European Economic Interest Group-
European Rail Traffic Management System.
133 Rue Froissart - 1040 Brussels - Belgium.
Phone (02) 673-99-33/fax 673-41-50. TVA 455-935.830

Reference EEIG : 04E084

Distribution date : 12.12.05
Document version : 1.0

Justification Report for the

"Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System".

Version and Modifications

Version No.	Date of distribution	Comments on the modification	Responsible for the modification
1.0 D4	19 Jan 2004	First draft derived from working paper 47/1	KA and RD
1.0 D5	30 Jan 2004	Document updated after working group meeting 21 January.	KA and RD
1.0 D6	13 Feb 2004	Document updated after working group meeting and comments received.	KA and RD
1.0 D7	16 Feb 2004	Hazard identification description updated after working group meeting	FL
1.0 D8	24 Feb 2004	Document updated after working group meeting. Especially chapter 4.2 System Definition and Functions.	KA and AC
1.0 D9	25 Feb 2004	Index 47 text added in the Justification Report. Index47 Text to be extracted for the final document.	KA
1.0 D10	03 Mar 2005	General update of document and examples of quantitative Safety Requirements added.	Working group
1.0 D10.1	22 Mar 2005	Comments from ISA and working group included	Working group
1.0 D11	24 Mar 2005	General update of document	Sub-working Group
1.0 D12	8 April 2005	General update of document and title changed	Working group
1.0 D13	14 April 2005	Document layout changed to A4	KA
1.0 D14	29 June 2005	Comments from the ISA Group implemented	FL, LN and KA
1.0 D15	15 July 2005	Comments from the ISA Group implemented after meeting 6 July	FL, LN and KA
1.0 D16	28 July 2005	References in document updated	KA
1.0	12-12-05	Version for formal distribution	RD

CONTENTS

Justification Report

1 Introduction

1.1.1.1 This document has been produced as an informative document to provide the Rationale and Justification for the requirements in “Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System” {Ref.: 1} (the Index 47 document) necessary for the Control-Command and Signalling Technical Specification for Interoperability for both High Speed {Ref.: 4} and Conventional Rail CCS CR TSI {Ref.: 5}. In the following “CCS TSI” is used and covers for both TSI’s. In the current version of the document the THR’s have not been harmonised, therefore chapter 6 includes examples from different countries. Throughout the document the text has been written as if harmonised THR’s have been achieved

1.1.1.2 The approach taken has been to make full use of existing documents and these are referenced from Index 47 Document {Ref.: 1} and this Justification Report. The present version of the Justification Report includes examples of THR’s from different Railways. It has not been possible in this version to harmonise the THR values.

1.1.1.3 Chapter 2 clarifies the scope of this document and Chapter 3 provides the description of the process used to derive the safety requirements in the Index 47 Document {Ref.: 1} and the justification. Chapter 4 clarifies the detailed System Definition of the Control-Command and Signalling system as defined in the TSI for the purposes of deriving the safety requirements. Chapter 4 also describes the relevant Functions of the Control-Command and Signalling system necessary to carry out a safe train run and to be used for the Hazard Identification.

1.1.1.4 Chapter 5 provides the Hazard identification and the Agreed Control-Command and Signalling Hazard List. This will lead to the safety requirements expressed as a THR corresponding to a SIL for each hazard described in chapter 6.

1.1.1.5 Chapter 7 is the References used in the Justification Report. Chapter 8 is 'Recommendation for next steps' and Chapter 9 is an Open Points list.

2 Scope

2.1 General

2.1.1.1 The scope of this informative document 'Justification Report' is to provide the Rationale and Justification for deriving the Safety Requirements specified in the Index 47 normative document {Ref.: 1}. The Index 47 Document {Ref.: 1} specifies the mandatory safety requirements for CCS TSI that have to be respected in any CCS implementation, to ensure that solutions to achieve safety do not jeopardise interoperability. According to EN 50129 {Ref.: 16} additional analysis work is necessary based on the system design (Causes for Hazards, Apportionment of safety targets). The apportionment of safety targets, concerning ETCS, is done in Index 27 (Subset 91 {Ref.: 6}) for the 'ETCS core hazard' (Exceedance of the safe speed / distance as advised to ETCS).

2.1.1.2 The scope of the Safety Requirements in Index 47 Document {Ref.: 1} is to cover part of phase 3 (EN 50126) {Ref.: 15}. It is not the intention to cover the whole Life Cycle of CCS TSI.

2.1.1.3 By using the Functional Approach for defining the Hazards the functionality of Class B systems will be included in the analyses since the functional approach will cover the functions provided by a Class A or Class B system as defined in the CCS TSI document, however it is not intended to define safety requirements for Class B equipment. The derived safety requirements will only be mandatory for the Class A system.

2.1.1.4 The scope has been aligned to the CCS TSI scope that had been decided through the political processes including Article 21 Committee. The CCS TSI scope can not in itself guarantee the overall safety since the National part is outside the CCS TSI scope.

2.1.1.5 It has also been decided through a political process that ERTMS Level 3 has been excluded from the scope of the Index 47 document {Ref.: 1}.

2.1.1.6 The figure below illustrates CCS TSI safety as part of the CCS overall safety. The Index 47 document {Ref.: 1} specifies the safety of "CCS TSI trackside" (item 1) and "CCS TSI onboard" (item 2) only. It should be noted that the items 3, 4 and 5 are not included. Nevertheless it is obvious that to certify the safety of the overall system the national part has to be considered.

2.1.1.7

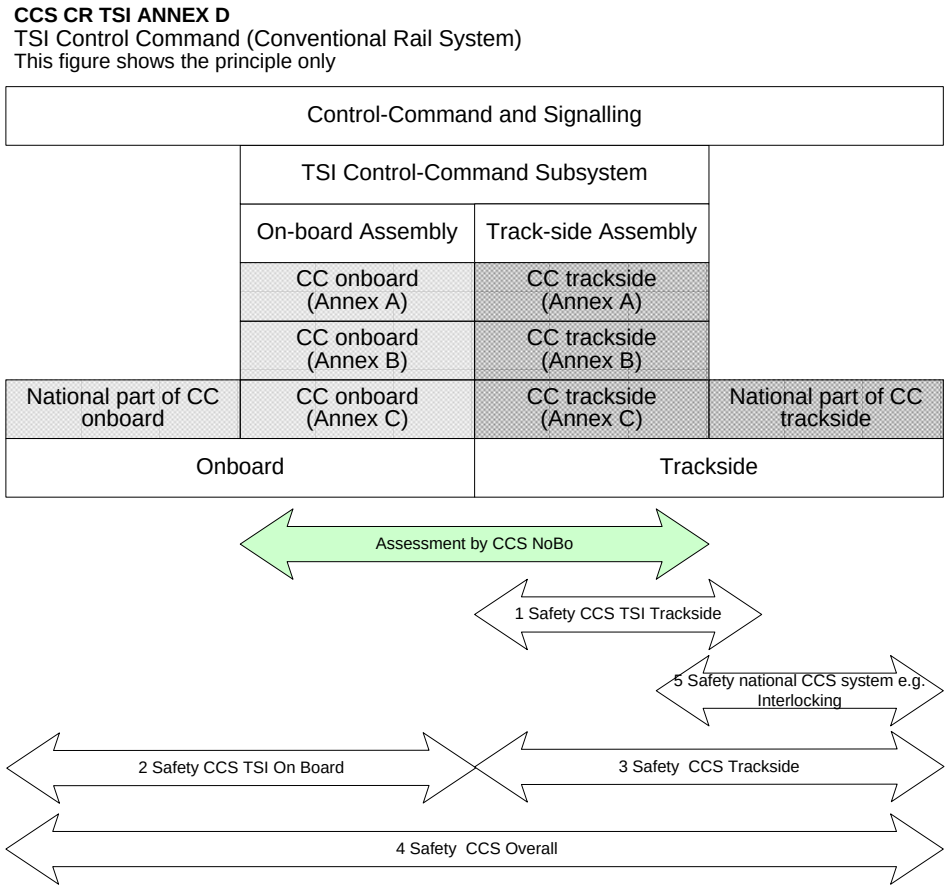


Figure 1 – Scope Diagram

2.1.1.8 The National Safety Assessments 3 and 5 from figure 1 must include the safety assessment of the interface to the CCS TSI Trackside part.

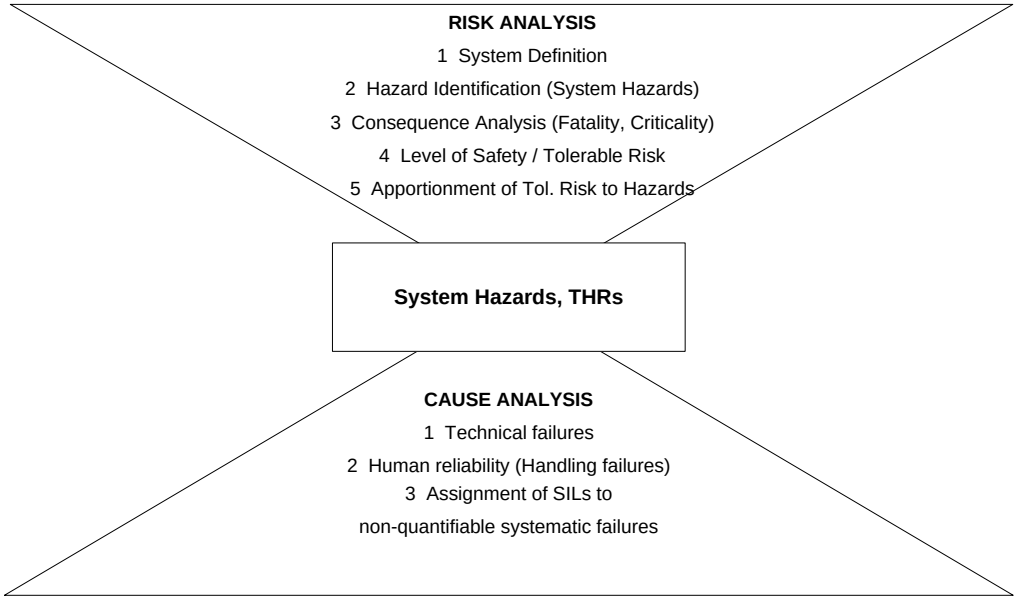
2.1.1.9 The Safety Assessment 1and 5 if carried out separately will require a clear definition of the interface between RBC and Interlocking.

2.1.1.10 The safety requirements will be developed according to EN 50129:2003 {Ref.: 16} Appendix A and derived not further than to tolerable hazard rates (THR) corresponding to a Safety Integrity Level (SIL). (See EN 50129:2003 {Ref.: 16} “Figure A.2 – Global process overview”).

2.2 Safety Concept

2.2.1.1 The applied safety concept - described in the drawing below - is compliant with EN 50126/50129 {Ref.: 15 and 16}. This concept consists of two parts, the Risk Analysis and the Causal Analysis.

2.2.1.2



2.2.1.3 Applying a top-down approach, a **Risk Analysis** serves to derive and introduce safety requirements (THR's / SIL's). This is normally done by the operating company (railways).

2.2.1.4 Via a bottom-up approach, hazard control is done by performing a **Causal Analysis** in order to meet the safety requirements and to ensure that from the system design no new system hazards arise. During a Causal Analysis causes of hazards are evaluated or analysed by a structured hierarchical approach to hazard analysis and hazard tracking (Methods are described in table E.6 of EN 50129 {Ref.: 16}). This is the supplier's responsibility.
While carrying out a Causal Analysis, the 'Fragile Points' {Ref.: 13} have to be considered in order to ensure that all safety relevant causes for hazards of the technical solution have been included.
In order to increase the contingent of quantifiable failures, the Causal Analysis shall consider handling failures (as described in Reason, J.T. Human Error {Ref.: 14}) e.g. train or RBC data entry and operational rules (as far as they describe procedures necessary in terms of handling) quantitatively. Since handling failures are systematic failures, the quantitative consideration is a deviation to EN standards.

2.2.1.5 The remit of Index 47 {Ref.: 11} comprehends step 1 and 2 of the Risk Analysis and the safety requirements. In order to harmonise safety requirements (THR's / SIL's) requirements it is not necessarily essential to carry out steps 3, 4 and 5. A harmonisation of safety requirements may as well take place on THR-level only.

2.2.1.6 While carrying out a Causal Analysis, the 'Fragile Points' {Ref.: 13} have to be considered in order to ensure that all safety relevant causes for hazards have been included.

2.2.1.7 Systematic failures (e.g. in terms of maintenance, creation of static line profile, software failures) are according to EN 50129 {Ref.: 16} not quantifiable. For this reason systematic failures are not considered by the risk budget of a THR, even though systematic failures are covered by the qualitative safety requirements of Index 47 in the System Hazards.

3 Rationale

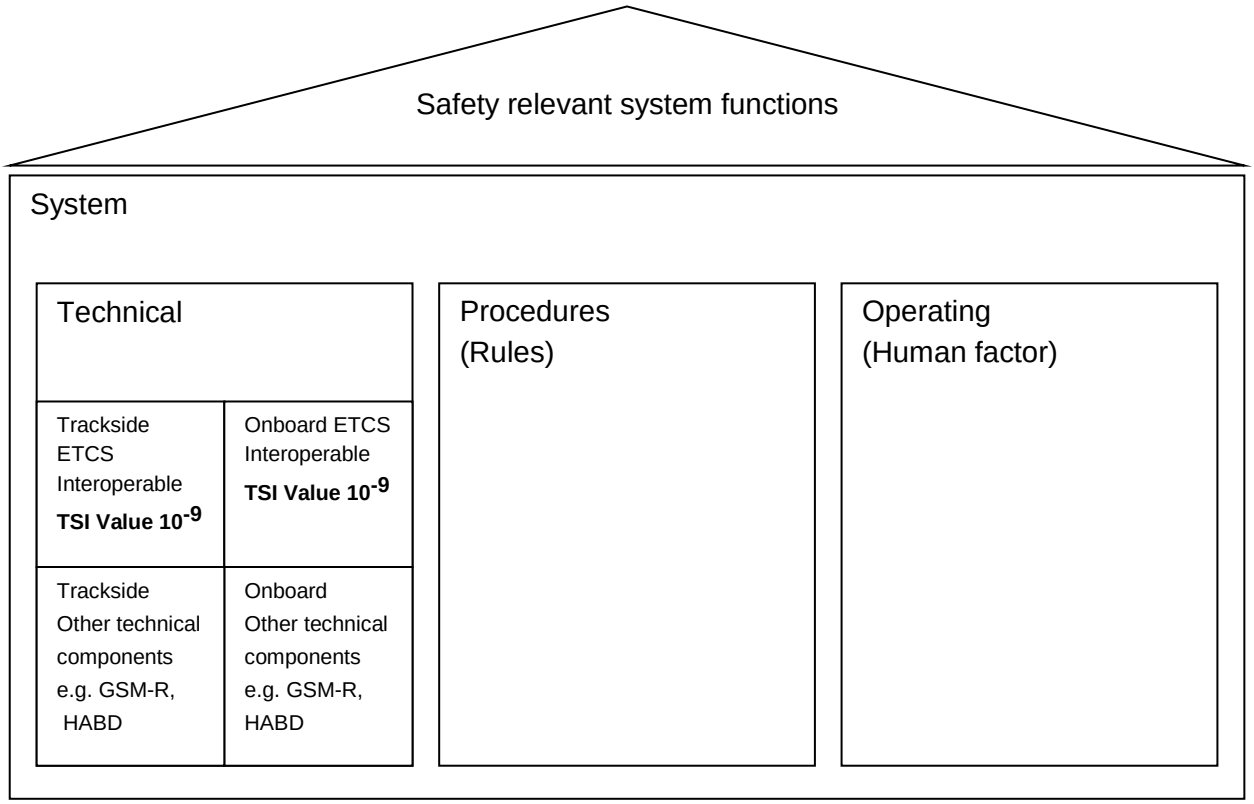
This chapter describes the justification for Index 47 and the detailed process used to identify potential areas of weakness and to derive the safety requirements in the Index 47 document.

3.1 Justification for Index 47.

3.1.1.1 A system is defined as “a group of interrelated, independent, or interacting elements forming a collective entity” [Collins English Dictionary, Millennium Edition]. In the case of the CCS the elements are the technical assemblies, the procedures and the people involved in operating the system.

3.1.1.2 To prove safety of a system it is therefore necessary to use a common approach including technical, procedures and operating aspects. The picture below shows this approach and that in the CCS TSI’s only requirements to technical assemblies (Trackside and Onboard) exist at the moment. CCS TSI contains more than Trackside and Onboard assemblies. Therefore the requirements to technical assemblies as stated in the CCS TSI do not cover the complete CCS TSI scope. Therefore this does not give the possibility to derive safety requirements for CCS using only the requirements in the CCS TSI.

3.1.1.3



3.1.1.4 The CCS TSI’s, CCS CR TSI {Ref.: 5} and CCS HS TSI {Ref.: 4} defines safety in the chapter 3.2.1 and 4.2.1 but this is not sufficient to define the safety requirements in detail to ensure the consideration of random and systematic failures including operating failures (e.g. train data input). Therefore an open point was raised and the

remit for Index 47 {Ref.:11} was approved on 15-09-03 to close the open point.

3.1.1.5 According to EN 50 129 {Ref.: 16} safety is defined by a declaration about risk. EN 50129:2003, defines in 3.1.45 safety as: freedom from unacceptable levels of risk of harm and in 3.1.43 risk is defined as: the combination of the frequency, or probability, and the consequence of a specified hazardous event. A THR - as introduced by CCS CR TSI - is not equivalent to risk. Thus it leads to the perception that the given THR without derivations is not sufficient to make a statement about safety. In addition to this the THR's given in CCS CR TSI lack reference parameters e.g. the system dimensions and reference time for the hazard. As result each nation draws up its individual risk and hazard analysis. The national approaches differ significantly in the majority of cases and in the end this may jeopardises interoperability.

3.1.1.6 The basis for the risk and hazard analyses has to be comparable, especially the system definition and the system boundaries. It is therefore the task of the Index 47 document to develop a common interoperable base which in this case is a system definition and an agreed list of CCS TSI hazards with proposals for THR's.

3.1.1.7 The basis for the development approach follows EN 50 129 {Ref.: 16} Appendix A.

3.1.1.8 In order to fulfil the process in EN 50 129 {Ref.: 16} a Functional approach is used to:

- ensure completeness
- ensure independence from technical solutions

allow safety requirements for single constituents to be derived

3.1.1.9 The Functional approach gives the possibility to map accident statistics to the hazards. Railway statistics for accidents normally reveal a systematic structure (This is the case for Germany: EDS, old STABAG). Accidents could be classified according to different causes which are on a functional level and independent from technical solutions. Since Index 47 uses the functional approach, this gives the possibility to relate Index 47 functions to the accident statistics. This mapping may then be used to derive the TIRF and related THR's based on fatality of accidents.

3.1.1.10 As a starting point all functions that are essential for the safe control of the railway traffic and that are essential for operations, including those required under degraded conditions are taken into account.

3.1.1.11 The functions used for the hazard identification are only the functions that are relevant for CCS TSI. That are functions that:

- are totally or partly carried out by the CCS TSI (issuing the brake command)
- that affects the CCS TSI (e.g. functions that provides information/input which is necessary for CCS TSI e.g. data input).

3.2 Process description

3.2.1.1 The process used in the development of the safety requirements is:

3.2.1.2 Step 1: Detailed System Definition – System Structure

Input: CCS TSI HS and CR

Task: Develop the System Definition from the CCS TSI and derive the architectural

structure according to a model including elements, interfaces and boundaries.

Target: System Architecture drawing, List of input & output interfaces

3.2.1.3 Step 2: Detailed System Definition - Functional Analysis

Input: Function Lists from European railways based on operational knowledge of the CCS system functions necessary to run a train safely.
Functional Analysis Of Trans – European Rail Operation {Ref.: 8}.

Task: Identify functions that are essential for the safe control of the railway traffic and that are essential for operations, including those required under degraded conditions.
Identify functions relevant for CCS TSI, that is functions that:

- are totally or partly carried out by the CCS TSI (issuing the brake command)
- that affects the CCS TSI (e.g. functions that provides information/input which is necessary for CCS TSI e.g. data input).

Identify list of failure modes.

Target: List of functions to be used for the Hazard Identification and list of failure modes.

3.2.1.4 Step 3: Hazard Identification

Input: List of functions (from Step 2).
List of failure modes.
Definition of a Hazard from EN50129 {Ref.: 16}.
System Architecture Drawing.

Task: Apply appropriate failure modes to the functions to identify the hazards according to the Hazard Definition.
Fill a table for each hazard including:

- function
- function description
- naming hazard
- limitations
- simplified consequence analysis
- examples for causes for the hazards
- output interface

Target: Log of Hazards.

3.2.1.5 Step 4: Identification of System Hazards

Input: Log of hazards (from Step 3)
System architecture (from Step 1)

Task: Allocate each hazard to the system architecture.
Hazards which can be allocated at the output interfaces of CCS TSI are System Hazards. Other hazards are causes for CCS TSI hazards or consequences of them.

Target: Division of Log of hazards into:

- CCS TSI System Hazard Log
- Log of Hazards on the interface to CCS TSI and causes found within the CCS TSI System.

