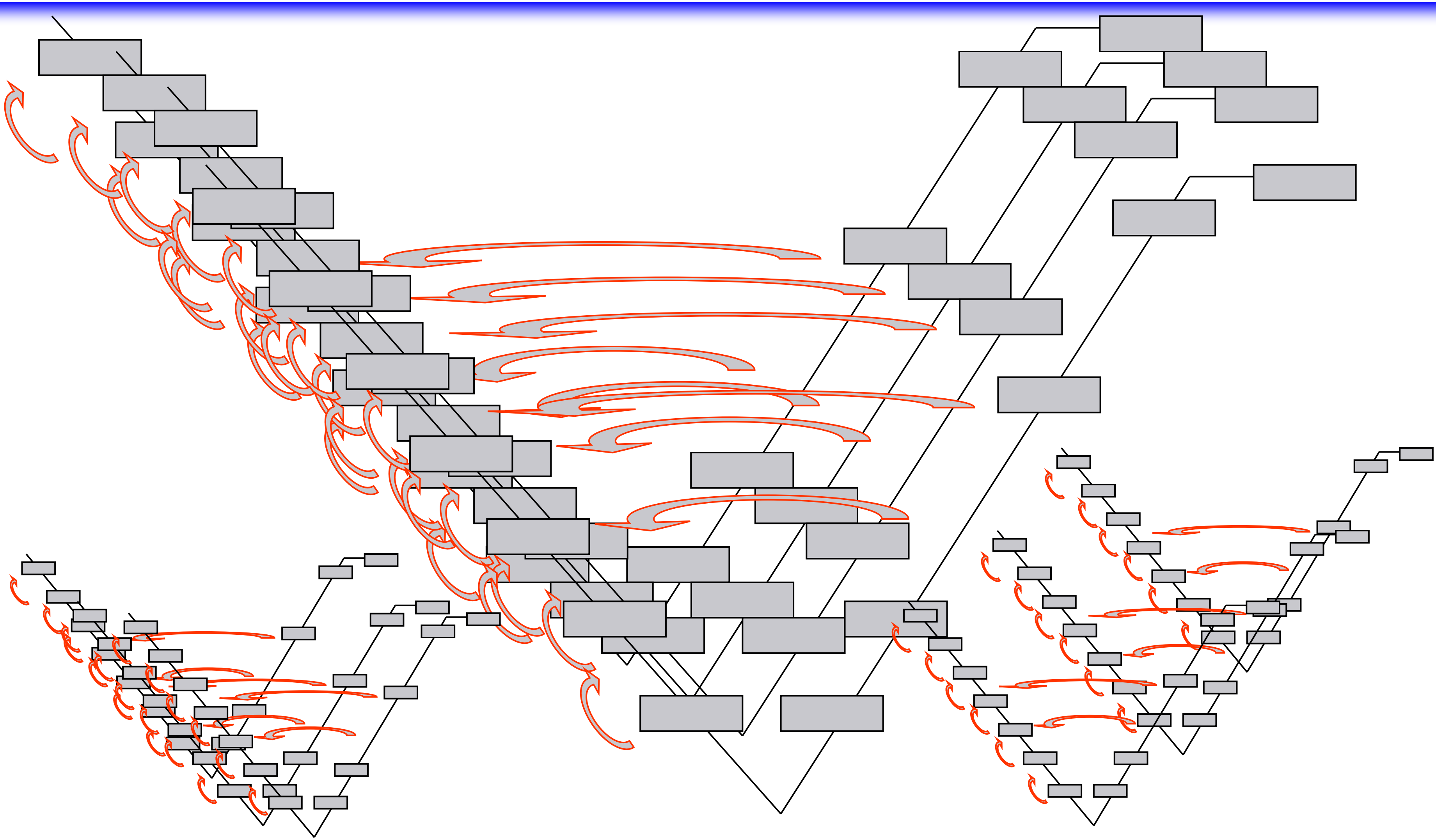
EN 5012x Development Process

Standard provides overall process structure



Safety Case

High Complexity of different argumentations



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]

