ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

openETCS

WP4 – 1st Workshop on Safety Assessment
OpenETCS Safety Analysis

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

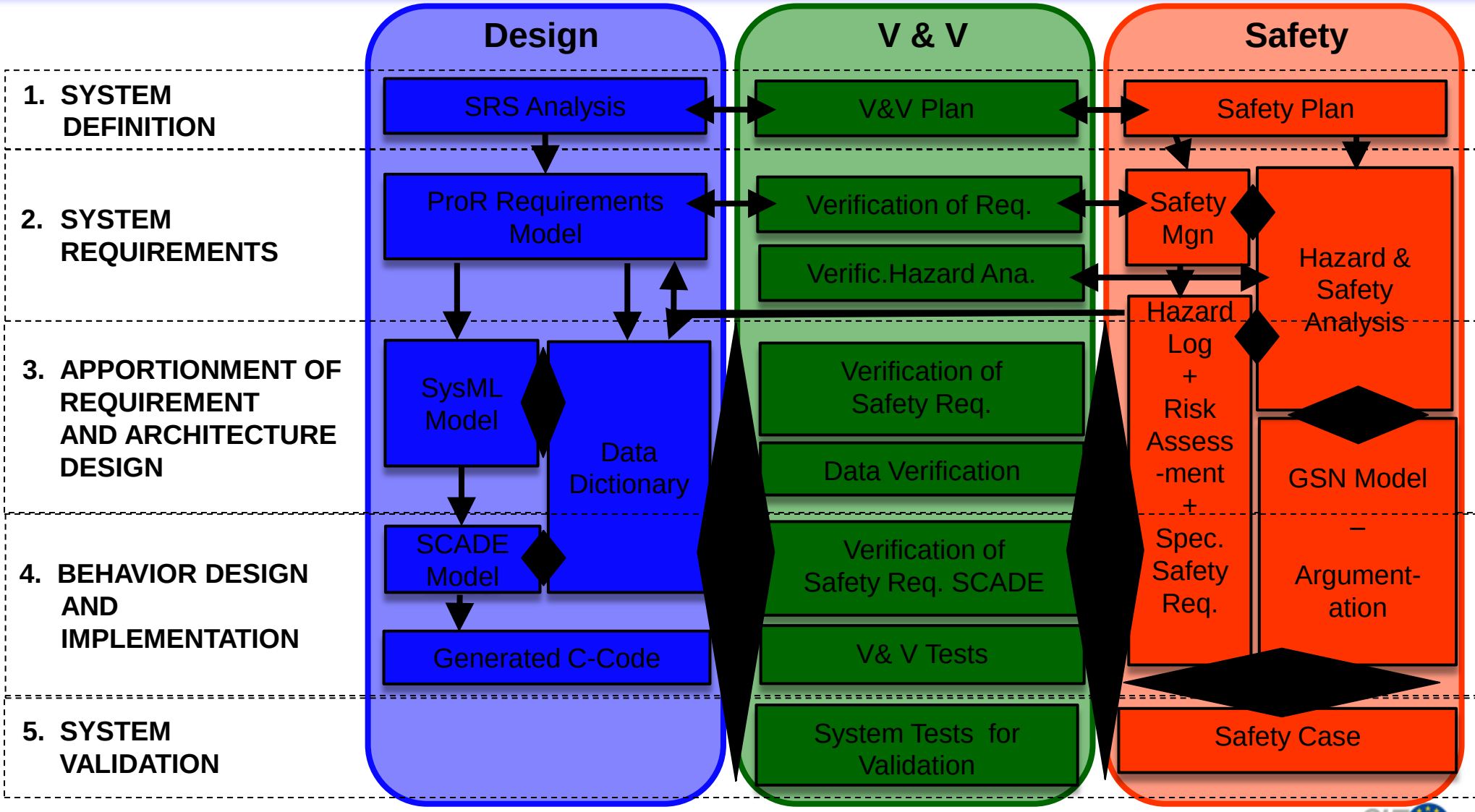
openETCS@ITEA2 Project

Jan Welte, TU-BS

Nürnber, 18.02.2014

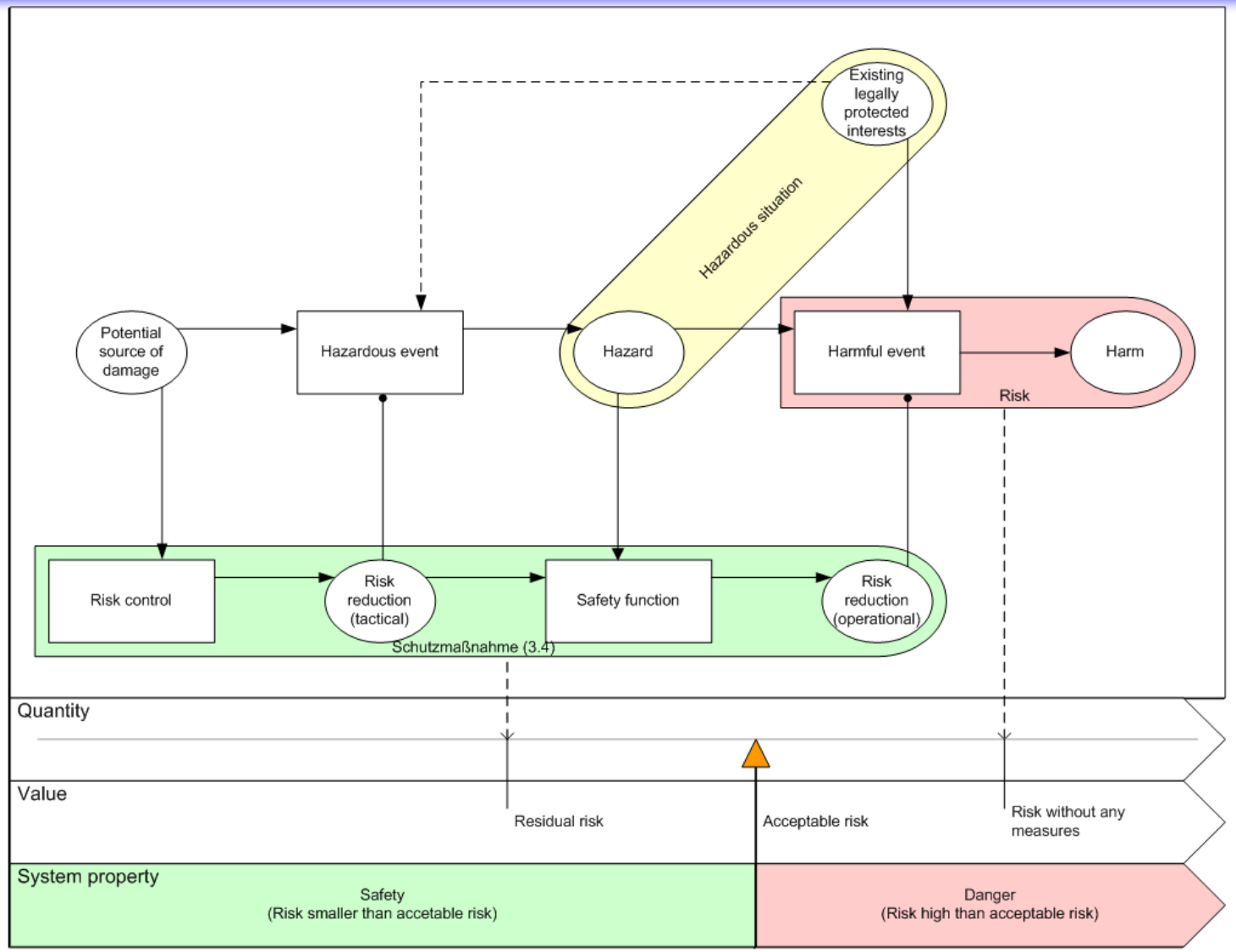
Safety Process Structure

Overview Artifacts



Safety

Risk-Genesis-Model



Exposure

Severity

Controllability

Safety Process

VnV Level 1 Safety activities – Hazard Identification

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 (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

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: 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 onboard, 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.

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