3.2.1.6 Step 5: Systematic check of the in/output to the CCS TSI system for consistency check.

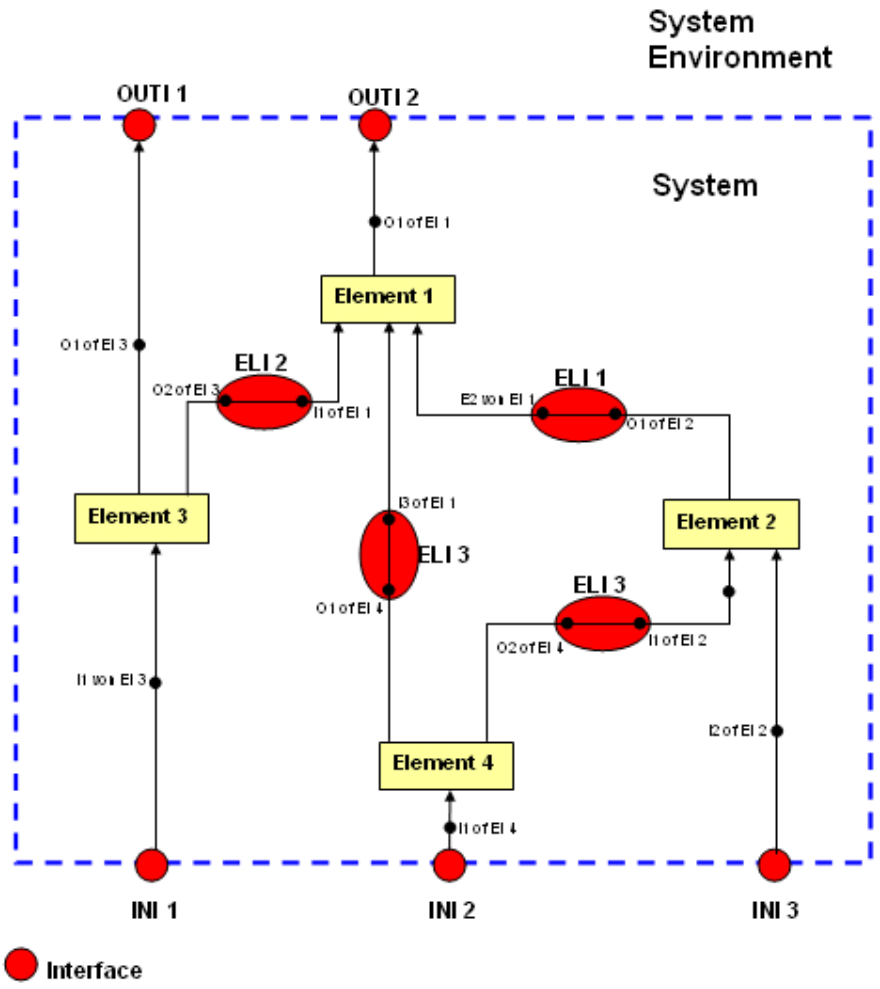
Input: Interfaces in/output to the CCS TSI system (from Step 1)

Task: Consistency check for identifying System Hazards.
Target: Complete CCS TSI Hazard Log.

3.2.1.7 Step 6: Introduction of safety requirements to CCS TSI System hazards

Input: CCS TSI System Hazard Log (from Step 4)
Task: Apply THR corresponding to a SIL to each System Hazard
Target: Safety Requirements for CCS TSI (THR corresponding to a SIL)

3.2.1.8 General 'model of system structure' used for the hazard identification process



OUTI Output interface (system >>> system environment)
INI Input interface (system environment >>> system)
ELI Element interface (element >>> element)
Ix Input no. x
Ox Output no. x
Elx Element no. x

3.3 Completeness of hazard identification

In order to ensure completeness of the system hazards identified, different approaches and methods are merged. The resulting synergetic effect ensures completeness at Risk Analysis level without the consideration of the technical solution (e.g. detailed ETCS specific functions).

3.3.1.1 Functional approach to hazard identification on operational level

3.3.1.2 Analysis of a generic train mission including consideration of preparatory conditions

3.3.1.3 Causal Analysis drawing links within the defined system and analysing all causes for system hazards

4 System Definition

4.1 Introduction

4.1.1.1 This chapter describes the system definition from CCS CR TSI according to “step 1” (from the process description in chapter 3.2) and elaborates a functional system definition according to “step 2”.

4.2 Detailed System Definition - System Structure

4.2.1 General

4.2.1.1 As an initial step in the preparation of Index 47, this document analyses the scope of the Control Command and Signalling subsystem as defined in the Technical Specifications for Interoperability (TSI) covering both conventional and high-speed applications.

4.2.1.2 The documents consulted in the process were as follows

- The Conventional Rail Directive – {Ref.: 3}
- The Conventional Rail CCS TSI – {Ref.: 5}
- The High-speed Rail Directive – {Ref.: 2}
- The High-speed Rail CCS TSI– {Ref.: 4}
- New Annex A for CCS TSI - {Ref.: 17}

4.2.1.3 The purpose of this analysis is to provide a definition of the system structure of the Control Command and Signalling TSI subsystem in the context of safety analysis. The task is to derive an architectural structure according to the model including elements, interfaces and boundaries.

4.2.1.4 In this chapter the system will be described in terms of its “hardware structure” only to define the elements and internal interfaces as well as the interfaces to the external environment (other TSI as well as non TSI environment) which need not be considered. Thus the borders of the system will become clear and the level of detail will be set.

4.2.1.5 These elements are supported by mandated operational processes such as

- Operational rules from the EEIG ERTMS User Group in the TSI Operation.

4.2.2 CCS TSI System Description

4.2.2.1 This chapter is an extract of the relevant chapters of CCS CR TSI {Ref.: 5}. The extract from the CCS TSI will be used to establish the Index 47 System definition and interfaces.
Exact reference to that document is provided within the headlines of the following subchapters.

4.2.2.2 The Control-Command subsystem is characterised by the following Basic

Parameters (Reference: CCS CR TSI {Ref.: 5}. chapter 4.1):

- Control-Command safety characteristics relevant to interoperability
- On-board ETCS functionality
- Track-side ETCS functionality
- EIRENE functions
- ETCS and EIRENE air gap interfaces
- On-Board Interfaces Internal to Control Command
- Trackside Interfaces Internal to Control Command
- Key Management
- ETCS-ID Management
- HABD (hot axle box detector)
- Compatibility with track-side Train Detection Systems
- Electromagnetic Compatibility
- ETCS DMI (driver machine interface)
- EIRENE DMI (driver machine interface)
- Interface to data recording for regulatory purposes
- Visibility of track-side Control-Command objects

4.2.2.3 Functional and technical specifications of the Subsystem (Reference: CCS CR TSI {Ref.: 5} chapter 4.2):

Control-Command safety characteristics relevant to interoperability
On-board ETCS functionality
Track-side ETCS functionality
EIRENE functions
ETCS and EIRENE air gap interfaces
On-Board Interfaces Internal to Control-Command
Interface between ETCS and STM
GSM-R/ETCS
Odometry
Trackside Interfaces Internal to Control-Command
Functional interface between RBC's
Technical interface between RBC's
GSM-R/RBC
Eurobalise/LEU
Euroloop/LEU
Requirements on pre-fitting of ERTMS track side equipment
Key Management
ETCS-ID Management
Hot axle box detector
Compatibility with Track-side Train Detection Systems
Electromagnetic Compatibility
Internal Control-Command Electromagnetic compatibility
Electromagnetic Compatibility Between Rolling Stock and Control-Command track-side Equipment

ETCS DMI (Driver Machine Interface)
EIRENE DMI (Driver Machine Interface)
Interface to Data Recording for Regulatory Purposes
Visibility of track-side Control-Command objects

4.2.2.4 Functional and technical specifications of the interfaces to other Subsystems**:**
(Reference: CCS CR TSI {Ref.: 5} chapter 4.3):

Interface to the Subsystem Traffic Operation and Management
Operating Rules
ETCS Driver Machine Interface
EIRENE Driver Machine Interface
Interface to data recording for regulatory purposes
Guaranteed train braking performance and characteristics
Isolation of ETCS on-board equipment
Key Management
Hot Axle Box Detectors
Driver Vigilance
Use of Sanding
Driver's External Field of View
Interface to the Subsystem Rolling Stock
Compatibility with track-side Train Detection Systems
Electromagnetic Compatibility Between Rolling Stock and CCS Track-side Equipment
Guaranteed train braking performance and characteristics
Position of Control-Command On-board Antennae
Physical environmental conditions
Electromagnetic Compatibility
Isolation of On-Board ETCS functionality
Data Interfaces
Hot Axle Box Detectors
Vehicle Headlights
Driver Vigilance
Odometry
Interface to data recording for regulatory purposes
Onboard pre-fitting
Interfaces to Subsystem Infrastructure
Train Detection Systems.
Track-side Antennae
Physical environmental conditions
Electromagnetic Compatibility
Interfaces to Subsystem Energy
Electromagnetic Compatibility

4.2.2.5 Operating rules
(Reference: CCS CR TSI {Ref.: 5} chapter 4.4)

4.2.2.6 Maintenance rules
(Reference: CCS CR TSI {Ref.: 5} chapter 4.5):
Responsibility of manufacturer of equipment
Responsibility of contracting entities

Responsibility of infrastructure manager or railway undertaking
Maintenance plan

4.2.2.7 Professional qualifications.
(Reference: CCS CR TSI {Ref.: 5} chapter 4.6)

4.2.2.8 Health and safety conditions.
(Reference: CCS CR TSI {Ref.: 5} chapter 4.7)

4.2.2.9 Infrastructure and Rolling stock registers.
(Reference: CCS CR TSI {Ref.: 5} chapter 4.8):

4.2.2.10 List of interoperability constituents in the Control-Command Assembly, its characteristics and interfaces

(Reference: CCS CR TSI {Ref.: 5} table 5.1a and 5.2a):

Interfaces considered in addition to TSI CCS (missing or unclear description in TSI CCS), necessary for a system definition in terms of safety analysis, are marked in italic text. (Those are announced to AEIF).
ON-BOARD

- ERTMS ETCS On-Board
  - Safety
  - On-board ETCS functionality
  - ETCS and EIRENE air gap interfaces:
    - RBC (level 2 and 3)
    - Radio in-fill unit (optional level 1)
    - Eurobalise airgap
    - Euroloop airgap (optional level 1)
  - Interfaces:
    - STM (implementation of interface K optional)
    - ERTMS GSM-R on-board
    - Odometry
    - Key management centre
    - ETCS ID Management
    - ETCS DMI
    - Key Management
    - Physical environmental conditions
    - EMC
    - Data interface (includes vigilance and train integrity)
    - Safety information recorder
    - Train (RS) external to CCS *Driver external to CCS (not mentioned in TSI)*
    - *Static Train Data (not mentioned in TSI)*
    - Maintenance ERTMS
- Safety Platform on-board
  - Safety
  - Interfaces:
    - None
- Safety Information Recorder:
  - On-Board ETCS functionality

Interfaces:
JRU downloading tool
ERTMS/ETCS on-board
Environmental conditions
EMC

- Odometry:
  Safety
  Onboard ETCS funtionality (only Odometry)
  Interfaces:
  ERTMS ETCS on-board
  Environmental conditions
  EMC
  Track external to CCS (not mentioned in TSI)
- External STM:
  Functions and safety (according to national specifications)
  Interfaces:
  ERTMS ETCS on-board
  Class B system air gap (according to national specifications)
  Environmental conditions (according to national specifications)
  EMC (according to national specifications)
- ERTMS/GSM-R on-board:
  EIRENE functions
  Interfaces:
  ERTMS ETCS on-board
  GSM-R
  EIRENE DMI
  Environmental conditions
  EMC

TRACK-SIDE

- RBC
  Safety
  Track-side ETCS funtionality
  ETCS and EIRENE air gap interfaces
  Interfaces:
  Neighbouring RBC
  ERTMS GSM-R track-side
  Key management centre
  ETCS-ID Management
  Interlocking
  Environmental conditions
  EMC
- Radio in-fill unit
  Safety
  Track-side ETCS functionality

ETCS and EIRENE air gap interfaces
Interfaces:
ERTMS GSM-R track-side
Key management system
ETCS-ID Management
Interlocking and LEU
Environmental conditions
EMC

- Eurobalise
  Safety
  ETCS and EIRENE air gap interfaces
  Interfaces:
  LEU Eurobalise
  ETCS-ID Management
  Environmental conditions
  EMC
- Euroloop
  Safety
  ETCS and EIRENE air gap interfaces
  Interfaces:
  LEU Euroloop
  ETCS-ID Management
  Environmental conditions
  EMC
- LEU Eurobalise
  Safety
  Track-side ETCS functionality
  Interfaces:
  Track-side signalling
  Eurobalise
  ETCS-ID Management
  Environmental conditions
  EMC
- LEU Euroloop
  Safety
  Track-side ETCS functionality
  Interfaces:
  Track-side signalling
  Euroloop
  ETCS-ID Management
  Environmental conditions
  EMC
- Safety Platform track-side
  Safety
  Interfaces: None
  CMI (RBC Operator) (not mentioned in TSI)
  Static Trackside Data (not mentioned in TSI)

Train detection
Train detection interfaces: (external to CCS?)

4.2.2.11 Example of Groups of Interoperability constituent in the CCS Assembly

(Reference: CCS CR TSI {Ref.: 5} table 5.1b and 5.2b):

ON-BOARD

- Safety Platform on-board,
  ERTMS ETCS on-board,
  Safety Information Recorder,
  Odometry.
  Safety
  On-Board ETCS functionality
  ETCS and EIRENE air gap interfaces
  RBC
  Radio in-fill unit
  Eurobalise airgap
  Euroloop airgap
  Interfaces
  STM (implementation of interface K optional)
  ERTMS GSM-R on-board
  Key management system
  ETCS ID Management
  ETCS DMI
  Physical environmental conditions
  EMC
  JRU downloading tool
  Data interface. This also includes vigilance (optional) and train integrity (only ERTMS / ETCS level 3)

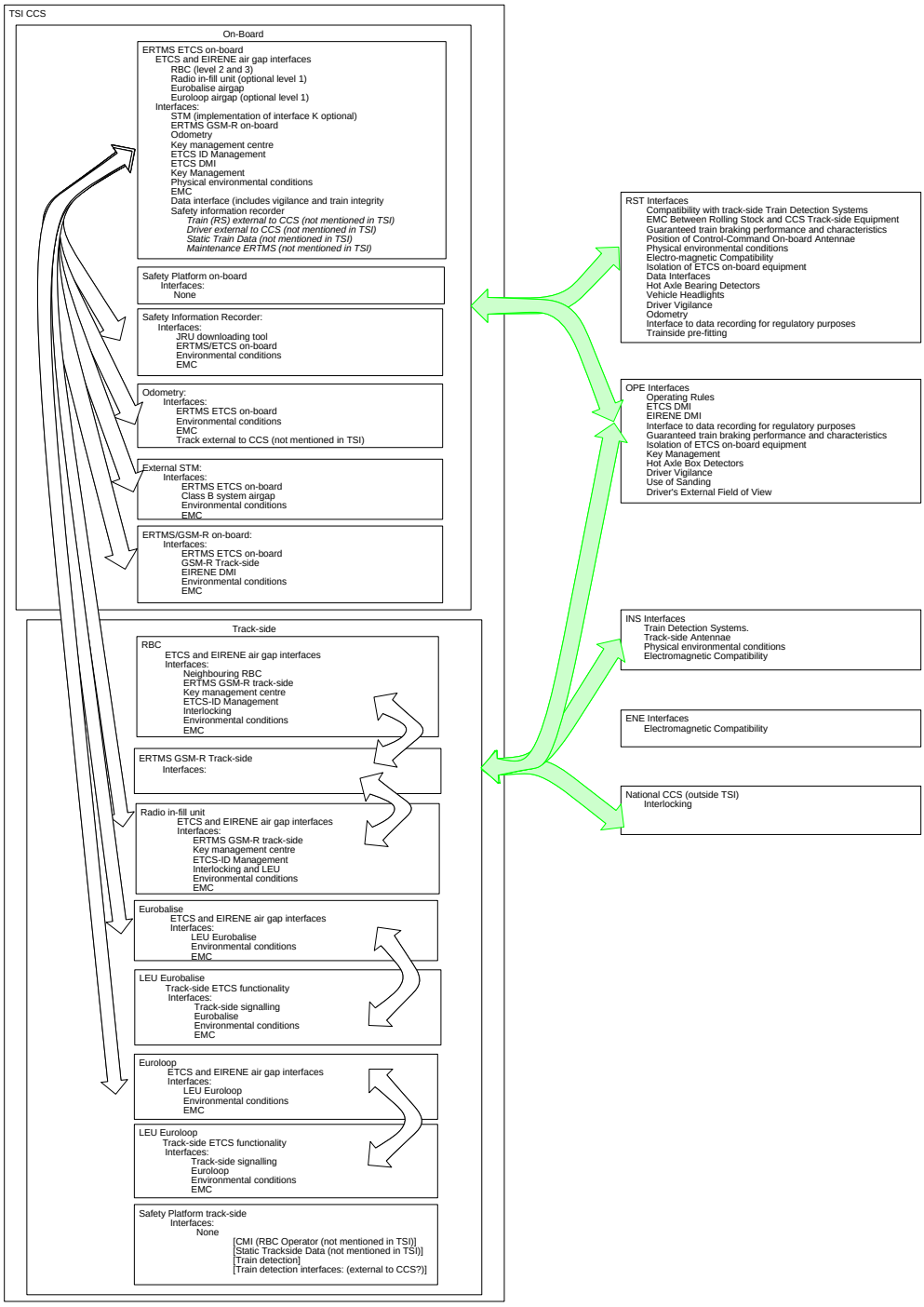
TRACK-SIDE

- Safety Platform track-side
  Eurobalise
  LEU Eurobalise
  Safety
  Track-side ETCS functionality
  ETCS and EIRENE air gap interfaces
  Interfaces
  Track-side signalling
  ETCS-ID Management
  Environmental conditions
  EMC
- Safety Platform track-side
  Euroloop
  LEU Euroloop
  Safety

Track-side ETCS functionality
ETCS and EIRENE air gap interfaces
Interfaces
Track-side signalling
ETCS-ID Management
Environmental conditions
EMC

4.2.3 System Structure Illustration

4.2.3.1 The following illustration is based on the 'Interoperability constituents' listed above (CCS CR TSI {Ref.: 5}. tables 5.1a & 5.2a), on the 'Functional and technical specifications of the interfaces to other Subsystems' (CCS CR TSI, chapter 4.3) and designed according to the 'Model of system structure' (see 3.2.1.8).

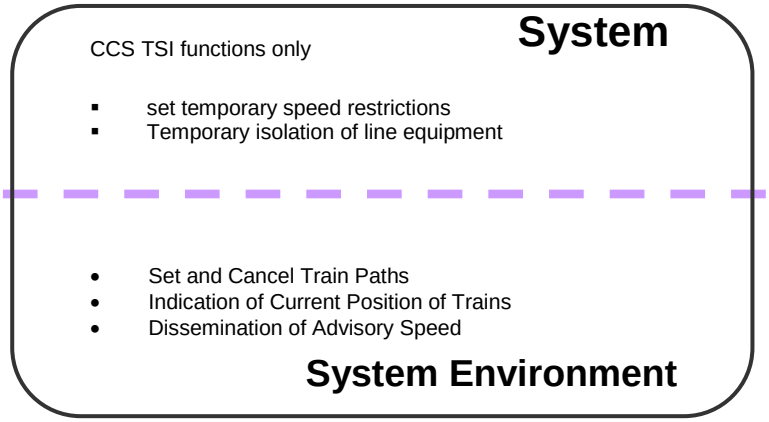


System Architecture - Detailed Drawing
Version: 01.03.2004

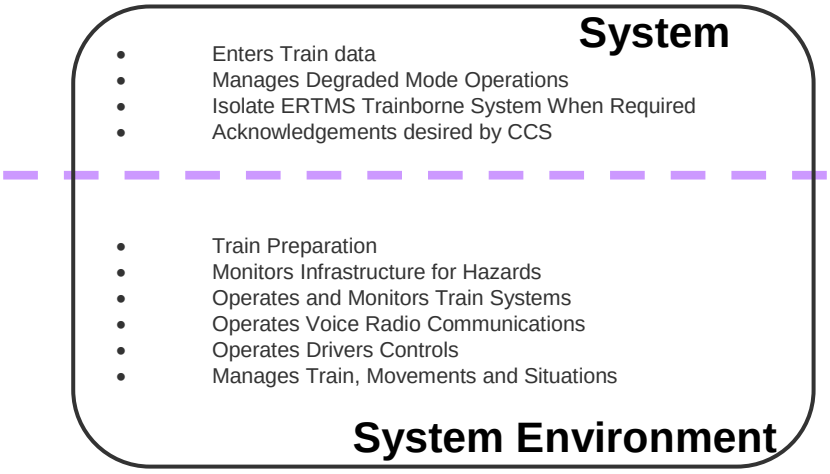
4.2.4 Interfaces

4.2.4.1 The allocation of functions of the Driver and Signalman in the system structure is based on the functionality fulfilled, which can be inside or outside the defined system. This can be obtained from the following drawings.