Goal Structuring Notation

Example for OpenETCS

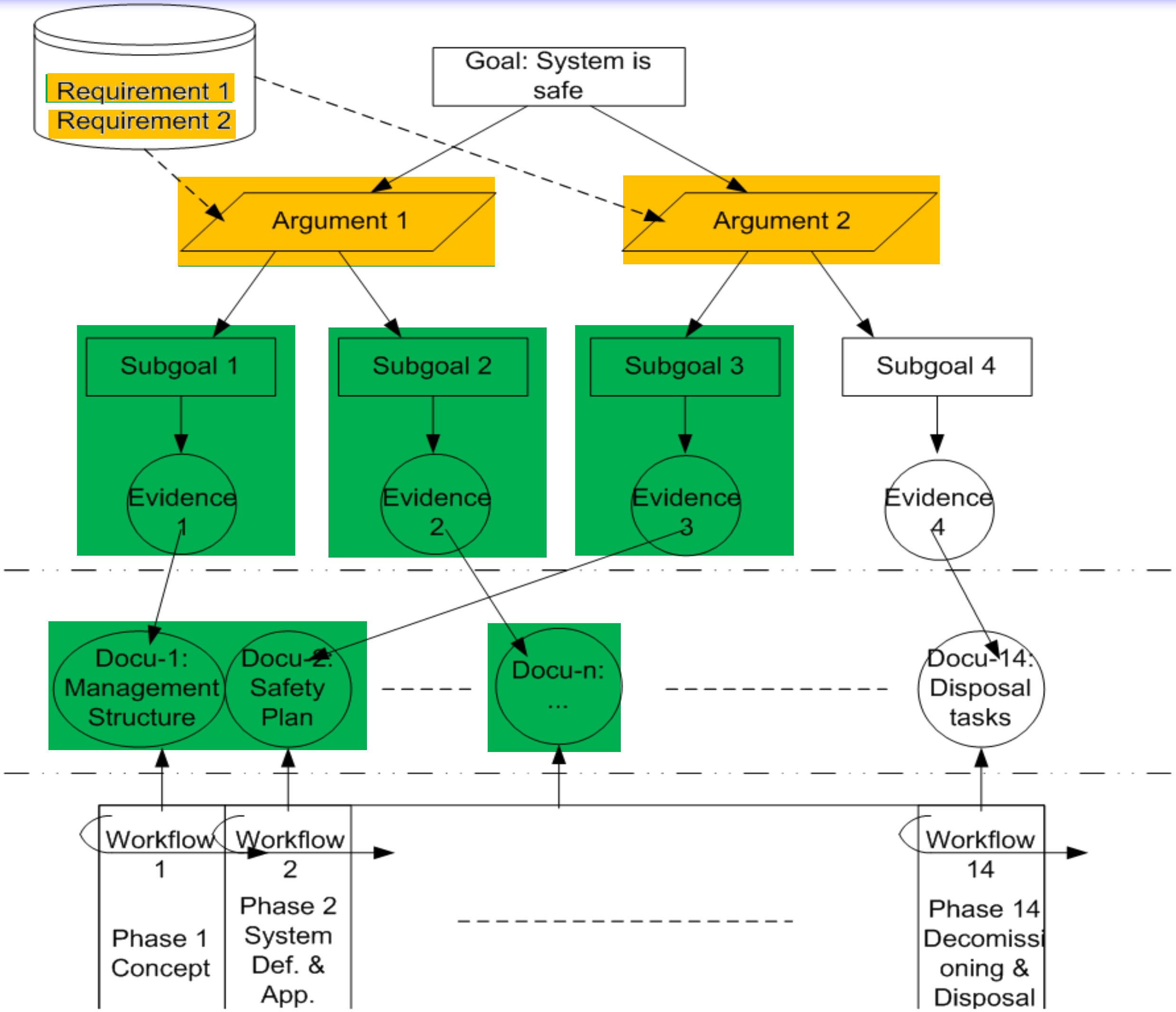
Overall System Goals („Goal Structure“)

Structured argument

Body of evidence

Database of Documents

Document Management System (Github)



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.