4.2.4.2 Signalman



4.2.4.3 The Driver has two functions: 1) ERTMS operator and 2) train driver. Even though there is only one driver, he comprises two types of functionalities. The interface is between the two functionalities: Concerning the "model of the system structure" in chapter 4, all functions the driver does in his function as operator of the train are allocated outside the defined system. Concerning functions the driver does in terms of ERTMS DMI, he is acting as operator of ERTMS (communicating, interacting with and monitoring ERTMS onboard device) and therefore these functions are allocated within the defined system.



4.2.4.4 Interoperability constituents' internal interfaces - List

The interfaces derived from the system architecture are listed in the table below. {CCS CR TSI {Ref.: 5}. table 5.1A and 5.2A}

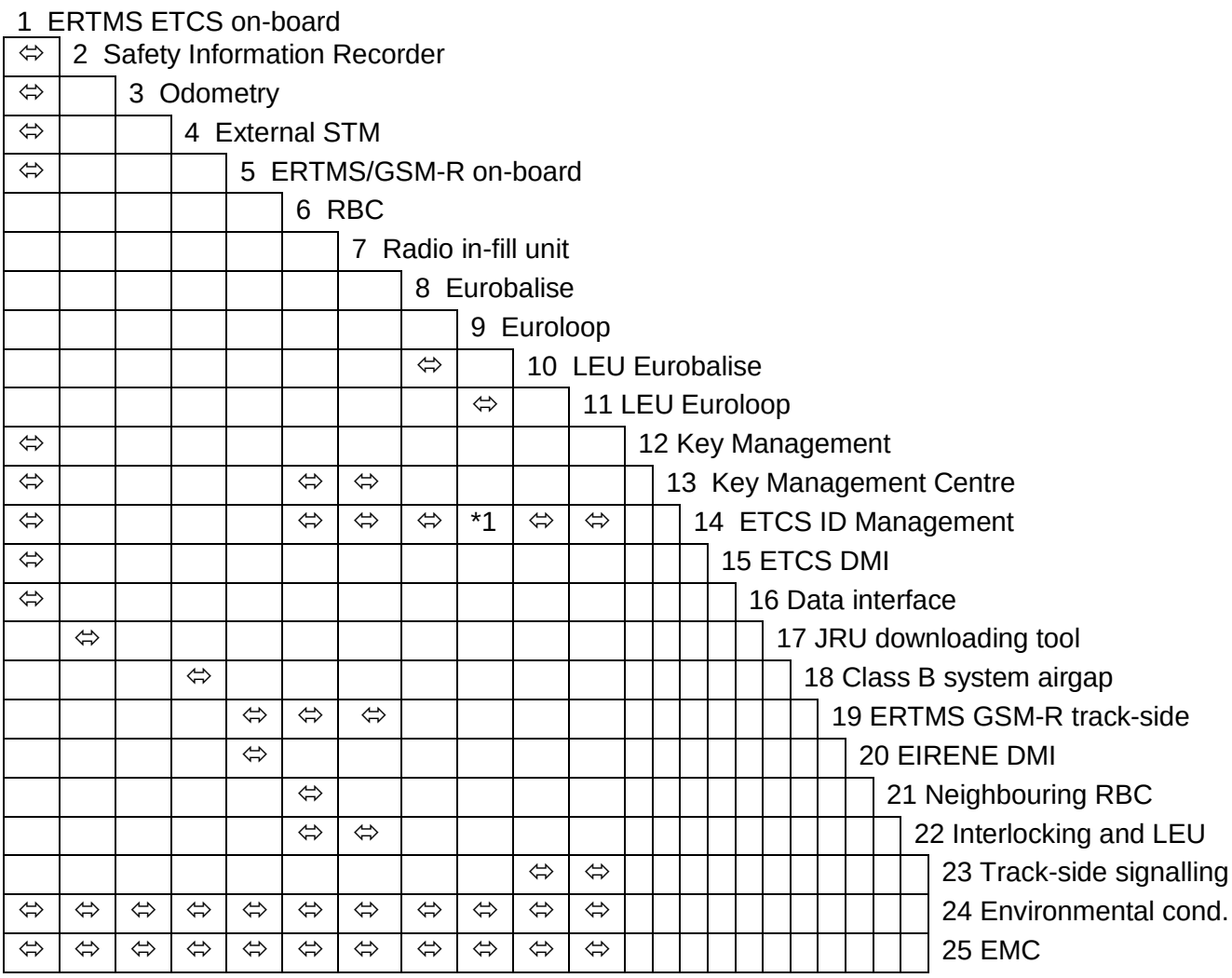
Interface #	Interface between	and:
1	ERTMS ETCS	STM (implementation of

	on-board	interface K optional)
2	ERTMS ETCS on-board	ERTMS GSM-R on-board
3	ERTMS ETCS on-board	Odometry
4	ERTMS ETCS on-board	Key management centre
5	ERTMS ETCS on-board	ETCS ID Management
6	ERTMS ETCS on-board	ETCS DMI
7	ERTMS ETCS on-board	Key Management
8	ERTMS ETCS on-board	Data interface (includes vigilance and train integrity
9	ERTMS ETCS on-board	Safety information recorder
10	Safety Information Recorder	JRU downloading tool
11	Safety Information Recorder	ERTMS/ETCS on-board
12	Odometry	ERTMS ETCS on-board
13	External STM	ERTMS ETCS on-board
14	External STM	Class B system airgap
15	ERTMS/GSM-R on-board	ERTMS ETCS on-board
16	ERTMS/GSM-R on-board	GSM-R (track-side)
17	ERTMS/GSM-R on-board	EIRENE DMI
18	RBC	Neighbouring RBC
19	RBC	ERTMS GSM-R track-side
20	RBC	Key management centre
21	RBC	ETCS-ID Management
22	RBC	Interlocking
23	Radio in-fill unit	ERTMS GSM-R track-side
24	Radio in-fill unit	Key management centre
25	Radio in-fill unit	ETCS-ID Management
26	Radio in-fill unit	Interlocking and LEU
27	Eurobalise	LEU Eurobalise
28	Euroloop	LEU Euroloop
29	LEU Eurobalise	Track-side signalling
30	LEU Eurobalise	Eurobalise
31	LEU Euroloop	Track-side signalling
32	LEU Euroloop	Euroloop
33	ERTMS ETCS on-board	Physical environmental conditions
34	ERTMS ETCS on-board	EMC
35	Safety Platform on-board	None
36	Safety Information	Environmental conditions

	Recorder	
37	Safety Information Recorder	EMC
38	Odometry	Environmental conditions
39	Odometry	EMC
50	External STM	Environmental conditions
41	External STM	EMC
42	ERTMS/GSM-R on-board	Environmental conditions
42a	ERTMS/GSM-R on-board	EMC
43	RBC	Environmental conditions
44	RBC	EMC
45	Radio in-fill unit	Environmental conditions
46	Radio in-fill unit	EMC
47	Eurobalise	Environmental conditions
48	Eurobalise	EMC
49	Euroloop	Environmental conditions
50	Euroloop	EMC
51	LEU Eurobalise	Environmental conditions
52	LEU Eurobalise	EMC
53	LEU Euroloop	Environmental conditions
54	LEU Euroloop	EMC
55	Safety Platform track-side	None
56	LEU Eurobalise	ETCS-ID Management
57	LEU Euroloop	ETCS-ID Management

4.2.4.5 Interoperability constituents' internal interfaces - Matrix

The interface matrix below is based on the CCS CR TSI {Ref.: 5}. table 5.1A and 5.2A



*1 Interface is in the CCS TSI and therefore in the list in 4.2.2.10 but the interface is via the LEU Euroloop. There are no Euroloop without LEU Euroloop.

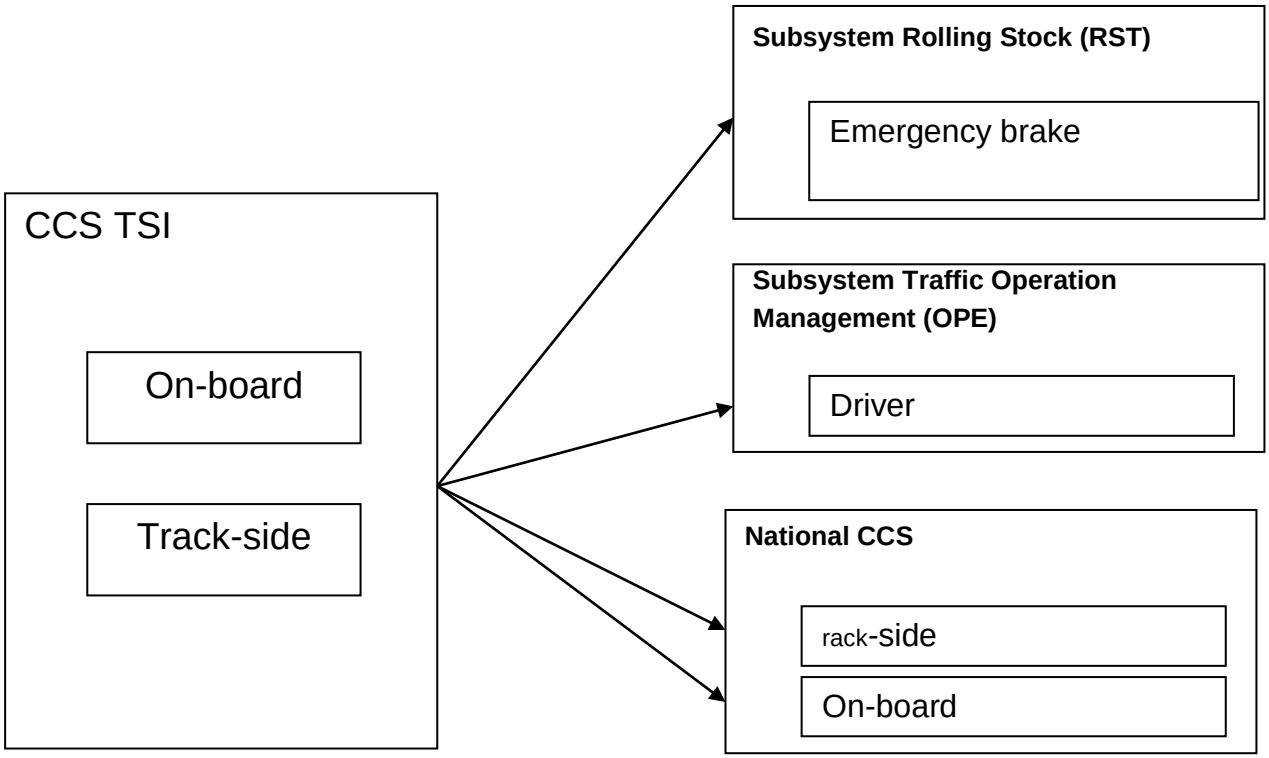
4.2.4.6 Input Interfaces

The following table lists the input interfaces of the defined system:

	From	To	Description
1	OPE: Maintenance / train coordination & disposition	CCS TSI track-side: RBC operator	data for temporary areas where ETCS is not allowed to be used (Temporary isolation of line equipment)
2	OPE: planning team for temporary speed restrictions, maintenance	CCS TSI track-side and/or RBC operator	data for temporary speed restrictions
3	OPE: creator of line profile	CCS TSI track-side	static line data
4	National CCS: Interlocking	CCS TSI track-side	information about locked track elements of section required for the movement, speed restrictions commanded by signals, operational aspects commanded by signals, ...
5	OPE: railway and producer of train	CCS TSI on-board	static train data
6	RST train: Brake	CCS TSI on-board	status of brake (applied / not applied)
7	Infrastructure INS: Track	CCS TSI on-board	Odometry (radar)
8	OPE: ERTMS DMI(driver)	CCS TSI: driver	driver has two functions: 1) ERTMS operator 2) train driver Even though there is only one driver, he comprises two types of functionalities. The interface is between the two functionalities: Concerning the "model of the system structure" in chapter 4, all functions the driver does in his function as operator of the train are allocated <u>outside</u> the defined system. Concerning functions the driver does in terms of ERTMS DMI, he is acting as operator of ERTMS (communicating, interacting with and monitoring ERTMS onboard device) and therefore these functions are allocated <u>within</u> the defined system.
9	RST	CCS TSI on-board	information about driving direction, information which drivers' cab is

			activated
10	RST	CCS TSI on-board	Odometry (tachometer)
11	National CCS: On-Board	CCS TSI On-Board	National CCS status: active, passive

4.2.4.7 The following illustration is based on the 'System Structure Illustration' and elaborated with focus on the output interfaces (Interfaces from CCS, as described in the CCS TSI, to other subsystems).



4.2.4.8 Output Interface List

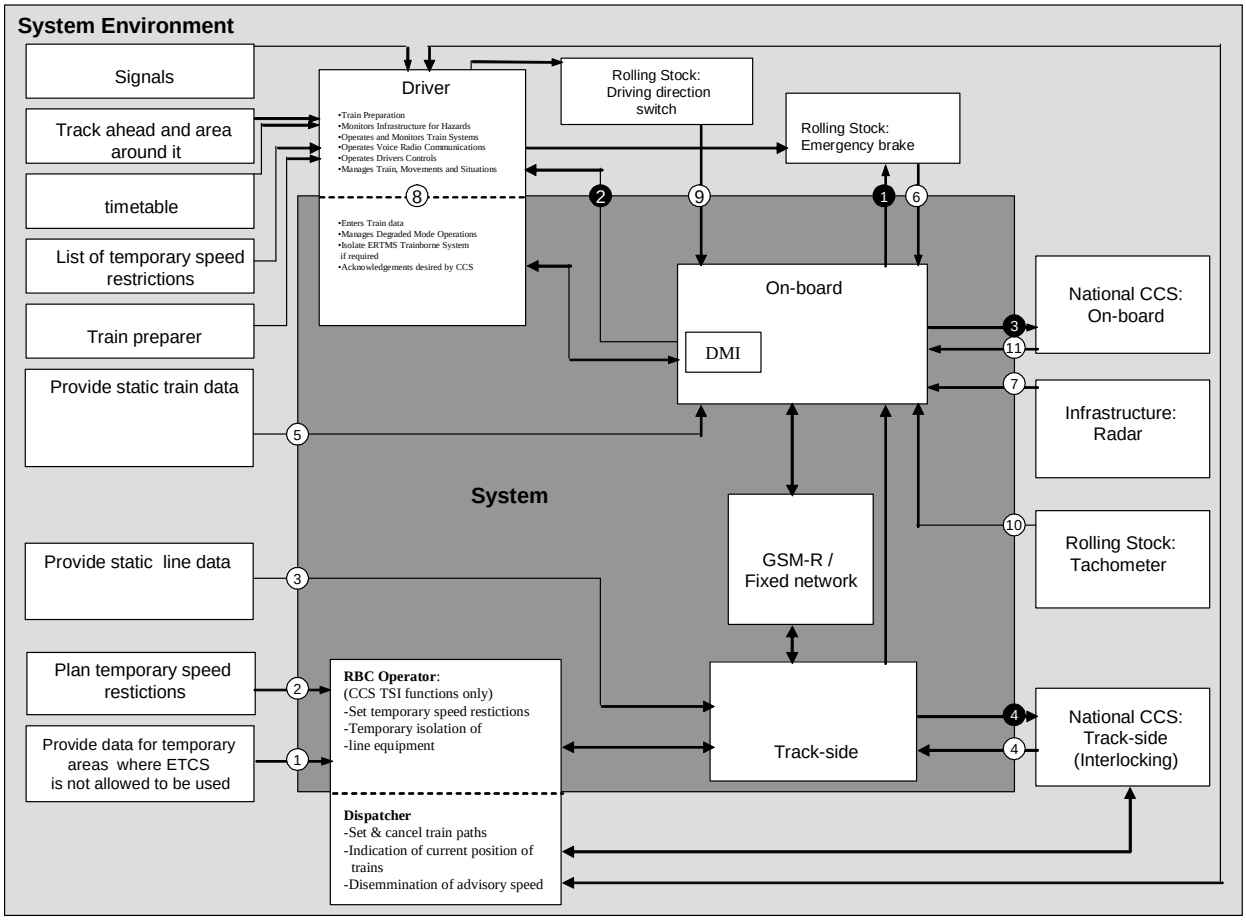
The following table lists the output interfaces of the defined system and exemplarily describes the information transmitted.

Interface #	Interface between	Direction	and:	Description	UNISIG reference {Ref.: 7}
1	CCS TSI: On-Board	→	Rolling Stock: Emergency brake	- braking command	- SUBSET 031 (2.0.0), page 8, figure 1: *'train order'*
2	CCS TSI: On-Board	→	OPE: Driver	e.g.: - 'ETCS ready-to-operate' indication - ETCS mode indication - ETCS level indication - actual speed indication - supervised maximum speed indication	SUBSET 031 (2.0.0), page 8, figure 1: *'MMI indication'*

				- distance to brake target indication - predicted speed at brake target indication - Auxiliary Driving Information (e.g. approaching a tunnel or lowering the pantograph) - text messages - acknowledgement request - emergency stop (via GSM-R voice)	
3	CCS TSI: On-board	→	National CCS: On-board	- activation command for national CCS	- SUBSET 091 (2.2.2), chapter 2, 2.5.3: *'STM'*
4	CCS TSI: Track-side	→	National CCS: Trackside	- synchronisation request - emergency stop notification -	- SUBSET 032 (2.0.0), page 7, figure 1: *'RBC information'*

4.2.5 System boundary

Concluding chapter 4.2 this picture puts the result into context.



x Output Interface No. x

Y Input Interface No. Y

(Note: All connecting lines are intended to be of the same line width)

4.2.5.1 Note 1

The System as described in 4.2.5 is dependant on other systems: Other systems may influence the defined system via the input interfaces. In the context of Index 47, other systems influencing the defined system are considered as being ideal (functioning without errors). Nevertheless, if the scope of safety assessment is expanded to the overall safety of railways, the influence of the other systems have to be considered.

4.2.5.2 Note 2

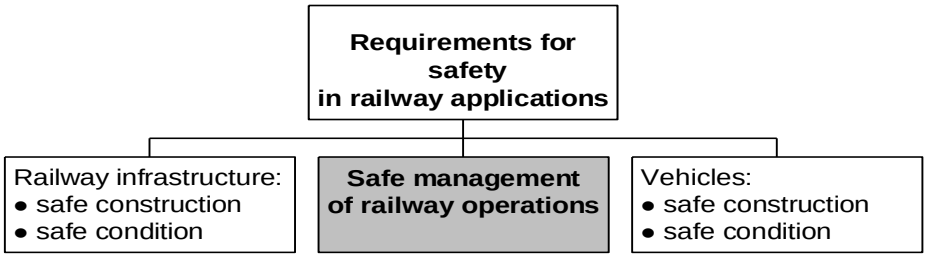
The analysis and evaluation of the link between input and output interfaces within the defined System (4.2.5) is the task of the Causal Analysis, according to the applied safety concept in 2.2.

4.3 Detailed System Definition - Functional Analysis

4.3.1 Functional consideration concerning safety in railway operations

4.3.1.1 The purpose of the following statements is to describe the fundamental connections that are to be considered in determining safety-relevant functions. Since these functions are often designated "operational functions", the description of the connections in railway operations represents the main area of the considerations.

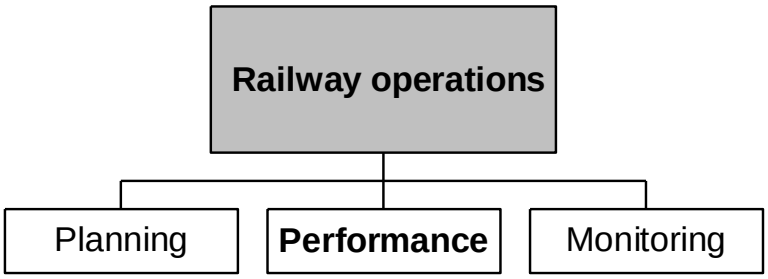
4.3.1.2 Following fundamental representation results:



4.3.1.3 Railway operations can be described as the totality of all measures that serve the conveyance of persons or goods.

4.3.1.4 In this, maintenance is regarded – although other definitions are possible – as not belonging to railway operations. The maintenance process is however included in determining the relevant functions for safe railway operation.

4.3.1.5 In consideration of the tasks to be performed here, the following further sub-division results:



4.3.1.6 "Planning" covers the following examples: route management – including the preparation of operational documents for the performance of moves –, planning of the conveyance of special consignments and vehicles, preparation of the necessary instructions for action by persons involved in railway operations, and the training and advanced training of those involved. This also however includes the principle that facilities are designed in such a manner that hazards arising from operating errors are prevented or, at least, made more difficult.

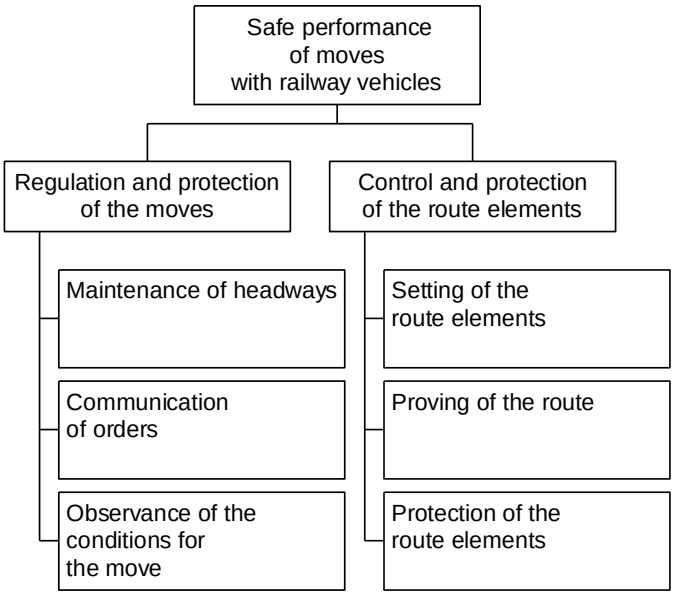
4.3.1.7 "Performance" includes railway operations in the narrower sense; this is to be defined as the intentional movement of railway vehicles on a railway infrastructure and comprises all measures directly connected with it. "Train operation" is a term commonly used for this as well. In the following, the term "moves" is used for the intentional movement of railway vehicles, since it is not necessary to distinguish between train and shunting moves in this connection.

4.3.1.8 "Performance" also includes the execution of construction and maintenance work, which can - insofar as it does not have any effect on the performance of moves - be disregarded.

4.3.1.9 "Monitoring" comprises all measures which serve to ensure that the rules applying to the safe performance of operations are complied with. This also includes the supervision of operational safety, the activity of railway traffic managers and the activity of those monitoring staff in actual railway operations. Scheduling tasks – even if they contain a "monitoring" component – are to be allocated to "performance" since they serve the performance of moves.

4.3.1.10 All of the areas mentioned above contribute to the safety of railway operations, but to different degrees. The following deals only with "performance" in more detail.

4.3.1.11 The fundamental connections below can be identified for the safe movement of railway vehicles:



4.3.1.12 For more far-reaching considerations, the definition as above does not seem sufficient since the terms are in part too theoretical and make a further examination of completeness more difficult. In addition, the classification is very much oriented towards the actual performance of moves and thus inevitably does not consider further aspects that are of significance for safety.

4.3.1.13 Instead, the functional approach will be used, where the relevant phases as in the time-related sequence of a move should first of all be defined and further functions allocated here.

4.3.2 Process

4.3.2.1 The functions used for the hazard identification are sufficient general to cover all possible applications and there will therefore not be a need for using an application approach in addition.

4.3.2.2 The functions used for the hazard identification are derived in a process according to the following.

4.3.2.3 The relevant phases as in the time-related sequence of a move should first of all be defined and further functions allocated here.

4.3.2.4 The following phases result of a train movement:

❶ Plan move
❷ Prepare move
❸ Schedule move
❹ Set up conditions for move
❺ Authorise move
❻ Perform move
❼ Conclude move

4.3.2.5 As a starting point all functions relevant for the railway operation are taken into account. Functions in terms of construction and maintenance works are considered if they affect the train run.

4.3.2.6 From these functions only those which are relevant for CCS TSI are kept. Those are functions that are totally or partly carried out by the CCS TSI effect the CCS TSI (e.g. functions that provide information/input which is necessary for CCS TSI). To decide if a function has relevance to CCS TSI and to verify it, adequate expertise is pre-requisite.

4.3.2.7 The remaining functions are to be detailed until a specific realisation level has been achieved. It becomes apparent that it is possible only as from a certain degree of detail to make meaningful definitions for functions which enable further sub-division and assessment.

4.3.2.8 According to the Rationale it is not desirable to deal with functions on a specific realisation level. Therefore the more general functions from (4.3.2.4) will be used assuring the detailed functions are covered. As far as the degraded modes are representing specific realisations, they are also covered.

4.3.2.9 The resulting functions are used for hazard identification.

4.3.3 Functional Analysis

4.3.3.1 Using the process described above and using the 'Functional Analysis Of Trans – European Rail Operation Reference' {Ref.: 8}. the CCS TSI relevant functions were derived.

4.3.3.2 The derived CCS TSI functional list have been verified by the EEIG Operational Rules Writing Group by performing a crosscheck of the functions {Ref: 12}

4.3.3.3 The relevant functions are listed in the following table below. If a function is CCS TSI relevant or not has been assessed by expert with knowledge of the system

Ref.	Functions relevant for railway operation		Function relevant for CCS TSI	
	Function	Annotations	X	Explanation

1	**Plan move**	The functions to be exercised at the planning level do not as yet govern any individual case (no single, concrete movement) but initially specify the boundary conditions; to this extent, an enumeration could be done without. Nevertheless, interfaces to the systems used during this phase may arise (e.g. with reference to data exchange).		
1.1	Check whether movement(s) can actually be performed (plausibility check for pathing application)	checking whether and under what conditions specified vehicles can run on specified infrastructure		
1.1.1	running system prerequisites			
1.1.2	brake system prerequisites			
1.1.3	requisite type of traction			
1.1.4	non-conflicting paths			
1.2	Design train paths			
1.2.1	elaborating the path			
1.2.2	timetable documents			
1.2.2.1	Produce			
1.2.2.2	Publicise			
1.2.3	special operational arrangements	This is required in the event of special provisions in/deviations from the rules, e.g. in respect of out-of-gauge loads/ vehicles, test runs		
1.2.3.1	Produce			
1.2.3.2	publicise			
1.3	Plan provision of vehicles (inclusive of means of traction)	Rolling stock rosters. No further subdivisions due to this not having a bearing on safety		
1.4	Plan rostering of staff	Job/duty rosters - but with no specification of duties in individual instances. No further subdivisions due to this not having a bearing on safety		
2	**Prepare move**			
2.1	Providing vehicles required (including means of traction)	vehicles must be suitable for the respective concrete scenario (i.e. specific movement).		
2.2	Providing staff	Staff are to be provided in the numbers required - i.e. in the numbers required to carry out the relevant movement in accordance with the applicable regulations.		
2.3	Forming the train			
2.3.1	mechanical coupling of individual vehicles	Screw or automatic coupling		
2.3.2	connecting up power supply lines			
2.3.3	connecting up control lines			
2.3.4	air pipe connections	Brake and air pipes		
2.3.5	documenting formation of train		**X**	information about braking characteristics
2.4	Checking that train is safe to operate and fit to run	Not a basic function of running; has purpose of establishing »safe condition of vehicles«.		
2.4.1	vehicle handling during running			

2.4.2	preparation of motive power stock			
2.4.3	establish condition and fitness for function of vehicle's brakes		**X**	functionality of brakes is prerequisite for correct calculation of braking curves
2.4.4	»train initialisation«	Train number, max. permissible speed, effective braking power, length, load if applicable.	**X**	information necessary
2.5	Providing information required for movement	The adjacent information may be known in advance (as a result of the planning phase) (e.g. timetable documents citing routing and destination as well as information about track-related deviations/particularities) or be announced at short notice (e.g. for shunting moves) (e.g. diversionary routes); also classified as special features are details of non-standard consignments that are not scheduled to run permanently in the train.		
2.5.1	purpose of movement			
2.5.2	destination of movement			
2.5.3	route of movement			
2.5.4	special features of movement		**X**	relevant for route suitability
3	**Schedule move**			
3.1	Arranging the sequence of movements			
3.1.1	determining actually possible time of departure	as a function of the current operating situation (capacity of line and stations)		
3.1.2	determining sequence of movements			
3.1.2.1	where movements cannot occur simultaneously	simultaneous occupation of track elements not possible (= conflicting routes)		
3.1.2.2	where interdependencies between movements	connecting service, vehicle transfer, staff transfer		
3.2	Adopt measures if schedule targets not adhered to	= short-notice alteration of schedule		
3.2.1	unscheduled change of stops	where a need arises at short notice (customer request) as well as leaving out a stop		
3.2.2	deviations from scheduled train formation			
3.2.2.1	exceedance of scheduled load			
3.2.2.2	exceedance of scheduled length			
3.2.2.3	exceedance of scheduled number of axles			
3.2.2.4	change in traction type	only has bearing on safety if change is from diesel to electric traction		
4	**Set up conditions for move**			
4.1	Prove reliability of movement (comparison with planning parameters)	Return to »Planning« or »Regulation« phase in event of deviations		
4.1.1	take account of restrictions on clearance			
4.1.2	take account of restrictions on load (permissible load per axle/metre)			

4.1.3	take account of restrictions on type of traction			
4.1.4	take account of restrictions on use of certain vehicles			
4.2	Setting track elements	Take account of reliability: e.g. do not switch occupied switches; this function is to be assigned to the »Protecting track elements« function for the preceding or following movement.		
4.2.1	track switches			
4.2.2	switches in safety overlap			
4.2.3	flank protection devices			
4.2.4	level crossings			
4.3	Checking track elements	Intended effect achieved, no deviations with a bearing on safety reported.		
4.3.1	correct position/correct status	Switch position, level crossings secured		
4.3.2	regular position or no fault message			
4.4	Securing track elements	Ensure they are at the requisite status for the duration of the movement		
4.4.1	»locking« of track elements prior to authorising the movement (over this track element)			
4.4.2	»locking« of track elements while movement is being performed	The »locking« state is to be maintained at least until the track element has been negotiated.		
4.4.3	revocation of movement authority if the status of the track elements subsequently changes			
4.5	Ensure that the section required for the movement is clear of vehicles to the extent necessary	The extent necessary is determined by the purpose of and the boundary conditions for the movement		
4.5.1	section to be travelled over			
4.5.2	additional sections if applic. (»overlap sections«)	Safety distance, safety overlap, section between fouling point for a track switch and flank protection device.		
4.6	Check that there are no other impediments to running			
4.6.1	evaluation of operational hazard reports	Wind warning, avalanche warning, landslide warning.	**X**	
4.6.2	reporting of engineering works/worksites		**X**	
4.6.3	perception of person responsible for checking			
4.6.4	report by other persons			
4.7	Maintaining headways	Exclusion of moves that might endanger each other		
4.7.1	protection against moves in rear			
4.7.2	protection against opposing moves	Opposing moves also include movements in the opposite direction to that allowed (e.g. inadmissible setting back).	**X**	function partly executed in the interlocking
4.7.3	protection against collisions at switches			
4.8	Protection against unintended movements by vehicles			
4.8.1	active flank protection considered as 'track elements'			
4.8.2	shunting prohibited		**X**	

5	**Authorising move**			
5.1	Convey orders/authorisations	No necessity for further subdivisions at this point, since it is already necessary to cite solutions (e.g. optical, written, acoustical orders, ...)	**X**	
6	**Perform move**			
6.1	Observing/obeying to max. permissible speeds			
6.1.1	taking account of line-related restrictions			
6.1.1.1	max. permissible speed as a function of track layout	Restriction due to radius of curves, cant, transition curves and length of cant gradient	**X**	
6.1.1.2	max. permissible speed when passing switches	Restrictions in the deflecting or more tightly curved section of the switch and in the case of trailable points.	**X**	
6.1.1.3	max. permissible speed when passing level crossings	Restriction of top speed, speed as a function of the length of the strike-in section.	**X**	
6.1.1.4	max. permissible speed on bridges		**X**	
6.1.1.5	max. permissible speed on embankments		**X**	
6.1.1.6	max. permissible speed due to the superstructure		**X**	
6.1.1.7	max. permissible speed due to the subgrade		**X**	
6.1.1.8	max. permissible speed due to the catenary design		**X**	
6.1.1.9	max. permissible speed at sections tight on gauge	if distance between tracks insufficient in terms of the kinematic envelope.	**X**	covered by function 6.2.10
6.1.1.10	max. permissible speed in the event of deviations in track elements from nominal state (with reference to movement at a defined speed)	Switch without signal interlocking, technical protection at level crossing has failed.	**X**	
6.1.1.11	max. permissible speed following engineering work		**X**	
6.1.2	taking account of vehicle-related restrictions			
6.1.2.1	max. permissible speed of train due to running properties of vehicles		**X**	
6.1.2.2	max. permissible speed due to braking properties of vehicles		**X**	
6.1.2.3	max. permissible speed in event of deviations from nominal state of vehicle components with a bearing on safety (with reference to movement at a defined speed)		**X**	
6.1.2.4	max. permissible speed when movements meet		**X**	
6.1.2.5	max. permissible speed in the event of cross-winds		**X**	
6.1.3	taking account of procedure-related restrictions			
6.1.3.1	max. permissible speed when running on sight	Observing this speed is not a function required in itself to guarantee safety; the intention, instead, is to facilitate performance of the »Stop at required point« function.	**X**	
6.1.3.2	max. permissible shunting speed	as above	**X**	
6.1.3.3	max. permissible speed for banked	as above		

	movements			
6.1.3.4	max. permissible speed when setting back in the event of danger	as above	**X**	
6.1.3.5	max. permissible speed when entering dead-end tracks	as above	**X**	
6.1.3.6	max. permissible speed when entering partially occupied tracks	as above	**X**	
6.1.3.7	max. permissible speed for reasons of safety of track works	not a function for protecting movement	**X**	
6.1.3.8	max. permissible speed in case of temporary speed restrictions		**X**	
6.2	Observing (further) line-related restrictions			
6.2.1	lower pantograph(s) at required point	Turntables, traversers, crane trackage, other sections without catenary or to be passed with pantograph down.	**X**	
6.2.2	switch off motive power unit current (main switch off) at required point	Insulated sections, changes of system, depot gates with insulated catenary adaptor.	**X**	
6.2.3	limiting current consumption (high-voltage limit values)			
6.2.4	no sanding at specified points	Points, turntables, traversers (in each case except in hazardous circumstances)		
6.2.5	where possible, prevent motive power units travelling light from stopping on sections they have sanded			
6.2.6	avoid stopping with pantographs raised beneath section insulators and section divisions			
6.2.7	warning by issuing acoustic signals at requisite point	Indication by means of trackside signals or corresponding instructions on what to do.		
6.2.8	avoid stopping at points not suitable for the adoption of auxiliary measures or only poorly so	Emergency brake override; function is only of relevance, however, in the event of an incident (notably fire).	**X**	
6.2.9	take account of restrictions in the use of specified brake designs	e.g. eddy-current brake	**X**	
6.2.10	Prove reliability of movementb	- loading gauge - power supply - axle load	**X**	route suitability
6.2.11	Reversing in the event of danger	ERTMS/ETCS FRS 11.3.2 and SRS 4.4.18 and 5.13	**X**	
6.3	Observing (further) vehicle-related restrictions			
6.3.1	no manual sanding during skidding			
6.3.2	take note of conditions governing the raising of lowered pantographs	Max. permissible speed as function of pantograph design; do not raise beneath overhead crossings and section insulators.		
6.3.3	take note of operating restrictions for motive power unit	E.g. do not exceed continuous tractive effort for any length of time; function has purpose of maintaining availability.		
6.4	Ensure stops required for reasons of safety			
6.4.1	stopping at a signal at danger	Cab display is synchronised with signals at danger. This includes the provision that onward movement following a stopping event may only occur once the stop has been revoked.	**X**	
6.4.2	stopping before stationary vehicles	to the extent that vehicles are not	**X**	

		protected by signals at danger (depending on the mode of operation)		
6.4.3	stopping at track closings	Reference may not be necessary, since track closings are indicated by means of signals at danger.	**X**	
6.4.4	stopping before other obstacles (than vehicles) on the track	to the extent that the movement has been specifically authorised to do so.	**X**	
6.5	Ensuring stops required (= scheduled) for other reasons	= customer stops		
6.5.1	stop for passenger entry/egress at designated point			
6.5.2	stop to load/unload			
6.5.3	stop for change of staff			
6.5.4	stop to alter train formation	also change of traction/detachment of banking locomotive		
6.6	Check for safety-related deviations to railway installations on used route and adopt measures	Not a basic function of train running; serves to ensure the »safe state of railway installations«.	**X**	
6.6.1	irregularities in track	e.g. broken rails, poor track geometry		
6.6.2	irregularities in structures	e.g. bridges		
6.6.3	irregularities in facilities for traction current supply	overhead line (catenary), live rail, feeder cable where applic.		
6.6.4	irregularities at level crossings	e.g. open barriers		
6.7	Check for safety-related deviations to vehicles on the movement concerned and adopt measures	Not a basic function of train running; serves to ensure the »safe state of railway installations«.		
6.7.1	running-gear irregularities			
6.7.2	irregularities in the brakes			
6.7.3	irregularities in the vehicle's safety equipment		**X**	
6.8	Protecting passenger entry/egress			
6.8.1	adapting door operation to throughput of passengers			
6.8.2	keeping doors closed while train is moving			
7	**Conclude move**			
7.1	Releasing track elements			
7.1.1	release »locking« of track elements			
7.1.2	return track elements to normal position (where applicable)	Normal position for level crossings is generally »Barriers open«, whilst no normal position is necessarily required for switches.		
7.2	Protecting parked vehicles			
7.2.1	applying brakes		**X**	
7.2.2	using safeguards	e.g. stop blocks, scotches		
7.3	Splitting up train	May - where technically feasible and permissible in a specific instance - also be carried out before the movement has finished (e.g. separating banking unit from train).		
7.3.1	disconnecting power supply lines			
7.3.2	disconnecting control lines			
7.3.3	disconnecting air pipes			
7.3.4	disconnecting mechanical coupling			
7.3.5	producing requisite documents	List of dividing points.		
7.3.6	closing-down service			

8	**Miscellaneous**			
8.1	Rules & Regulations			
8.1.1	develop	comprises the processing of experience and feedback		
8.1.2	distribute			
8.1.3	observer / obey to	comprises examination e.g. by authorities		
8.2	accident, (hazardous) incident			
8.2.1	operation control centre			
8.2.2	emergency management			
8.2.3	accident investigation		**X**	juridical recording
8.3	Ensure safe condition of railway infrastructure		**X**	
8.4	Ensure safe condition of vehicles		**X**	
8.5	Formation, Training and Qualification	comprises safety instructions, accident prevention und 'safety at work'	**X**	

4.3.4 Failure Modes

Failure modes are derived in a process of brainstorming accompanied by the usage of a checklist:
Function required but not fulfilled
Function fulfilled but not required
Right function with wrong object
Wrong function with right object
Wrong function with wrong object
Interface failure
Information missing
Information wrong
Information incomplete
Information misleading
Information to complex
Wrong order
Wrong direction
Too early/too late
Too high/too low
Too long/too short
Too much/not enough
Outdated
Inconsistent
Disregard information
Misinterpretation
Complexity functionality and information
Miscommunication

5 Hazard Identification

5.1 Process

5.1.1.1 The hazard identification is based on the abstract functional system definition (chapter 4). For this reason the hazards identified are independent of specific realisations or applications. Specific realisations or circumstances are to be taken into consideration by the Causal Analysis, which evaluates/analyses the technical solution in order to identify causes for hazards and verify if new hazards arise from system design.

5.1.1.2 Following a systematic approach all aspects taken into account while analysing functions and their failure modes are written down to a Hazard Identification Table.

5.1.1.3 Hazard Identification Table

Panel headline	Headline explanation
Function **[Reference chapter 4.3.3]**	CCS TSI relevant function from chapter 4.3.3 'Functional Analysis'
Function description	Detailed explanation and description of the Function. In case the function is only partly carried out by CCS TSI, this part is to be described here.
Hazard **[Number]**	Failure mode of CCS TSI relevant function (CCS TSI relevant hazard)
Limitations	If the description of the function or the hazard may lead to misunderstandings it is to be mentioned here, what is NOT covered by the function.
Simplified consequence analysis	Possible direct consequences of the hazard
Examples for causes for the hazard	Examples for direct causes for the hazard
Annotation	If anything else which does not fit in the boxes above is of greater importance, it is to be mentioned here. Also grouping of hazards to a single hazard is to be mentioned here.
System border check	Allocation of hazard according to the system structure. (see 5.1.1.9 for details).

5.1.1.4 The functions considered as CCS TSI relevant, resulting from the functional analysis (chapter 4.3.3) are taken into account as a basis for hazard identification. Such functions that are only in part CCS TSI relevant, the part of the function which is CCS TSI relevant is taken into account for hazard identification. (Only this part is described in the panel 'Function description')

5.1.1.5 With expert knowledge failure modes (key words to identify typical failure modes, see check list in chapter 4.3.4) has been applied to CCS TSI relevant functions. Failure modes of CCS TSI relevant functions are CCS TSI relevant hazards. Experts from different railways have been consulted in order to check the completeness of the

hazards identified.

5.1.1.6 CCS TSI relevant hazards are to be checked, if they are safety relevant or not, based on a simplified consequence analysis. If there is a probability higher than 0 of an accident as direct consequence of a CCS TSI relevant hazard, the hazard is safety relevant.

5.1.1.7 EN 50129:2003 {Ref.: 16} defines in 3.1.1 accident as “an unintended event or series of events that results in death, injury, loss of a system or service, or environmental damage”. For deriving the CCS TSI relevant hazards the accidents taken into account are:

Accident	Explanation
Derailment	a) Vehicle sliding off or lifting-off from track, even if it rerails itself again b) double-track movement of a vehicle
Collision	Railway vehicle drives against another railway vehicle
Contact	Driving against persons (not passengers) or obstacles within the structure gauge (e.g. buffer stop, derailer, tree, stop block) but not against another railway vehicle
Collision with road traffic	Collision between railway vehicle and road traffic on a level crossing (excluding misuse of level crossings).
Industrial Accident	Accident at work (railway workers)

5.1.1.8 The accidents mentioned above are only considered in case they are arising from a CCS TSI failure. Only CCS TSI relevant hazards which are safety relevant are kept for further consideration.