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

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

Based on

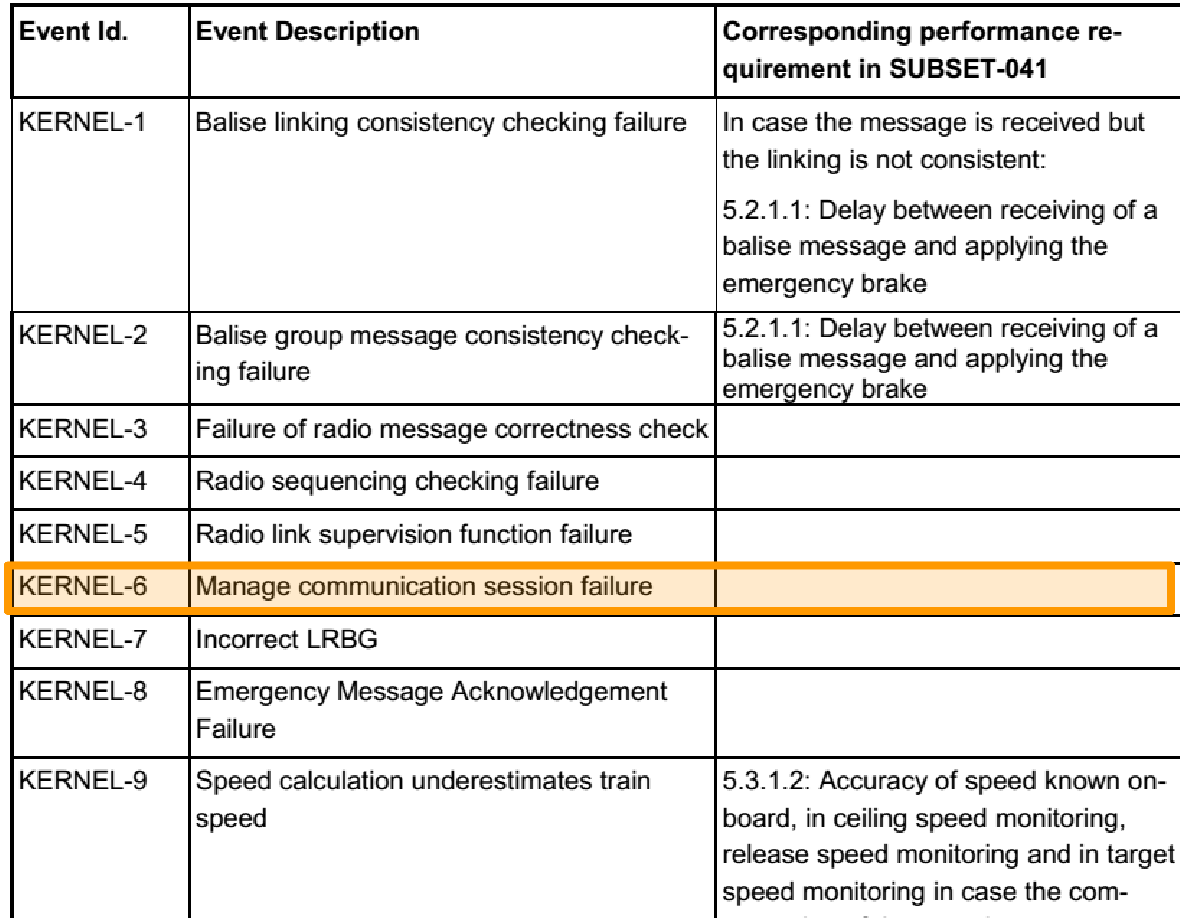
SUBSET 91	*Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 (Baseline 3)*
SUBSET 88	*ETCS Application Levels 1 & 2 - Safety Analysis (Baseline 2)*

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



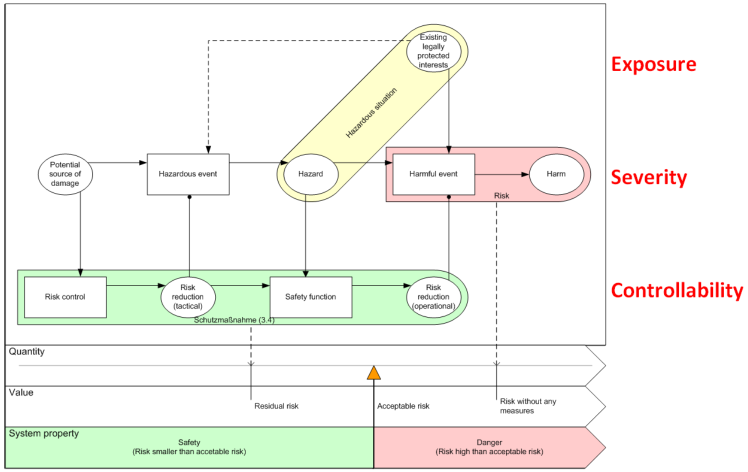
Event Id.	Event Description	Corresponding performance requirement in SUBSET-041
KERNEL-1	Balise linking consistency checking failure	In case the message is received but the linking is not consistent: 5.2.1.1: Delay between receiving of a balise message and applying the emergency brake
KERNEL-2	Balise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

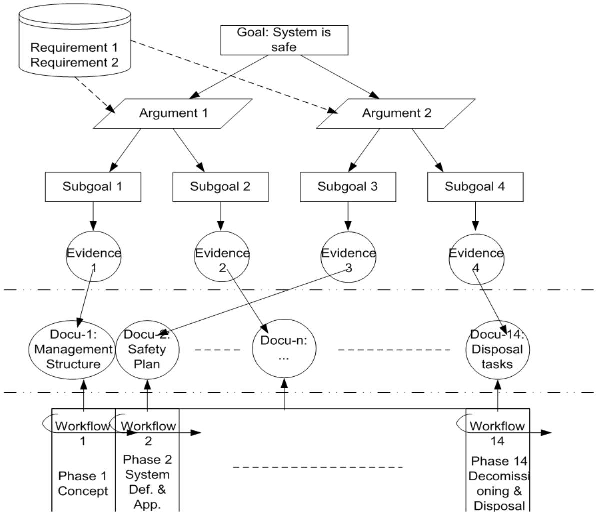
Overall results

- 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