5.1.1.9 System Border Check

As final step the resulting hazards from step 3 are put to a 'system border check' to decide about the allocation in the system model (chapter 3.2.1.8):

5.1.1.10 System Hazard: Hazard Type A

If an output interface (OUTI) transmits erroneous information to the System Environment, we are dealing with a System Hazard.

5.1.1.11 Causes for System Hazards:

Type B

Type C

5.1.1.12 Hazard Type B

A failure has either been occurred within the OUTI (The appropriate element works correctly, but the information is transmitted erroneously via the OUTI to the System Environment) or the System provides the OUTI with erroneous information.

Causes for that could be:

- A hazard has occurred within an ELI as a result of information processing.
- A hazard has occurred within an ELI. (The appropriate transmitting element(s) work correctly, but the information is transmitted erroneously to the receiving element(s))
- A hazard has occurred within an INI (The incoming information from the System Environment is correct, but it is transmitted erroneously to the system)

5.1.1.13 Hazard Type C

The System Environment provides the INI with erroneous information

5.1.1.14 In case of a hazard matching type (**A**) it is a System hazard. Taking into account the considerations of chapter 3.2 it is to decide which output interfaces are involved ('Output Interfaces', chapter 4.2.4.7 and 4.2.4.8). For each output interface involved, an individual hazard is to be included in the final System hazard log (chapter 5.3). For each of those System Hazards THR/SIL will be introduced.

5.1.1.15 In case of a hazard matching type (**B**) it is a cause for another hazard. It will be documented to show that this hazard is considered. The analysis or evaluation of this hazard shall be done by a Cause Analysis (see 2.2.1.4).

5.1.1.16 In case of a hazard matching type (**C**) it is either completely outside of the defined system or occurs at the input interface to the defined system. Hazards occurring at the input interfaces to the system are not considered since those are hazards belonging to other systems (see also 4.2.5.1). If correct information from other systems is falsified within an input interface, then this is considered as hazard, but analysed/evaluated by a Causal Analysis (see 2.2.1.4). If the hazard is completely outside of the defined system, no further evaluation in terms of the defined system is done since those hazards are not in the scope of TSI CCS..

5.1.1.17 In case some hazards are considered to have the same causes and consequences, they are merged together and handled as a single hazard.

5.1.1.18 Examples for the causes are listed for each hazard.

5.1.1.19 Systematic consistency cross-check of the inputs/outputs to/from the defined system in order to ensure completeness of the hazards found

5.1.1.20 The Hazard Identification Table with a more complete set of panels is supposed to be used if a failure mode of a function turns out to be a System Hazard. If a function during analysis turns out to have no relevance in finding a new System Hazard, the amount of panels of the Hazard Identification Table may be reduced appropriately.

5.2 Assumptions

5.2.1 Common Cause

Two ore more hazards may occur together as a result of a common cause. The consideration and evaluation of common causes is the task of a Causal Analysis, as defined in EN 50129 {Ref.: 16} Figure A.2.

5.2.2 Link of Causes to System Hazards

According to EN50129 figure A.4 shows, that the cause of a hazard at system level (Hazard Type A) may be considered as a hazard at subsystem level (Hazard Type B). A link of Hazards Type B towards hazard(s) Type A can be drawn by a structured hierarchical approach to hazard analysis and hazard tracking. Table E.6 of EN50129 {Ref.: 16} provides methods for failure and hazard analysis. According to A.4.2 of EN 50129{Ref.: 16}, the supplier carries out a Causal Analysis, which includes the analysis of system/sub-system to meet the requirements. Concluding, EN 50129 {Ref.: 16} reveals, that the link of Hazards Type B towards Hazards Type A is analysed while carrying out a Causal Analysis

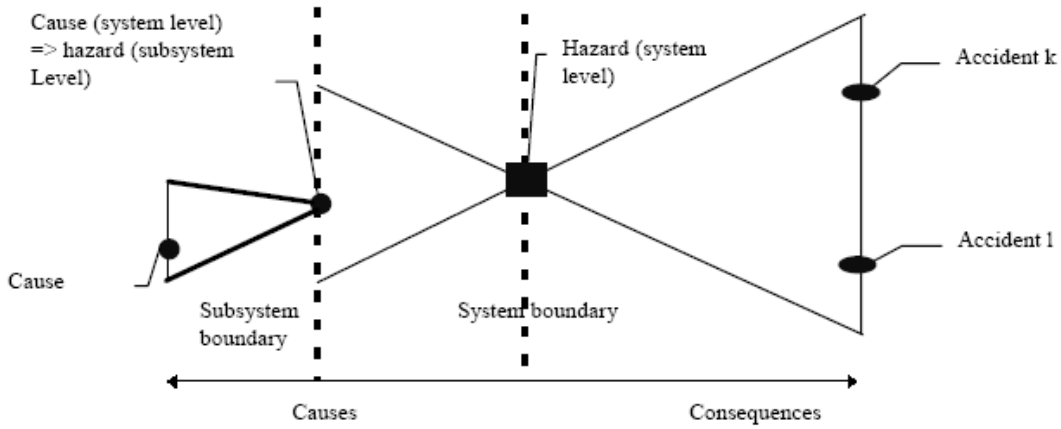


Figure A.4 – Definition of hazards with respect to the system boundary

5.2.3 Untimely brake application or train trip

At the moment "Untimely brake application or train trip" has not been considered as a system hazard, but it is added to the Open Points List. The potential amount of risk has to be evaluated and the Railways consulted.

The result could be:

- hazard exist but commercial requirement on the system is higher then the requirements due to this risk
- new class of accident to be added and hazard included.

5.3 Log of hazards

Function [2.3.5]	documenting formation of train
Function description	For braking curves to be correctly established, the data used for calculation purposes have to be consistent with actual conditions. The data documented here form the basis for inputting data into ETCS.
Hazard **[2.3.5]**	**greater effective braking power documented than actually available**

Limitations	It is assumed in the case of this hazard that EBP has been correctly established. Data input into ETCS is considered separately.
Simplified consequence analysis	incorrect data input
System border check	Hazard Type C

Function [2.4.3]	establish condition and fitness for function of vehicle's brakes
Function description	ETCS generates prescribed values for brakes (braking curves) on the basis of the train’s calculated braking capacity; the fitness for function of brakes is a precondition for the calculated and actual curves for a braking event being consistent.
Hazard [2.4.3-1]	**fitness for function of brakes not properly established**
Limitations	does not contain the proper train formation
Simplified consequence analysis	given proper train formation and fit-for-function brakes: none otherwise: braking curve incorrectly established
System border check	Hazard Type B

Function [2.4.3]	establish condition and fitness for function of vehicle's brakes
Function description	For braking curves to be correctly established, the data used for calculation purposes have to be consistent with actual conditions.
Hazard [2.4.3-2]	**greater effective braking power (EBP) calculated than actually available**
Simplified consequence analysis	incorrect starting data for establishing braking curve
System border check	Hazard Type B

Function [2.4.4]	'train initialisation'
Function description	train number acts as means of identification

Hazard [2.4.4-1]	**wrong train number in system**
Annotation	**Train number is service related not ETCS.**

Function [2.4.4]	'train initialisation'
Function description	ETCS checks that V(max) entered is adhered to
Hazard [2.4.4-2]	**max. permissible speed of train (VMAX) entered in system too high**
Limitations	no other speed limits and restrictions are affected
Simplified consequence analysis	max. permissible speed for vehicles on account of their running or braking properties not monitored
System border check	Hazard Type B

Function [2.4.4]	'train initialisation'
Function description	The train length is used to check that, where sections with restrictions are concerned (e.g. speed restrictions or sections that may only be negotiated with pantographs down), the whole section is traversed before the restriction is revoked.
Hazard [2.4.4-3]	**train length entered in system too low**
Simplified consequence analysis	speed increased too early pantograph raised too early motive power unit switched on too early
System border check	Hazard Type B

Function [2.4.4]	'train initialisation'
Function description	For braking curves to be correctly established, the data used for calculation purposes have to be consistent with actual conditions.
Hazard [2.4.4-4]	**greater effective braking power entered in system than available**

Limitations	In the case of this hazard, only the inputting of data is considered.
Simplified consequence analysis	braking curve incorrectly established
System border check	Hazard Type B

Function [2.4.4]	'train initialisation'
Function description	To correctly establish braking curves, details of the brake design/equipment on the rake - referred to here as »brake type« - are also required.
Hazard [2.4.4-5]	**wrong »brake type« entered in system**
Limitations	Incorrect entry of effective braking power is considered separately.
Simplified consequence analysis	braking curve incorrectly established
System border check	Hazard Type B

Function [2.5.4]	special features of movement
Function description	Information that is required to protect route suitability
Annotation	Failure modes of this function are causes for hazards [6.2.10-0] / [6.2.10-1]

Function [4.6.1]	evaluation of operational hazard reports
Function description	The evaluation of operational hazard reports is done by the interlocking operators. They take the appropriate measures (limitation of speed or blocking routes)
Annotation	The failure modes of this function are causes for further hazards dealt with in hazard [6.1-0] / [6.1-1].
System border check	Hazard Type C.

Function [4.6.2]	reporting of engineering works/worksites
Function description	The reporting of engineering works/worksites is directed to the interlocking operators. They may - if necessary - take measures (limitation of speed or blocking routes).
Annotation	The failure modes of this function are causes for further hazards dealt with in hazard [6.1-0] / [6.1-1].
System border check	Hazard Type C

Function [4.7.2]	protection against opposing moves
Function description	This function is partly carried out by the interlocking, the CCS TSI functionality considered here solely is the monitoring of the correct direction of running in relation to the assigned route.
Hazard [4.7.2]	**Unauthorised setting back**
Limitations	The hazard arising from any unintentional movement by the vehicle is considered separately.
Simplified consequence analysis	Collision collision with road traffic derailment
Examples for causes for the hazard	- error by staff - monitoring function inactive
Annotation	This function is carried out in the ETCS on-board unit.
System border check	Hazard Type A (Output Interface No. 1)

Function [4.8.2]	shunting prohibited
Function description	The 'prohibition to shunt' is an indirect measure to protect against unintended movements of vehicles or for flank protection.
Hazard [4.8.2]	**passing the defined border of the shunting area**

Limitations	
Simplified consequence analysis	Collision collision with road traffic
Examples for causes for the hazard	monitoring function inactive intervention function inactive error by staff (inadmissible auxiliary action to override the intervention function)
Annotation	
System border check	Hazard Type A (Output Interface No. 1)

Function [5.1]	Convey orders/authorisations
Function description	ETCS generates the movement authority with reference to permissible speeds and end of authority on the basis of information from the signalbox.
Hazard [5.1-1]	**movement authority inadmissibly generated**
Limitations	Proving that the preconditions for permission to proceed have been met is considered separately.
Simplified consequence analysis	move is inadmissibly authorised
Annotation	The term »inadmissible permission to proceed« also applies if • an order to run on sight is (not) given or displayed • a movement authority continues to be given or displayed beyond the area monitored (transfer to another automatic train control system).
System border check	Hazard Type B

Function [5.1]	Convey orders/authorisations
Function description	ETCS transmits permission to proceed with reference to permissible speeds, special factors to be considered and end of authority.
Hazard [5.1-2]	**move inadmissibly authorised**

Limitations	Proving that the preconditions for permission to proceed have been met is considered separately.
Simplified consequence analysis	Derailment contact collision with road traffic collision
Examples for causes for the hazard	error by staff (assisted move permitted or inadmissible issue of command authorising motive power unit to proceed) incorrect information from signalbox regarding meeting the preconditions for permission to proceed movement authority inadmissibly generated in the ETCS central unit incorrect information transmitted from the ETCS central unit incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit incorrect data displayed on DMI Incorrect use of 'track ahead free' ackowledgement
Annotation	The term »inadmissible permission to proceed« also applies if • an order to run on sight is (not) given or displayed • a movement authority continues to be given or displayed beyond the area monitored (transfer to another automatic train control system).
System border check	Hazard Type A (Output Interface No. 2)

Function [5.1]	Convey orders/authorisations
Function description	CCS transmits permission to proceed with reference to permissible speeds and end of authority. Where the conditions for permission to proceed cease to be met and the movement authority (from a given point) is accordingly withdrawn, information to this effect is required.
Hazard [5.1-3]	**permission to proceed not withdrawn in time in the event of danger**
Limitations	The »Withdraw permission to proceed« function is executed in the signalbox. Only the hazard arising from information omitted or incorrectly transmitted and evaluated is considered at this point.

Simplified consequence analysis	Derailment contact collision with road traffic collision
Examples for causes for the hazard	incorrect information from signalbox information incorrectly evaluated in the ETCS central unit information incorrectly transmitted from the ETCS central unit information incorrectly evaluated in the ETCS on-board unit incorrect transmission of emergency stop via GSM-R (voice)
System border check	Hazard Type A (Output Interface No. 2)

Function	various (see *Limitations*)
Function description	ETCS monitors adherence to section-related speed restrictions (max. permissible speed as well as speed reductions prior to the section concerned and increases in speed at the end of same) and prevents these being disregarded by intervening accordingly.
Hazard [6.1-0] / [6.1-1]	**permissible speed as a function of route characteristics incorrectly shown / not enforced**
Limitations	This hazard is a collective representation of those that follow (reference being made to the fact at the relevant points), since the consequences of all of the latter are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment

Examples for causes for the hazard	project-planning errors (speed restriction not provided for, incorrect value for permissible speed, start or end of restricted speed section wrongly projected) data input omitted (speed restriction not entered, incorrect value for permissible speed) in respect of temporary speed restrictions data incorrectly entered (start or end of a restricted-speed section) in respect of temporary speed restrictions position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (start or end of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard.
System border check	Hazards Type A [6.1-0] Output Interface No. 2 [6.1-1] Output Interface No. 1

Function [6.1.1.1]	max. permissible speed as a function of track layout
Function description	ETCS monitors adherence to section-related speed restrictions (including the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.1.1-1]	**max. permissible speed as a function of the track layout incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment

Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.1]	max. permissible speed as a function of track layout
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard [6.1.1.1-2]	**speed not reduced in time in case of speed restrictions as a function of the track layout**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.1]	max. permissible speed as a function of track layout
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard [6.1.1.1-3]	**speed increased too early at speed restrictions as a function of the track layout**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.

Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.2]	max. permissible speed when passing switches
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.1.2-1]	**max. permissible speed when negotiating switches is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.2]	max. permissible speed when passing switches
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard [6.1.1.2-2]	**speed not reduced in time at speed restrictions when negotiating switches**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.

Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.2]	max. permissible speed when passing switches
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard [6.1.1.2-3]	**speed increased too early at speed restrictions when negotiating switches**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.3]	max. permissible speed when passing level crossings
Function description	In the range of level crossings speed restrictions may be imposed, because of - missing sight - length of distance from the level crossing to the point where it is activated - limitation of extent of damages at accident of road traffic with railway traffic The mentioned speed restrictions shall be displayed and monitored by the command and control system.

Hazard [6.1.1.3-0] / [6.1.1.3-1]	**permissible speed when passing level crossings is incorrectly shown / not enforced**
Simplified consequence analysis	Collision with road traffic
Annotation	The speed restriction is part of the safety concept of level crossings. Due to the fact, that in this case the consequences are significantly different to other hazards concerning speed restrictions it is considered as a separate hazard.
System border check	Hazards Type A [6.1.1.3-0] Output Interface No. 2 [6.1.1.3-1] Output Interface No. 1

Function [6.1.1.4]	max. permissible speed on bridges
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.1.4-1]	**max. permissible speed when running on bridges is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.4]	max. permissible speed on bridges
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.

Hazard [6.1.1.4-2]	**speed not reduced in time given speed restrictions when running on bridges**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.4]	max. permissible speed on bridges
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard [6.1.1.4-3]	**speed increased too early given speed restrictions when running on bridges**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.5]	max. permissible speed on embankments
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.1.5-1]	**max. permissible speed when running along embankments is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.

Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.5]	max. permissible speed on embankments
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard [6.1.1.5-2]	**speed not reduced in time given speed restrictions when running along embankments**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.5]	max. permissible speed on embankments
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard [6.1.1.5-3]	**speed increased too early given speed restrictions when running along embankments**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.6]	max. permissible speed due to the superstructure
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard **[6.1.1.6-1]**	**max. permissible speed on account of the track superstructure is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.6]	max. permissible speed due to the superstructure
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard **[6.1.1.6-2]**	**speed not reduced in time given speed restrictions on account of the track superstructure**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.6]	max. permissible speed due to the superstructure

Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard [6.1.1.6-3]	**speed increased too early given speed restrictions on account of the track superstructure**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.7]	max. permissible speed due to the subgrade
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.1.7-1]	**max. permissible speed on account of the subgrade is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.7]	max. permissible speed due to the subgrade
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard [6.1.1.7-2]	**speed not reduced in time given speed restrictions on account of the subgrade**

Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.7]	max. permissible speed due to the subgrade
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard **[6.1.1.7-3]**	**speed increased too early given speed restrictions on account of the subgrade**
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.1.8]	max. permissible speed due to the catenary design
Function description	ETCS monitors adherence to section-related speed restrictions (max. permissible speed as well as reductions in speed at the beginning of the respective section and increases in speed at the end thereof) and prevents these being disregarded by intervening accordingly.
Hazard **[6.1.1.8-0] / [6.1.1.8-1]**	**permissible speed on account of the design of the overhead line is incorrectly shown / not enforced**
Limitations	This hazard is a collective representation of hazards, since their consequences are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.

Simplified consequence analysis	damage to vehicle damage to railway facilities contact
Examples for causes for the hazard	project-planning errors (speed restriction not provided for, incorrect value for permissible speed, start or end of restricted speed section wrongly projected) data input omitted (speed restriction not entered, incorrect value for permissible speed) in respect of temporary speed restrictions data incorrectly entered (start or end of a restricted-speed section) in respect of temporary speed restrictions position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (start or end of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard.
System border check	Hazards Type A [6.1.1.8-0] Output Interface No. 2 [6.1.1.8-1] Output Interface No. 1

Function [6.1.1.9]	max. permissible speed at sections tight on gauge
Function description	At sections tight on gauge the speed is restricted for vehicles / loads, which deviate from the values designated for a route section.
Annotation	The max. permissible speed at sections tight on gauge at the moment cannot be displayed, monitored or enforced by ETCS (The function is carried out by written orders comprising speed restrictions), hence no further consideration is necessary.

Function [6.1.1.10]	max. permissible speed in the event of deviations in track elements from nominal state (with reference to movement at a defined speed)
Function description	The limitation of speed in the event of deviations in track elements from nominal state (disruption, exceedance of limit values) is a measure to guarantee the safe condition of railway infrastructure. It is the task of the command and control system to display and monitor the appropriate speed restrictions.
Annotation	Speed restrictions in the event of deviations in track elements from nominal state result in temporary speed limits and are considered in hazard [6.1-0] / [6.1-1].

Function [6.1.1.11]	max. permissible speed following engineering work
Function description	Following engineering work it may be necessary to impose speed restrictions with the relevant infrastructure (e.g. superstructure, switch)
Annotation	Speed restrictions following engineering work result in temporary speed limits and are considered in hazard [6.1-0] / [6.1-1].

Function [6.1.2.1]	max. permissible speed of train due to running properties of vehicles
Function description	ETCS monitors the max. permissible speed for the movement, entered as VMAX, which is limited as a function of the ride engineering on the vehicles in the rake, and prevents this being exceeded by intervening accordingly.
Hazard [6.1.2.1-0] / [6.1.2.1-1]	**permissible speed of train due to running properties of vehicles is incorrectly shown / not enforced**
Limitations	Restrictions in speed on account of the brake system on vehicles are considered separately. All other speed restrictions arising out of the interaction between vehicle/vehicle components and track/track components are assigned to hazards 6.1 ff. (»line-related speed restrictions«).
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment
Examples for causes for this hazard	error by staff incorrect data input monitoring function inactive intervention function inactive

System border check	Hazards Type A [6.1.2.1-0] Output Interface No. 2 [6.1.2.1-1] Output Interface No. 1

Function [6.1.2.2]	max. permissible speed due to braking properties of vehicles
Function description	ETCS monitors the max. permissible speed for the movement, entered as VMAX, which is limited as a function of the brake system on the vehicles, and prevents this being exceeded by intervening accordingly.
Hazard [6.1.2.2]	**max. permissible speed as a function of the brake system on vehicles is not adhered to**
Limitations	Restrictions in speed on account of the ride engineering on vehicles are considered separately.
Simplified consequence analysis	inadequate braking effect
System border check	Hazard Type B

Function [6.1.2.3]	max. permissible speed in event of deviations from nominal state of vehicle components with a bearing on safety (with reference to movement at a defined speed)
Function description	The limitation of speed in event of deviations from nominal state of vehicle components (e.g. hot axle bearings) is a measure to guarantee the safe condition of the vehicles.
Annotation	The harmonised specification for HABD is revealed in the TSI rolling stock subsystem. This function is completely carried out outside the defined system.

Function [6.1.2.4]	max. permissible speed when movements meet
Function description	Dependent on the combination of - trains and - characteristics of the infrastructure (tunnel, distance between tracks) on the appropriate section, speed restrictions when movements meet, may be necessary. The command and control system ought to display and monitor the appropriate speed restrictions.
Hazard [6.1.2.4]	**max. permissible speed when movements meet incorrectly shown not enforced**

Simplified consequence analysis	damage of trains derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.2.5]	max. permissible speed in the event of cross-winds
Function description	Dependent on the composition of the train on the appropriate section speed restrictions in the event of cross-winds exceeding a certain degree may be necessary.
Hazard [6.1.2.5]	**permissible speed in the event of cross-wind incorrectly shown / not enforced**
Simplified consequence analysis	damage of trains derailment
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form [6.1-0] / [6.1-1] and is no longer considered separately.

Function [6.1.3.1]	max. permissible speed when running on sight
Function description	ETCS monitors observance of the max. permissible speed when running on sight and prevents this being exceeded by intervening accordingly.
Hazard [6.1.3.1-0] / [6.1.3.1-1]	**permissible speed when running on sight incorrectly shown / not enforced**
Limitations	This hazard is a collective representation of hazards, since their consequences are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.
Simplified consequence analysis	in the case of collision, collision with road traffic or contact: extent of damage greater

Examples for causes for this hazard	project-planning errors (start or end of applicable section wrongly projected) position of movement incorrectly identified incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI monitoring function inactive intervention function inactive
Annotation	Hazards arising from non-observance of speed restrictions for other reasons are dealt with as separate hazards. Exceedance of the max. permissible speed on account of sighting conditions is not considered here, as approximate values only can be given for this speed, which is variable in any case, and the attendant function (ensure stop before obstacles) is by definition irrelevant to the ETCS DB pilot, moreover.
System border check	Hazards Type A [6.1.3.1-0] Output Interface No. 2 [6.1.3.1-1] Output Interface No. 1

Function [6.1.3.1]	max. permissible speed when running on sight
Function description	ETCS monitors observance of the max. permissible speed when running on sight and prevents this being exceeded by intervening accordingly.
Hazard [6.1.3.1-2]	**permissible speed when running on sight is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Simplified consequence analysis	in the case of collision, collision with road traffic or contact: extent of damage greater

Examples for causes for this hazard	project-planning errors (start of applicable section wrongly projected) position of movement incorrectly identified incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI monitoring function inactive intervention function inactive
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.1.3.1-0] / [6.1.3.1-1] and is no longer considered separately.

Function [6.1.3.1]	max. permissible speed when running on sight
Function description	ETCS monitors observance of the max. permissible speed when running on sight. This involves the applicable speed being achieved at the beginning of the running-on-sight section.
Hazard [6.1.3.1-3]	**speed not reduced in time when running on sight**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Simplified consequence analysis	in the case of collision, collision with road traffic or contact: extent of damage greater
Examples for causes for this hazard	project-planning errors (start of applicable section wrongly projected) position of movement incorrectly identified incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form [6.1.3.1-0] / [6.1.3.1-1] and is no longer considered separately.

Function [6.1.3.1]	max. permissible speed when running on sight
Function description	ETCS monitors observance of the max. permissible speed when running on sight. This involves speed being monitored until the front of the leading vehicle has left the section in question.
Hazard [6.1.3.1-4]	**speed increased too early when running on sight**
Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Simplified consequence analysis	in the case of collision, collision with road traffic or contact: extent of damage greater
Examples for causes for this hazard	project-planning errors (start of applicable section wrongly projected) position of movement incorrectly identified incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form [6.1.3.1-0] / [6.1.3.1-1] and is no longer considered separately.

Function 6.1.3.2	max. permissible shunting speed
Function description	The permissible speed while shunting is to be displayed and monitored by the control command system.
Hazard [6.1.3.2-0] / [6.1.3.2-1]	**permissible shunting speed is incorrectly shown / not enforced**
Limitations	The speed limit caused by track characteristics is dealt with separately. Since in this case other functions are authoritative (e.g. 6.4.2 ,6.4.4) the exceedance of the permissible shunting speed as a single cause does not lead to an accident/incident.
Simplified consequence analysis	Increase of extent of damage or avoidance of accident / incident (Collision, damage to vehicles)

System border check	Hazards Type A [6.1.3.2-0] Output Interface No. 2 [6.1.3.2-1] Output Interface No. 1

Function [6.1.3.4]	max. permissible speed when setting back in the event of danger
Function description	When reversing the permissible speed is to be displayed and monitored by the command and control system.
Hazard [6.1.3.4-0] / [6.1.3.4-1]	**permissible speed when reversing** in the event of danger **is incorrectly shown / not enforced**
Limitations	The speed limit caused by track characteristics is dealt with separately. Since in this case other functions are authoritative (6.4.1 and 6.4.3) the exceedance of the permissible speed as a single cause does not lead to an accident/incident.
Simplified consequence analysis	In case of collision, collision with road traffic: Increase of extent of damage
System border check	Hazards Type A [6.1.3.4-0] Output Interface No. 2 [6.1.3.4-1] Output Interface No. 1

Function [6.1.3.5]	max. permissible speed when entering dead-end track
Function description	The end of a dead-end track is a location at which a stop is always required. In ETCS, this stop is monitored like a stop at an end of movement authority and no special speed restriction is monitored. This function is covered by hazard [6.4.1-1].
Hazard [6.1.3.5-1]	**max. permissible speed when entering dead-end tracks is exceeded**
Annotation	The restriction of speed when entering dead-end tracks is a procedure-related restriction serving to reduce the extent of any damage in the event of contact. The respective function and the hazards derived there from are enumerated merely for the sake of completeness and are not considered in any greater detail hereafter. This function is covered by hazard [6.4.1-1]

Function [6.1.3.5]	max. permissible speed when entering dead-end track

Function description	The end of a dead-end track is a location at which a stop is always required. In ETCS, this stop is monitored like a stop at an end of movement authority and no special speed restriction is monitored. The function is covered by hazard [6.4.1-1].
Hazard [6.1.3.5-2]	**speed not reduced in time when entering dead-end tracks**
Annotation	The restriction of speed when entering dead-end tracks is a procedure-related restriction serving to reduce the extent of any damage in the event of contact. The respective function and the hazards derived there from are enumerated merely for the sake of completeness and are not considered in any greater detail hereafter. This function is covered by hazard [6.4.1-1].

Function [6.1.3.6]	max. permissible speed when entering partially occupied tracks
Function description	A stop is always required at the end of the approach to a partially occupied track. This stop is secured by means of a corresponding end of movement authority. In ETCS, this stop at an end of movement authority - but no special speed restriction - is monitored. The function is covered by hazard 6.4.1-1.
Hazard [6.1.3.6-1]	**max. permissible speed when entering partially occupied tracks is exceeded**
Annotation	The restriction of speed when entering a partially occupied track is a procedure-related restriction serving to reduce the extent of any damage in the event of a collision. The respective function and the hazards derived therefrom are enumerated merely for the sake of completeness and are not considered in any greater detail hereafter. This function is covered by hazard 6.4.1-1.

Function [6.1.3.6]	max. permissible speed when entering partially occupied tracks
Function description	A stop is always required at the end of the approach to a partially occupied track. This stop is secured by means of a corresponding end of movement authority. In ETCS, this stop at an end of movement authority - but no special speed restriction - is monitored. The function is covered by hazard 6.4.1-1.
Hazard [6.1.3.6-2]	**speed not reduced in time when entering partially occupied tracks**

Annotation	The restriction of speed when entering a partially occupied track is a procedure-related restriction serving to reduce the extent of any damage in the event of a collision. The respective function and the hazards derived therefrom are enumerated merely for the sake of completeness and are not considered in any greater detail hereafter. This function is covered by hazard 6.4.1-1.

Function [6.1.3.7]	max. permissible speed for reasons of safety of track works
Function description	ETCS monitors adherence to section-related speed restrictions (max. permissible speed as well as reductions in speed at the beginning of the respective section and increases in speed at the end thereof) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.3.7-0] / [6.1.3.7-1]	**permissible speed on grounds of track works is incorrectly shown / not enforced**
Limitations	This hazard is a collective representation of hazards, since their consequences are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.
Simplified consequence analysis	industrial accident
Examples for causes for the hazard	data input omitted (speed restriction not entered, incorrect value for permissible speed) data incorrectly entered (start or end of a restricted-speed section) position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (start or end of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	The speed restriction involved is always temporary.
System border check	Hazards Type A [6.1.3.7-0] Output Interface No. 2 [6.1.3.7-1] Output Interface No. 1

Function [6.1.3.7]	max. permissible speed for reasons of safety of track works
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard **[6.1.3.7-2]**	**max. permissible speed because of track works is incorrectly shown / not enforced**
Limitations	Reductions and increases in speed are considered separately.
Simplified consequence analysis	industrial accident
Examples for causes for the hazard	data input omitted (speed restriction not entered, incorrect value for permissible speed) position of movement incorrectly identified incorrect information transmitted from the ETCS central unit incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI monitoring function inactive intervention function inactive
Annotation	The speed restriction involved is always temporary. For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.1.3.7-0] / [6.1.3.7-1] and is no longer considered separately.

Function [6.1.3.7]	max. permissible speed for reasons of safety of track works
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of reductions in speed, it is additionally ensured by specifying appropriate control variables that these are executed at the beginning of the section.
Hazard **[6.1.3.7-3]**	**speed not reduced in time at speed restrictions on grounds of track works**

Limitations	Observance of the respective (section-related) max. permissible speed and increases in speed is considered separately.
Simplified consequence analysis	industrial accident
Examples for causes for the hazard	data incorrectly entered (start of a restricted-speed section) position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (start of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	The speed restriction involved is always temporary. For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.1.3.7-0] / [6.1.3.7-1] and is no longer considered separately.

Function [6.1.3.7]	max. permissible speed for reasons of safety of track works
Function description	ETCS monitors adherence to section-related speed restrictions (inclusive of the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly. In the case of increases in speed, it is additionally checked that these are not executed until the entire length of the train has cleared the section in question.
Hazard **[6.1.3.7-4]**	**speed increased too early at speed restrictions on grounds of track works**
Simplified consequence analysis	industrial accident
Limitations	Observance of the respective (section-related) max. permissible speed and reductions in speed is considered separately.

Examples for causes for the hazard	data incorrectly entered (end of a restricted-speed section) position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (end of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI monitoring function inactive intervention function inactive
Annotation	The speed restriction involved is always temporary. For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.1.3.7-0] / [6.1.3.7-1] and is no longer considered separately.

Function [6.1.3.8]	max. permissible speed in case of temporary speed restrictions
Function description	ETCS monitors adherence to temporary speed restrictions (including the relevant max. permissible speed) and prevents these being disregarded by intervening accordingly.
Hazard [6.1.3.8-0] / [6.1.3.8-1]	**max. permissible speed in case of temporary speed restriction incorrectly shown / not enforced**
Limitations	-
Simplified consequence analysis	damage to vehicle damage to railway facilities derailment

Examples for causes for the hazard	RBC displays to RBC operator, that temporary speed restriction has been applied successfully when in fact no temporary speed restriction had been applied to on-board data input omitted (speed restriction not entered, incorrect value for permissible speed) in respect of temporary speed restrictions data incorrectly entered (start or end of a restricted-speed section) in respect of temporary speed restrictions position of movement incorrectly identified incorrect information transmitted from the ETCS central unit (start or end of a restricted-speed section wrongly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI inadequate braking effect monitoring function inactive intervention function inactive
Annotation	No distinction is made between permanent and temporary speed restrictions, as this has no bearing on the relevant function/hazard. For the following processing steps, this hazard is grouped together with further hazards to form hazards [6.1-0] / [6.1-1] and is not considered separately.

Function [6.2.1]	lower pantograph(s) at required point
Function description	ETCS transmits the order to lower the pantograph before locations at which this is required.
Hazard [6.2.1-0]	**Lowering pantograph indication incorrectly shown** (FRS ref.: 4.8.1.5a)
Limitations	This hazard is a collective representation of hazards, since their consequences are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.
Simplified consequence analysis	damage to vehicle damage to overhead line equipment contact

Examples for causes for the hazard	project-planning error (section in which pantograph is to be lowered not projected, start or end of section wrongly projected) data input omitted (section in which pantograph is to be lowered is not entered or else the start or end of the section is incorrectly entered) in respect of a temporary requirement to lower the pantograph position of movement incorrectly identified information incorrectly transmitted from the ETCS central unit (start or end of section in which pantograph is to be lowered incorrectly transmitted) incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff
System border check	Hazard Type A (Output Interface No. 2)

Function [6.2.1]	lower pantograph(s) at required point
Function description	ETCS transmits the order to lower the pantograph before locations at which this is required.
Hazard [6.2.1-1]	**pantograph not lowered**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment contact
Examples for causes for the hazard	project-planning error (section in which pantograph is to be lowered not projected) data input omitted (section in which pantograph is to be lowered is not entered) in respect of a temporary requirement to lower the pantograph position of movement incorrectly identified order to lower pantograph not transmitted by the ETCS central unit incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (order not carried out)

Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.1-0] and is no longer considered separately.

Function [6.2.1]	lower pantograph(s) at required point
Function description	ETCS transmits the order to lower the pantograph before locations at which this is required.
Hazard **[6.2.1-2]**	**pantograph not lowered in time**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment contact
Examples for causes for the hazard	project-planning error (section in which pantograph is to be lowered not projected) data input omitted (section in which pantograph is to be lowered is not entered) in respect of a temporary requirement to lower the pantograph position of movement incorrectly identified order to lower pantograph not transmitted by the ETCS central unit incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (order not carried out)
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.1-0] and is no longer considered separately.

Function [6.2.1]	lower pantograph(s) at required point
Function description	ETCS transmits the order to raise the pantograph at the end of sections at the beginning of which the pantograph was to be lowered.
Hazard **[6.2.1-3]**	**pantograph raised too early**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment contact

Examples for causes for the hazard	project-planning error (end of section in which pantograph is to be lowered incorrectly projected) incorrect data input (end of section in which pantograph is to be lowered) in respect of a temporary requirement to lower the pantograph position of movement incorrectly identified information incorrectly transmitted from the ETCS central unit (end of section in which pantograph is to be lowered incorrectly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (pantograph raised without authorisation)
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.1-0] and is no longer considered separately.

Function [6.2.2]	switch off motive power unit current (main switch off) at required point
Function description	ETCS transmits the order to switch off the motive power unit before locations at which this is required.
Hazard [6.2.2-0]	**motive power unit not switched off at requisite location**
Limitations	This hazard is a collective representation of hazards, since their consequences are identical. Proceeding in this way makes the material more manageable and straightforward for further processing.
Simplified consequence analysis	damage to vehicle damage to overhead line equipment

Examples for causes for the hazard	project-planning error (section in which motive power unit is to be switched off not projected, start or end of section wrongly projected) data input omitted (section in which motive power unit is to be switched off not entered or else the start or end of the section is incorrectly entered) in respect of a temporary requirement to switch the motive power unit off position of movement incorrectly identified information incorrectly transmitted from the ETCS central unit (start or end of section in which motive power unit is to be switched off incorrectly transmitted) order to switch motive power unit on transmitted too early by the ETCS central unit incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (order not carried out)
Annotation	The wording »switch off motive power unit« generally means that the master switch on the motive power unit is to be switched off. Owing to the fact that Index 47 is focusing on personal injuries and that the consequences of this hazard being considered here only concern damage to property, it will no longer be considered hereafter.

Function [6.2.2]	switch off motive power unit current (main switch off) at required point
Function description	ETCS transmits the order to switch off the motive power unit before locations at which this is required.
Hazard **[6.2.2-1]**	**motive power unit not switched off**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment

Examples for causes for the hazard	project-planning error (section in which motive power unit is to be switched off not projected) data input omitted (section in which motive power unit is to be switched off not entered) in respect of a temporary requirement to switch the motive power unit off position of movement incorrectly identified order to switch motive power unit off not transmitted by the ETCS central unit incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (order not carried out)
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.2-0] and is no longer considered separately.

Function [6.2.2]	switch off motive power unit current (main switch off) at required point
Function description	ETCS transmits the order to switch off the motive power unit before locations at which this is required.
Hazard **[6.2.2-2]**	**motive power unit not switched off in time**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment

Examples for causes for the hazard	project-planning error (start of section in which motive power unit is to be switched off incorrectly projected) incorrect data input (start of section in which motive power unit is to be switched off) in respect of a temporary requirement to switch the motive power unit off position of movement incorrectly identified information incorrectly transmitted from the ETCS central unit (start of section in which motive power unit is to be switched off incorrectly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (order carried out too late)
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.2-0] and is no longer considered separately.

Function [6.2.2]	switch off motive power unit current (main switch off) at required point
Function description	ETCS transmits the order to switch off the motive power unit before locations at which this is required.
Hazard **[6.2.2-3]**	**motive power unit switched off too early**
Simplified consequence analysis	damage to vehicle damage to overhead line equipment

Examples for causes for the hazard	project-planning error (end of section in which motive power unit is to be switched off incorrectly projected) incorrect data input (end of section in which motive power unit is to be switched off) in respect of a temporary requirement to switch the motive power unit off position of movement incorrectly identified information incorrectly transmitted from the ETCS central unit (end of section in which motive power unit is to be switched off incorrectly transmitted) incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI error by staff (motive power unit switched back on without authorisation)
Annotation	For the following processing steps, this hazard is grouped together with further hazards to form hazard [6.2.2-0] and is no longer considered separately.

Function 6.2.8	avoid stopping at points not suitable for the adoption of auxiliary measures or only poorly so
Function description	This function serves to ease the rescue and to limit the extent of damage in case of an incident (avoid stopping in tunnels in case of fire). The command and control system is to display the appropriate sections.
Hazard [6.2.8]	**stopping at points where stopping is not permitted**
Simplified consequence analysis	Only in case of an incident: Increase of extent of damage
Examples for causes for the hazard	project-planning errors (speed restriction not provided for, incorrect value for permissible speed, start or end of restricted speed section wrongly projected) position of movement incorrectly identified incorrect information transmitted from the ETCS central unit incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit data incorrectly displayed on DMI
System border check	Hazard Type A (Output Interface No. 2)

Function 6.2.9	take account of restrictions in the use of specified brake designs
Function description	The command and control system is to display and monitor sections where the use of specified brake designs is not allowed.
Hazard [6.2.9]	**prohibition to use specified brake designs is not enforced**
Simplified consequence analysis	This hazard is a cause of further hazards (interferences at railway infrastructure, which are in turn causes for accidents/incidents)
Annotation	This function helps to avoid interferences at railway infrastructure (e.g. biasing train detection systems, heating of rails) triggered by the use of inappropriate brake designs. Failure modes of this function are causes of further hazards and are no longer considered separately.
System border check	Hazard Type B

Function [6.2.10]	Prove reliability of movement
Function description	This function compares the actual train characteristics with the actual infrastructure data of the route set for the train to establish that the train may operate over the line concerned. (FRS v4.29: 4.6.11)
Hazard [6.2.10-0] / [6.2.10-1]	**Information about unsuitability not advised to the driver / Enter a section of the route which is not permitted to**
Limitations	
Simplified consequence analysis	Contact Damage of railway vehicle Damage of catenary
Examples for causes for the hazard	project-planning data input omitted position of movement incorrectly identified information incorrectly transmitted from the ETCS central incorrect evaluation of order in the ETCS on-board unit wrong values prescribed by ETCS on-board unit error by staff
System border check	Hazards Type A [6.2.10-0] Output Interface No. 2 [6.2.10-1] Output Interface No. 1

Function [6.2.11]	Reversing in the event of danger
Function description	FRS 11.3.2 SRS 4.4.18 and 5.13
Hazard [6.2.11]	**Authorisation for reversing in the event of danger not given**
Limitations	The hazard arising from any unintentional movement by the vehicle is considered separately in fuction 4.7.2. The supervision in distance and speed when reversing in the event of danger is considered separately in function 6.1.3.4.
Simplified consequence analysis	Only in case of an incident: Increase of extent of damage
Examples for causes for the hazard	project-planning errors position of movement incorrectly identified incorrect information transmitted from the ETCS central unit incorrect evaluation of information in the ETCS on-board unit wrong values prescribed by ETCS on-board unit
System border check	Hazard Type A (Output Interface No. 1)

Function [6.4.1]	stopping at a signal at danger
Function description	ETCS monitors the execution of stops at locations before which it is necessary to stop on grounds of safety; by specifying appropriate control variables (having account to the braking properties of the vehicles involved), right-time stopping is already facilitated on the run-in to these locations.
Hazard [6.4.1-1]	**not stopping at the end of a movement authoritiy (without stopping beyond the end of movement authority)**
Limitations	No consideration is given to stops made on the basis of written or verbal orders.
Simplified consequence analysis	Collision collision with road traffic contact derailment

Examples for causes for the hazard	faulty project planning (position of possible stopping place) end of route release incorrectly transmitted by ETCS central unit end of route release not taken account of in ETCS on-board unit monitoring function inactive intervention function inactive error by staff (inadmissible auxiliary action to override the intervention function)
Annotation	Signal at danger is taken to mean all orders that, on grounds of safety (e.g. end of route, occupation by vehicles of the section in advance, non-negotiability of the section in advance), prescribe a stop for a movement at a specified location.
System border check	Hazard Type A (Output Interface No. 1)

Function [6.4.1]	stopping at a signal at danger
Function description	ETCS monitors the execution of stops at locations before which it is necessary to stop on grounds of safety; by specifying appropriate control variables (having account to the braking properties of the vehicles involved), right-time stopping is already facilitated on the run-in to these locations.
Hazard [6.4.1-2]	**not stopping at the end of a movement authoritiy (but stopping beyond the end of movement authority)**
Limitations	No consideration is given to stops made on the basis of written or verbal orders.
Simplified consequence analysis	where there is no or insufficient »overlap«: collision collision with road traffic contact derailment

Examples for causes for the hazard	end of route release incorrectly transmitted by ETCS central unit end of route release incorrectly evaluated in ETCS on-board unit braking curve incorrectly identified position of movement incorrectly identified monitoring function activated too late intervention function activated too late error by staff (brake operated too late) inadequate braking effect
Annotation	Signal at danger is taken to mean all orders that, on grounds of safety (e.g. end of route, occupation by vehicles of the section in advance, non-negotiability of the section in advance), prescribe a stop for a movement at a specified location.
System border check	Hazard Type A (Output Interface No. 1)

Function [6.4.1]	stopping at a signal at danger
Function description	ETCS monitors the execution of stops at locations before which it is necessary to stop on grounds of safety; by specifying appropriate control variables (having account to the braking properties of the vehicles involved), right-time stopping is already facilitated on the run-in to these locations. This also applies in the case of intermediate stops for other reasons (e.g. passengers boarding/ alighting).
Hazard [6.4.1-3]	**start moving without having a correct movement authority**
Limitations	No consideration is given to stops made on the basis of written or verbal orders.
Simplified consequence analysis	Collision collision with road traffic contact derailment
Examples for causes for the hazard	position of movement incorrectly identified monitoring function inactive intervention function inactive error by staff (inadmissible auxiliary action to override the intervention function)

Annotation	Signal at danger is taken to mean all orders that, on grounds of safety (e.g. end of route, occupation by vehicles of the section in advance, non-negotiability of the section in advance), prescribe a stop for a movement at a specified location.
System border check	Hazard Type A (Output Interface No. 1)

Function 6.4.2	stopping before stationary vehicles
Function description	If necessary the move is especially authorised to stop before stationary vehicles. This may come along with a shunting move or when a move is authorised by a written order.
Annotation	This function is not a CCS TSI function, but it is supported by supervising a maximum speed in the appropriate operation mode.
System border check	Hazard Type C

Function [6.4.3]	stopping at track closings
Function description	The stop required before track closings is a special form of signal at danger, as the location in question is already established prior to the movement being authorised and it is always necessary to stop there. The ETCS protection function corresponds to that activated to prevent signals being passed at danger. Hence the comments made in respect of hazard 6.4.1-1 apply by analogy.
Hazard **[6.4.3]**	**not stopping before track closings**
Simplified consequence analysis	Contact

Function [6.4.4]	stopping before other obstacles (than vehicles) on the track
Function description	If necessary the move is especially authorised to stop before other obstacles (than vehicles). This may come along with a shunting move or when a move is authorised by a written order.
Annotation	This function is not a CCS TSI function, but it is supported by supervising a maximum speed in the appropriate operation mode.
System border check	Hazard Type C

Function [6.6]	Check for safety-related deviations to railway installations on used route
Function description	It is to be ensured with the aid of suitable means of diagnosis/display that irregularities in the ETCS central unit and trackside equipment are detected where they have a bearing on safety.
Hazard [6.6]	**Irregularities in the ETCS central unit or in trackside equipment not detected**
Limitations	Maintenance and the irregularities to be detected within this framework are considered separately.
Simplified consequence analysis	movement authority inadmissibly generated incorrect information transmitted from the ETCS central unit position of movement incorrectly identified monitoring function inactive
System border check	Hazard Type B

Function [6.7.3]	detect irregularities in the vehicle's safety equipment
Function description	It is to be ensured with the aid of suitable means of diagnosis/display that irregularities in the ETCS on-board unit are detected where they have a bearing on safety.
Hazard [6.7.3]	**irregularities in on-board equipment with a bearing on safety not detected**
Limitations	Maintenance and the irregularities to be detected within this framework are considered separately.
Simplified consequence analysis	monitoring function inactive
System border check	Hazard Type B

Function [7.2.1]	applying brakes
Function description	When switching-off the ETCS on-board equipment, the air brake is automatically applied in order to avoid unintended movements.
Hazard [7.2.1]	**air brake not applied when vehicle parked**

Simplified consequence analysis	where the vehicle is properly secured: none otherwise: collision collision with road traffic contact derailment
Examples for causes for the hazard	error by staff (air brake not manually applied) function not actuated by ETCS on-board unit function not executed by brake system
System border check	Hazard Type A (Output Interface No. 1)

Function [8.2.3]	accident investigation
Function description	This function is partly carried out by the emergency management, the CCS TSI functionality considered here solely is the juridical recording.
Annotation	The emergency management (comprising accident investigation and juridical recording) is not part of the train run. A hazard cannot be derived from this function. Therefore no further consideration is necessary.

Function [8.3]	Ensure safe condition of railway infrastructure
Function description	Proper maintenance of railway infrastructure helps guarantee its safe condition. This also applies with regard to those ETCS components that form part of the railway infrastructure.
Hazard [8.3]	**improper maintenance of ETCS central unit and trackside equipment**
Annotation	Given that maintenance is an on-going process, it is cited separately - in juxtaposition to project planning. However, in view of the fact that it is not possible to effect a quantitative appraisal of maintenance as part of any risk/hazard analysis exercise and hence that neither can values for reliability be prescribed, maintenance will not be considered in greater detail hereafter but is, rather, merely enumerated for the sake of completeness.

Function [8.4]	Ensure safe condition of vehicles
Function description	Proper maintenance of vehicles and their components (inclusive of protection equipment) helps guarantee their safe condition. This also applies with regard to the ETCS on-board unit.
Hazard **[8.4]**	**improper maintenance of ETCS on-board unit**
Annotation	Given that maintenance is an on-going process, it is cited separately - in juxtaposition to project planning. However, in view of the fact that it is not possible to effect a quantitative appraisal of maintenance as part of any risk/hazard analysis exercise and hence that neither can values for reliability be prescribed, maintenance will not be considered in greater detail hereafter but is, rather, merely enumerated for the sake ofcompleteness.

Function [8.5]	Formation, Training and Qualification
Function description	This function serves to ensure a safe operation of the railway.
Annotation	Formation, Training and Qualification are not part of the train run. A direct hazard cannot be derived from this function. Failure modes of this function are causes for further hazards.

5.4 Log of System hazards

No.	Ref.	System hazard	Output Interface No
1	[4.7.2-2]	unauthorised setting back	1
2	[4.8.2]	passing the defined border of the shunting area (balise 'stop if in shunting')	1
3	[5.1-2]	move inadmissibly authorised	2
4	[5.1-3]	permission to proceed not withdrawn in time in the event of danger	2

5	[6.1-0]	permissible speed as a function of route characteristics incorrectly shown	2
6	[6.1-1]	permissible speed as a function of route characteristics not enforced	1
7	[6.1.1.3-0]	permissible speed when passing level crossings incorrectly shown	2
8	[6.1.1.3-1]	permissible speed when passing level crossings not enforced	1
9	[6.1.1.8-0]	permissible speed on account of the design of the overhead line incorrectly shown	2
10	[6.1.1.8-1]	permissible speed on account of the design of the overhead line not enforced	1
11	[6.1.2.1-0]	permissible speed of train due to running properties of vehicles incorrectly shown	2
12	[6.1.2.1-1]	permissible speed of train due to running properties of vehicles not enforced	1
13	[6.1.3.1-0]	permissible speed when running on sight incorrectly shown	2
14	[6.1.3.1-1]	permissible speed when running on sight not enforced	1
15	[6.1.3.2-0]	permissible shunting speed incorrectly shown	2
16	[6.1.3.2-1]	permissible shunting speed not enforced	1
17	[6.1.3.4-0]	permissible speed when reversing in the event of danger incorrectly shown	2
18	[6.1.3.4-1]	permissible speed when reversing in the event of danger not enforced	1
19	[6.1.3.7-0]	permissible speed on grounds of track works incorrectly shown	2
20	[6.1.3.7-1]	max. permissible speed on grounds of track works not enforced	1
21	[6.2.1-0]	lowering pantograph indication incorrectly shown	2
22	[6.2.8]	stopping at points where stopping is not permitted	2
23	[6.2.10-0]	Information about route unsuitability not advised to the driver	2
24	[6.2.10-1]	enter a section of the route which is not permitted to (due to route suitability)	1
25	[6.2.11]	Authorisation for reversing in the event of danger not given	

26	[6.4.1-1]	not stopping at the end of a movement authoritiy (without stopping beyond the end of movement authority)	1
27	[6.4.1-2]	not stopping at the end of a movement authoritiy (but stopping beyond the end of movement authority)	1
28	[6.4.1-3]	start moving without having a correct movement authority	1
29	[7.2.1]	air brake not applied when vehicle parked	1

5.5 Consistency check of input/output interfaces to/from CCS TSI

5.5.1.1 The whole process of hazard identification was accompanied by a systematic check of the input/output interfaces to/from CCS TSI in order to ensure completeness. The log of hazards in 5.3 as well as the final hazard log “Log of System hazards” in 5.4 comprise the results of this check, thus a separate listing is not necessary.

6 Control-Command and Signalling Safety Requirements

6.1 General

This chapter contains so far examples of national safety requirements. Some work is still to be done in order to enable harmonisation of THRs and SILs imposed on the System Hazards, constituting the harmonised safety requirements for CCS for interoperability: First the comparison of national examples for safety requirements has to be triggered. Therefore the member states are asked to contribute to chapter 6 of the document by deriving - on basis of Index 47 - national values for THRs (In order to achieve a high level of comparability, assumptions about Level of tolerable Risk, Criticality, Fatality and the apportionment of the tolerable Risk to the System Hazards should be included). Secondly the Causal Analysis has to be carried out and linked to the 'Log of System Hazards' of chapter 5.4 to ensure as well, that additional System Hazards arising from system design will be discovered.

After finishing these 'next steps' this chapter will contain the harmonised mandatory CCS safety requirements.

6.2 DB example for quantitative safety requirements

6.2.1 Introduction

6.2.1.1 This summary describes the general approach and the results of the risk analysis for the ETCS pilot line of DB.

6.2.2 Preconditions

6.2.2.1 The considered hazards correspond to the Index 47 log of system hazards. Due to their close affinity, hazards no. 5&6, 9&10, 11&12, 13&14 and 19&20 are not considered separately. Because the operational condition of the test –track requires not all ETCS function defined in the CCS TSI annex A, the quantitative Safety Requirements presented here are restricted to that functionality and for this reason the TIRF distributed among its System Hazards is reduced to 70%. In general, two different fatalities (one at 40km/h, one at 200km/h) were applied to derive THRs from the TIRF resulting in two different THRs per hazard. (The intention was to meet the safety target also in degraded modes. In degraded modes the effect of a lower supervised max speed was taken into account by a lower fatality.)

6.2.3 Results of the Risk Analysis

6.2.3.1 The TIRF and the fatalities used in the risk analysis were defined on the basis of assessed statistic investigations. Based on the TIRF, assuming a criticality of 1 and the above mentioned fatality, the THR’s for the different hazards were calculated (see chapter 6.2.4).

6.2.3.2 The TIRF (chapter 6.2.4) and the THR´s shown in chapter 6.2.5 is the basis for the safety case.

6.2.4 Relation of TIRF to THRs

6.2.4.1 TIRFETCS = 0,23 · 10-9 O/(R·h)

6.2.4.2 70% of the TIRFETCS is used for the restricted functionality of the pilot line. 10% of the tolerable risk is used to derive the quantitative safety requirements (only for random failures including handling errors).

6.2.4.3 $$TIRF_{ETCSpilotLine,randomFailures} = 0{,}1 \cdot 0{,}7 \cdot TIRF_{ETCS} = 1{,}61 \cdot 10^{-11} \frac{victims}{passenger \cdot hour}$$

6.2.4.4 This is in a first approach equally distributed among the pilot line's 13 ETCS System Hazards:

6.2.4.5 $$TIRF_{ETCSpilotLine,randomFailures,perHazard} = \frac{0{,}1 \cdot 0{,}7 \cdot TIRF_{ETCS}}{13}$$

6.2.4.6 $$TIRF_{ETCSpilotLine,randomFailures,perHazard} = 1{,}24 \cdot 10^{-12} \frac{victims}{passenger \cdot hour}$$

6.2.4.7 $$THR_{SystemHazard} = \frac{TIRF_{ETCSpilotLine,randomFailures,perHazard}}{F_k \cdot C_k}$$

Assuming a general criticality C=1:

6.2.4.8 $$THR_{SystemHazard} = \frac{TIRF_{ETCSpilotLine,randomFailures,perHazard}}{F_k}$$

As F, the fatality of the most fatal accident which may occur as consequence of a hazard is taken into consideration.

6.2.5 Values

1	2	3	4	5	6
No	System hazard	average fatality at v=40km/h [victims / (passenger x accident)]	average fatality at v=200km/h [victims / (passenger x accident)]	THR (hazards/hour)	
				v=40km/h	v=200km/h
1	unauthorised setting back	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
2	passing the defined border of the shunting area (balise 'stop if in shunting')				
3	move inadmissibly authorised	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
4	permission to proceed not withdrawn in time in the event of danger	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
5	permissible speed as a function of route characteristics incorrectly shown	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
6	permissible speed as a function of route characteristics not enforced				
7	permissible speed when passing level crossings incorrectly shown				
8	permissible speed when passing level crossings not enforced				
9	permissible speed on account of the design of the overhead line incorrectly shown	$2{,}6 \cdot 10^{-5}$	$6{,}4 \cdot 10^{-4}$	$5 \cdot 10^{-8}$	$1{,}93 \cdot 10^{-9}$
10	permissible speed on account of the design of the overhead line not enforced				
11	permissible speed of train due to running properties of vehicles incorrectly shown	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
12	permissible speed of train due to running properties of vehicles not enforced				
13	permissible speed when running on sight incorrectly shown	$8{,}3 \cdot 10^{-4}$	--	$1{,}5 \cdot 10^{-9}$	-
14	permissible speed when running on sight not enforced				
15	permissible shunting speed incorrectly shown				
16	permissible shunting speed not enforced				
17	permissible speed when reversing incorrectly shown				

18	permissible speed when reversing in the event of danger not enforced				
19	permissible speed on grounds of track works incorrectly shown	$0{,}77$	$0{,}77$	$1{,}61 \cdot 10^{-12}$	$1{,}61 \cdot 10^{-12}$
20	max. permissible speed on grounds of track works not enforced				
21	lowering pantograph indication incorrectly shown	$2{,}6 \cdot 10^{-5}$	$6{,}4 \cdot 10^{-4}$	$5 \cdot 10^{-8}$	$1{,}93 \cdot 10^{-9}$
22	stopping at points where stopping is not permitted				
23	Information about route unsuitability not advised to the driver				
24	enter a section of the route which is not permitted to (due to route suitability)				
25	authorisation for reversing in the event of danger not given				
26	not stopping at the end of a movement authoritiy (without stopping beyond the end of movement authority)	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
27	not stopping at the end of a movement authoritiy (but stopping beyond the end of movement authority)	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
28	start moving without having a correct movement authority	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$
29	air brake not applied when vehicle parked	$4 \cdot 10^{-4}$	$1 \cdot 10^{-2}$	$3{,}1 \cdot 10^{-9}$	$1{,}24 \cdot 10^{-10}$

6.2.6 Experience on working with the Risk Analyses (RA)

6.2.6.1 Even if the safety analysis is not finalised, it seems, that the safety target from the RA could be met at least for the condition of the ETCS pilot line of DB.

6.2.6.2 The defined hazards are on a high functional level, thus it can be assumed, that the risk analysis will be stable even if technical functionality or operational regulations will be adapted / modified in future.

6.2.6.3 The mapping of the safety requirements to the industrial product has required a deep co-operation between the railway and the supplier. In future the effort could be minimised by providing a description of the operational assumptions (incl. human factor) to the supplier.

6.2.6.4 One issue of a risk analysis is to derive a safety target in form of an acceptable risk (TIRF). The allocation to different hazards and the transformation to hazard rates is another important step in order to join the risk analysis and the hazard analysis of the supplier. The TIRF is the fundamental value which has to be fulfilled, whereas the distribution of the TIRF to the THRs may alter due to the applied system design and the appropriate Causal Analysis. The experience during the process of adapting the suppliers' Causal Analysis to the risk analysis showed that the safety requirements can

be reduced by a factor up to 10 taking into account:

- That the hazards from the RA do not reflect, that only a few causes have a major influence on several hazards (they should not be considered repeatedly).
- The analysis of the causes on the basis of the railway specific operational conditions can reduce the requirements in addition as well as
- the analysis of the criticality for different hazards.

6.2.6.5 As expected the influence of the operational handling is the most important one. Further investigation has to consider processes of the train data entry (especially the max. speed of the train and the train length) and the entry of temporary speed restrictions on track-side.

6.3 UK example for quantitative safety requirements

No.	Ref.	System hazard	UK Safety Req	UK Rationale
1	[4.7.2-2]	unauthorised setting back	10^{-9}/hr	Amend wording to 'Unauthorised movement reverse direction'.
2	[4.8.2]	passing the defined border of the shunting area (balise 'stop if in shunting')	10^{-5}/hr	Same Rationale as 23, 24, 25. Ensure that shunting is not authorised without a Balise List being issued without operational controls being in place. A 'shunting overlap' is required to protect against propelling moves and/or the stopping distance after the emergency brake has been triggered. Reliant on reading a single balise/balise group. Operational rules and layout of the track currently provide the main protection and this situation is assumed to continue and thus a low safety requirement is used.
3	[5.1-2]	move inadmissibly authorised	10^{-9}/hr	Core functionality of train control system. Maximum level of safety realistically attainable. Taken to include safety of trackworkers in a protected area.
4	[5.1-3]	permission to proceed not withdrawn in time in the event of danger	10^{-4}/hr	Delete 'in time in the event of danger'. Due to quality of service, it is important that the UK does not rely on ETCS alone for removal of movement authorities and continues to use voice communication as well. Within this hazard the reliability of the datalink is included. Control of hazard is dominated by the ability to discover the hazardous circumstances in practice. There would be very significant GSM-R cost implications should this requirement be made more demanding.

5	[6.1-0]	Permissible speed as a function of route characteristics not shown to the driver	10^{-4}/hr	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard. Considered only as permanent static speed profile. Temporary and emergency speed restrictions considered at 30xxx.
6	[6.1-1]	Permissible speed as a function of route characteristics not enforced	10^{-7}/hr speeds up to & including 25% over speed; 10^{-9}/hr speeds in excess of 25% over speed;	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Assumes that there are sufficient definitions of train types to cater for hazards such as train/OHLE compatibility.
7	[6.1.1.3-0]	max. permissible speed when passing level crossings is not shown to the driver	10^{-4}/hr	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard.

8	[6.1.1.3-1]	max. permissible speed when passing level crossings is not enforced	10^{-7}/hr speeds up to & including 25% over speed; 10^{-9}/hr speeds in excess of 25% over speed;	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Consequences for level crossing may be different but not considered to be a material affect based on preliminary assessment.
9	[6.1.1.8-0]	max. permissible speed on account of the design of the overhead line is not shown to the driver	NA	Not required by UK, fully covered by items 5 & 6.
10	[6.1.1.8-1]	max. permissible speed on account of the design of the overhead line is not enforced	NA	Not required by UK, fully covered by items 5 & 6.
11	[6.1.2.1-0]	max. permissible speed of train due to running properties of vehicles is not shown to the driver	10^{-4}/hr	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the display system is only marginally safety related. Hazard associated by enforcement is covered in the next hazard.
12	[6.1.2.1-1]	max. permissible speed of train due to running properties of vehicles is not enforced	10^{-7}/hr speeds up to & including 10% overspeed; 10^{-9}/hr speeds in excess of 10% overspeed;	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge. Note: Relies on data entry.
13	[6.1.3.1-0]	max. permissible speed when running on sight is not shown to the driver	NA	Given that this speed is only optionally displayed, it cannot have a safety requirement.

14	[6.1.3.1-1]	max. permissible speed when running on sight is not enforced	10^{-7}/hr speeds up to & including 25% overspeed; 10^{-9}/hr speeds in excess of 25% overspeed;	UK philosophy is that safety is in the enforcement system rather than the driver/displayed information and hence the enforcement system provides the safety. It is considered that there is an element of mitigation in the driver not speeding excessively due to his route knowledge.
15	[6.1.3.2-0]	permissible shunting speed is not shown to the driver	NA	Given that this speed is only optionally displayed, it cannot have a safety requirement.
16	[6.1.3.2-1]	permissible shunting speed is not enforced	10^{-4}/hr	To be controlled by operational process in the UK. Low value required. Risks considered generally to be mitigated by low speed of operation. Speed enforcement functions are likely to be dominated by the most demanding speed enforcement requirement.
17	[6.1.3.4-0]	permissible speed when reversing is not shown to the driver	NA	Given that this speed is only optionally displayed, it cannot have a safety requirement.
18	[6.1.3.4-1]	permissible speed when reversing in the event of danger not enforced	NA	To be controlled by operational process in the UK. Not intending to use this functionality in the UK.
19	[6.1.3.7-0]	max. permissible speed on grounds of track works is not shown to the driver	NA	Hazard relates to protection of trackworkers only.
20	[6.1.3.7-1]	max. permissible speed on grounds of track works is not enforced	10^{-7}/hr	Hazard relates to protection of trackworkers only. Scenarios considered – reducing linespeed on the line where the workers are working to enable red zone arrangements to be established and reducing linespeed on open lines adjacent to workers.
21	[6.2.1-0]	lowering pantograph information is not shown to driver	NA	Controlled by Operational process in UK.
22	[6.2.8]	stopping at points where stopping is not permitted	10^{-4}/hr	Primarily controlled by operational process in UK.

23	[6.2.10-0]	Information about unsuitability not advised to the driver	10^{-4}/hr	In the UK this hazard is adequately controlled through existing operational procedures. The UK will reinforce this operational control of this hazard even when ETCS is implemented. Therefore a SIL0 target has been assigned.
24	[6.2.10-1]	enter a section of the route which is not permitted to	10^{-4}/hr	In the UK this hazard is adequately controlled through existing operational procedures. The UK will reinforce this operational control of this hazard even when ETCS is implemented. Therefore a SIL0 target has been assigned.
25	[6.2.11]	Authorisation for reversing in the event of danger not given		
26	[6.4.1-1]	signal passed at danger (without train stopping afterwards)	10^{-9}/hr	Change 'Signal' to 'Danger Point' Highest integrity realistically achieved. Workshop assumption is that this relates to errors in definition to where the train should stop. No braking - Justification Report to be clarified.
27	[6.4.1-2]	not stopping at a signal at danger in time	10^{-9}/hr	Change 'Signal' to 'Danger Point' Highest integrity realistically achieved. Since the System Definition includes the Driver entering the data, this value is only achievable if the system protects against data entry errors. Insufficient braking – Justification Report to be clarified.
28	[6.4.1-3]	starting move towards a signal at danger	10^{-9}/hr	Add 'and proceeding past Danger Point'. Highest integrity realistically achieved. Since the System Definition includes the Driver entering the data, this value is only achievable if the system protects against data entry errors. Justification Report to be clarified.
29	[7.2.1]	air brake not applied when vehicle stabled	10^{-4}/hr	Replace description with 'Brake not commanded when vehicle parked'. Low value since safety resides elsewhere ie in the braking system.
30	new	Voice radio unavailable to warn Driver of dangerous situation	EIRENE availability value	Add Safety requirement based on EIRENE availability – principally to drive similar availability requirements into supporting infrastructure eg power supplies and application of EIRENE to trains and infrastructure.

31	new	Train detection failure due to EMC Train to Trackside & Static Parameters not complied with	10-7/hr	Probability of not complying with the static parameters and Gabarit in Annex A Appendix 1 thus causing the train detection to fail wrongside. See attachment providing justification.
32		Giving authority to the rear train where two trains are within section	10^{-9}/hr	Where train is on same train detection, eg a split train, and the rear train is given the movement authority. Could arise through a variety of circumstances eg train splitting, train assisting faulty train and train SPADing into section. May require more than one THR for different circumstances.
33		Temporary speed restriction not enforced	10^{-7}/hr speeds up to & including 10% overspeed; 10^{-9}/hr speeds in excess of 10% overspeed;	Application/Data preparation likely to be the key issue. The safety feature will therefore be driven by the procedures. Includes emergency speed restrictions. Need to consider further the tolerance rating stated with Civil/Wagon Engineer.

7 References

Ref #	Document
1	Safety Requirements and Requirements to Safety Analysis for Interoperability for the Control-Command and Signalling Sub-System.
2	Directive 96/48/EC of 23 July 1996 on the interoperability of the trans-European high-speed rail system
3	Directive 2001/16/EC of 19 March 2001 on the interoperability of the trans-European conventional rail system
4	Commission Decision of 30 May 2002 concerning the technical specification for interoperability relating to the control-command and signalling subsystem of the trans-European high-speed rail system referred to in Article 6(1) of Council Directive 96/48/EC (notified under document number C(2002) 1947)
5	CCS TSI CR: 2001/16/EC - 01/16-ST01 part 2 Version EN 07 24.11.2004
6	Index 27/UNISIG Subset 91 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2
7	All Class 1 specifications for ETCS as defined in Annex A of the Control-Command and Signalling Technical Specification for Interoperability
8	Functional Analysis Of Trans – European Rail Operation Reference EEIG:01 E 129 version 2 dated 08.07.04.
9	ETCS and GSM-R Change Control Process
10	All Class 1 specifications for GSM-R as defined in Annex A of the Control-Command and Signalling Technical Specification for Interoperability
11	Index 47 Remit V1EEIG : 03E415
12	EEIG Operational Rules Writing Group: Crosscheck of functions
13	ERTMS Operational Rules Writing Group: Fragile Points
14	Reason, J. T. (1990) Human Error. Cambridge: Cambridge University Press
15	EN 50126:1999 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
16	EN 50129:2003 Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
17	Commission Decision of 29 April 2004 modifying Annex A to Decision 2002/731/EC of 30 May 2002 and establishing the main characteristics of Class A system (ERTMS) of the control - command and signalling subsystem of the trans- European conventional rail system referred to in Directive 2001/16/EC of the European Parliament and of the Council (notified under document number C(2004) 1559) (2004/447/EC)

8 Recommendation for next steps.

8.1.1 Comparison of national examples for safety requirements

According to the safety concept applied (see drawing 2.2.1.2) and aiming for harmonised 'mandatory safety requirements' on THR level, the member states are asked to contribute to chapter 6 of the document by deriving - on basis of Index 47 - national values for THR's. (To achieve a high level of comparability, assumptions about Level of tolerable Risk, Criticality, Fatality and the apportionment of the tolerable Risk to the System Hazards should be included).

8.1.2 Link between Causal Analysis and Index 47

In order to fulfil the safety concept according to drawing 2.2.1.2 to ensure that further System Hazards arising from system design will be discovered, the linking of the Causal Analysis to the 'mandatory safety requirements' Index 47 has to be done with help of the appropriate experts, especially for human factor and technical aspects (e.g. UNISIG, human factor group).

Since systematic failures play a major role - considering total risk - we recommend to analyse/evaluate the effectiveness of the normative measures against systematic failures in detail.

8.1.3 Mandatory safety requirements

The comparison of national examples for safety requirements (8.1.1) and the Causal Analysis (8.1.2) have to be carried out in order to enable harmonisation of THR's and SIL's for System Hazards, constituting the harmonised safety requirements for CCS for interoperability.

8.1.4 Consolidation of Index 47 by application in practice

Apply Index 47 on projects for example the "POS project".

8.1.5 Apportionment of safety requirements to On-board and Track-side

In addition to Interoperability also the commercial benefits when purchasing, the safety requirements ought to be apportioned between On-board and Track-side at Causal Analysis level.

8.1.6 Apportionment of safety requirements to constituents

For the sake of commercial benefits when purchasing, the safety requirements ought to be apportioned to the single constituents.

9 Open Points List.

#	Description	Solution/ Workstream	Status/Notes
1	System Definition	Index 47	**Closed.** Index 47 completing drafting. ISA review and acceptance outstanding. ISA comments received and discussed in meeting. ISA acceptance expected by September.
2	Agreed CCS Hazard list	Index 47	**Closed.** Index 47 completing drafting. ISA review and acceptance outstanding. ISA acceptance expected by October.
3	ETCS On-Board Equipment *(Safety Requirements for the constituent products/* *Product safety case)*	Subset 91/ Index 27	**Closed.** Drafted by UNISIG Reviewed by ISA some compatibility issues with Operational rules. Approval by CCSG outstanding.
4	GSM-R On-Board Equipment *(Safety/ availability* *Requirements for the constituent products/* *Product safety case)*	GSM-R Class 1 Specs/EEIG	**GSM-R Functional Group Actioned.** Functionality requirements specified in Class 1 specification, Signal strength requirements specified, but RAM requirements for voice need to be addressed. Preliminary GSM-R voice RAM requirements are included in draft Index 47 and these may later transfer into the Class 1 Specs. Discussed with Klaus Konrad and agreement has been reached that Index 48 will include the GSM-R RAM and Testing requirements.
5	The application of ETCS to trains (Application *Safety Requirements/*	Index 47	**Open.** Topic is in the scope of the

	application safety case)		Causal Analysis
6	The application of GSM-R to trains (Application *Safety Requirements/* application safety case)	Index 47	**Open**. is in the scope of the Causal Analysis
7	EMC	AEIF CoCoSig EMC Subgroup/ CENELEC A4-2	**TSI EMC Group (L Lochman) Actioned.** Simple parameters drafted. EMC work outstanding. The tolerable hazard rate must be defined. [Expectations to the work of the Annex A Appendix 1 group to be defined. Discussed with Tom Lee, confirmation from Libor Lochman required.]
8	ETCS Trackside equipment (*Safety/ availability* *Requirements for the constituent products/* *Product safety case)*	Subset 91	**Closed.** Drafted by UNISIG Reviewed by ISA some compatibility issues with Operational rules. Approval by CCSG outstanding.
9	GSM-R Trackside equipment (*Safety/ availability* *Requirements for the constituent products/* *Product safety case)*	GSM-R Class 1 Specs	**GSM-R Functional Group Actioned.** Functionality requirements specified in Class 1 specification, Signal strength requirements specified, but RAM requirements for voice need to be addressed. Preliminary GSM-R voice RAM requirements are included in draft Index 47 and these may later transfer into the Class 1 Specs. Discussed with Klaus Konrad and agreement has been reached that Index 48 will include the GSM-R RAM and Testing requirements.
10	The application of ETCS to infrastructure (Application *Safety Requirements/* application safety case)	Index 47	**Open**. Topic is in the scope of the Causal Analysis
11	The application of GSM-R to infrastructure (Application *Safety Requirements/* application safety case)	Index 47	**Open**. Topic is in the scope of the Causal Analysis
12	Operation of the CCS assemblies	EEIG Rules work	**Actioned.** Drafted by EEIG

			Reviewed by ISA Some rules validated, some open points outstanding.
13	Safety requirements confirmed as complete and consistent	Index 47 subgroup	**Actioned.** Justification report being drafted. ISA review and acceptance of Index 47 & Justification report outstanding.
14	4.2Operational Assumptions. (Section 10.4 of Subset 091 refers). 4.2.1 External Entities A global assumption has been that information supplied to ETCS from outside of the ETCS domain such as interlocking is correct. (Section 4.2 of Thus the event is defined as 'Incorrect data from external entities' Failure to supply correct information to ETCS may result in a train exceeding its safe speed and distance envelope. The event is therefore hazardous.		**Closed.** In the event that the hazard is as a result of a failure at the trackside, the hazard could result in a failure to meet the national service objectives but it would not affect international operation. Control of such hazards is therefore assumed to be a national issue. Errors onboard from could however lead to hazards that have international repercussions. Concerning the 'External Entities', 'Failure to supply correct information to ETCS' is not a hazard but a cause for hazards in the system environment (see 4.2.4.12 Model of the system structure) , e.g. Hazard No. 6 ' Permissible speed/ speed restriction caused by track characteristics not met ' or Hazard No. 16 'Passing a stop sign (braking not in time)'. Therefore this matter is not dealt with in index 47 (see chapter 2 'Scope'). Failure within the interlocking is not in the scope of index 47, but failure of transmission of the interlocking-information (appropriate interface) is in the scope of index 47.
15	4.2 Operational Assumptions. (Section 10.4 of Subset 091 refers).		**Actioned.** The following events were

	4.2.2 Driver Error The event considered is that of Driver Error resulting from operations where ETCS does not provide protection.		considered by Unisig • Transition from unfitted areas to areas fitted for Level I or Level 2 operation. • Operation in Level 1 without lineside signals A rule has been derived in subset 088 part 3 Annex A at section 6.4.2 to manage the entry into an ETCS area from an unfitted area. This rule (which requires assessment) denoted as rule A is, Although not part of the SRS requirements, it is assumed that entry of a train into a level 1 or level 2 equipped area will be controlled by a line side entry signal. It is further assumed that, when needed (e.g., in the case of ETCS areas without optical signals), this signal or other means not part of ETCS, will be used to prevent unauthorised trains (or trains with a failed onboard system) from entering the area. Related to this rule, the assumption made in the balise calculations is that the driver of a train will, on average, fail to verify that the level transition from unfitted to level 1 / 2 has been made once time in every 1000 entry procedures. Therefore he will continue the journey in the wrong mode. A second rule has been derived regarding the operation of trains in Staff Responsible mode in a Level 1 area without lineside signals. This rule (which requires assessment) denoted as rule B is, It is assumed that in level 1 applications without line side

			signals that there is some external marker to indicate stopping points. Clearly such a marker will not display any aspect information. Therefore it is assumed that the driver will be authorised by operational procedures outside the scope of this document. Related to this rule, the assumption made in the balise calculations is that the driver of a train will, on average, exceed his authorisation 1 time in every 1000 SR procedures when operating in level 1 without line side signals. Embedded in the consideration of Driver Error is the issue Driver Training and qualification, its content and frequency. The requirements on driver training need proper definition. Associated with driver error is the need to consider the effect of failure of a driver to respond to ETCS commands such as Lowering Pantograph and Managing Route Unsuitability. {To be addressed by the Human Factors Group}
16	4.3 Transmission System Reliance is placed on cryptographic techniques to minimise the possibility of a security hazard resulting from the Masquerading of a message over the radio link		**Closed.** Unisig have made the assumption that the confidentiality of the keys would be such as not to undermine the effectiveness of the code. Clear guidance is required on how to assess the process to ensure compatibility with overall safety targets. Using a key for the transmission system fulfils the overall safety targets.
17	5.UNISIG Derived Requirements.		**Actioned.**

	5.1 Accuracy of Data Presented to ETCS. 5.1.2 Data Entry.(Section 12.6.4. of Subset 088 Part 3 refers). Unisig have identified that the event of entering of incorrect data can in some instances, lead to a train exceeding its safe speed and distance envelope. The event is therefore considered to be hazardous as it could affect service objectives both nationally and internationally.		Unisig have indicated that complete process from establishing the data, releasing the data to the correct driver I train and its subsequent entry into ETCS must be commensurate with a SIL 4 system. Responsibility for controlling the hazard is national issue. However, proof of hazard control must be done in way such that satisfy other networks intending to accept that train. This does not mean that the complete procedure has to be harmonised across Europe but Cross Acceptance must be achieved. Consideration will need to be given to the number of times that a driver will need to enter data as part of a journey. This may result in the need for a harmonised means of presenting data to the driver It is noted that CENELEC does not provide guidance on the control of systematic errors within procedural processes that need satisfy specific Safety Integrity Levels and therefore guidance to the European railways should be provided by the EEIG.
18	5.UNISIG Derived Requirements. 5.1 Accuracy of Data Presented to ETCS. 5.1.3 Data Preparation. (Section 12.6.2. of Subset 088 Part 3 refers). The whole process of dimensioning a line (e.g. curvature, cant, gradient etc.) and the subsequent process of data preparation to achieve network performance objectives has the potential to undermine the safety integrity invested		**Actioned.** Based on the considerations, Unisig have mandated that the data preparation process should be of a quality commensurate with a Safety Integrity Level (SIL) 4 system. It is noted that CENELEC does not provide guidance on the control of systematic errors

	in the ETCS equipment.		within procedural processes that need satisfy specific Safety Integrity Levels and therefore guidance to the European railways should be provided by the EEIG. Thus, the process of trackside data preparation is deemed to be potentially hazardous although just within a national domain. The hazard is deemed to need controlling at the project level. Incorrect onboard data such as deceleration rates will however have international consequences and such hazards need controlling at an international level. Concerning 'Data Preparation' practical experiences tought us that applying Safety Integrity Levels does not lead to the desired result of quality. For static data an application of a SIL is applicable, im terms of dynamic data (train length, deceleration data, maximum permitted speed for the train [taking into account the maximum speed of every vehicle contained in the train]) it should be proceeded as done with the 'human factor' and therefore is to be adressed to the 'human factor group'.
19	5.1 Acuracy of Data Presented to ETCS. 5.1.4 System Deployment. (Section 12.6.3. of Subset 088 Part 3 refers). The siting of infrastructure such as balises and ensuring that these items contain the correct data is yet another area that has the potential to undermine national safety objectives.		**Actioned.** Based on the considerations, Unisig have mandated that the system deployment process should be of a quality commensurate with a Safety Integrity Level (SIL) 4 system. It is noted that CENELEC does not provide guidance on the

			control of systematic errors within procedural processes that need satisfy specific Safety Integrity Levels and therefore guidance to the European railways should be provided by the EEIG. The process of system deployment is therefore deemed to be potentially hazardous although just within a national domain. Thus, the hazard is deemed to need controlling at the project level. Considering the 'model of the system structure' (4.2.4.12) the function of 'Data entry' has to be allocated within the system. Therefore it is not dealt with in the risk analysis. 'Data entry' in terms of 'System Deployment' is a topic which has to be addressed to the 'human factor group' to be quantified.
20	5.UNISIG Derived Requirements. Emergency Messages. (Section 9.3.4. of Subset 088 Part 3 refers). Emergency messages are transmitted by a high priority channel independent of the normal data and voice channels. Therefore it will be a National issue to assess the effect of problems due to insertion, delay, deletion and corruption.		**Actioned.** It may be necessary to provide harmonised targets. The use of the Emergency Message service should not detract from the safety of the technical system. This topic is covered by the work untertaken by the Operational Rules Writing Group.
21	5.UNISIG Derived Requirements. 5.3 Signalling Principles. The design of ETCS utilises the principle wherever possible that the undetected deletion of information does not lead to a less restrictive situation.		**Actioned.** It is necessary that national additions and national functions maintain adherence to this rule.

22	5.UNISIG Derived Requirements. 5.4 Operational Modes. The primary mode of operation should be Full Supervision as this affords the maximum protection against Driver Error and MMI failures. Modes other than Full Supervision where the driver assumes an increased level of responsibility must have the responsibility clearly defined.		**Open**. Topic is in the scope of the Causal Analysis.
23	6. ISA CONCERNS. 6.1 MMI. 6.1.1 Level 0. Concern has been expressed at the lack of an integrity requirement on the MM! in Level 0.		**Open.** In Level 0 ETCS can protect against overspeeding such that failure of the MMI may not be an issue. However, the driver may be reliant on the display for Temporary Speed Restrictions (TSRs) and determining when to brake in response to line side signals. Level 0 is not in the scope of Index 47.
24	6. ISA CONCERNS. 6.2 Error Tolerability The ISAs have noted that apart from the Unisig document Dimensioning and Engineering Rules (Subset 040) there are no general limits applied to the error tolerability of data such as distances, gradients, curvature, cant etc.		**Open.** These items need to be examined to assess if they need dealing with on a national or international level. This topic is not in the Scope of Index 47. Although it is addressed to EEIG.
25	7. USER GROUP CONCERNS. 7.1.1 Non-Stopping Areas. The EEIG have identified non-stopping areas as an item of concern as there is no uniform means of dealing with them. Typical questions are, • Can the driver override a non-stopping instruction in the event of an emergency? • Is there a rule to ensure that the RBC does not issue movement authorities that would cause a train or any part thereof, to come to a stand in a non-stopping area?		**Closed.** The event of erroneous stopping in a non-stopping area may be hazardous particularly if the train is stopped for a prolonged period. Conversely, it may be hazardous not to stop if, by proceeding, a greater danger is encountered. Very clear and unambiguous harmonised rules will be required.

	• There is no uniform interface between the Passenger Emergency brake request and ETCS. This complicates the definition of harmonised rules.		Index 47 System hazard identified covering this aspect.
26	To be considered: Those aspects of infrastructure that are National issues are outside the scope of the TSI, but the following must be respected: The infrastructure designer shall: i) assume that an interoperable train complies with the on-board safety requirements, ii) not change the safety requirements for the trackside constituents other than through the formal change control process, and iii) apply the certified elements of CoCoSig in a way that is compliant with the Index 47 Justification Report? generic safety case and certification.]		Closed Aspects are taken into account in our proposal 'recommendation for post-Index 47 steps'
27	Untimely brake application or train trip “Untimely brake application or train trip” was discussed and if new hazard should be added to the Log of System Hazards. If the Hazard is included an new accident type will have to be included. It was discussed how high the risk is. This would be discussed in the working group and Railways consulted to see how high the risk is. The result could be: o hazard exist but commercial requirement on the system is higher then the requirements due to this risk o new class of accident to be added and hazard included	At the moment "Untimely brake application or train trip" has not been considered as a system hazard	**Open**.