Rail to Digital automated up to autonomous train operation

D13.1 – Moving Block Specifications applying a train-centric approach, Part 3 – Safety Analysis

Due date of deliverable: 01/09/2024

Actual submission date: 07/07/2025

Leader/Responsible of this Deliverable: Manuel Schleiffelder ÖBB-INFRA

Reviewed: Y

Document status		
Revision	Date	Description
01	08/01/2024	Draft for internal review
02	29/05/2024	Draft for internal review
03	22/07/2024	Internal review comment implemented
04	03/12/2024	Update to new document template
05	07/07/2025	JU comments solved

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	X
SEN	Sensitiv – limited under the conditions of the Grant Agreement	

Start date: 01/12/2022 Duration: 21 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union's Horizon Europe research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Lars Behrendt	ÖBB-PV	Author
Jürgen Flötzer	FRQ/ÖBB-Affiliate	Author
Jens J. Franke	DB Infra GO	Author
Andreas Gerstinger	FRQ/ÖBB-Affiliate	Author
Felix Schaber	Thales/GTS_AT	Author
Manuel Schleiffelder	ÖBB-INFRA	Author / Task Lead
Balaz Toth	ÖBB-PV	Reviewer
Harish Narayanan	Nextrail	Reviewer
F. Javier González	Renfe	Reviewer
Daniel Kolář	AŽD	Reviewer
Iván Velado	CAF	Reviewer

ABBREVIATIONS AND ACRONYMS

AoC	Area of Control
APS	Advanced Protection System
AS	Adjacent System (neighbouring systems)
ASM	Assumption
CBO	Common Business Objectives
CCS	Command, Control, and Signalling
CELEX	Communitatis Europeae Lex
CES	Conditional Emergency Stop
CMD	Cold Movement Detection
CS	Control and Supervision
CSM-RA	Common Safety Method for Risk Evaluation and Assessment
DMI	Driver Machine Interface
DPS	Drive Protection Section
DR	Digital Register
EB	Emergency brake
EoM	End of Mission
ERA	European Railway Agency
ERJU	Europe's Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EULYNX	European initiative by 14 Infrastructure Managers to standardise interfaces and elements of the signalling systems
FA	Flagship Area (1 or 2) of ERJU IP
FRMCS	Future Railway Mobile Communication System
FS	Full Supervision
GSMR	Global System for Mobile Communications – Railway
HCS	Hierarchical Control Structure
ID	Unique Identifier
IM	Infrastructure Manager
IP	Innovation Pillar
IVV	Integration, Verification and Validation

IXL	Interlocking
JU	Joint Undertaking
L2	Level 2 (ETCS level definition)
L3	Level 3 (ETCS level definition), obsolete with enactment of TSI 2023
LX	Level Crossing
MA	Movement Authority
MBD	Moving Block Demonstrator
MBS	Moving Block System
OBU	On-Board Unit
OC	Object Controller
OM	Operations Manager
OS	On Sight
PDI	Process Data Interface protocol
PE	Plan Execution
Picop	Person in charge of possession
PKI	Public Key Infrastructure
PRAMSS	Performance Reliability Availability Maintainability Safety and Security
R2DATO	Rail to Digital automated up to autonomous train operation
RAMS	Reliability, Availability, Maintainability and Safety
RBC	Radio Block Centre
RCA	Reference CCS Architecture
Ref	Reference
RU	Railway Undertaking
SB	Stand By
SCI	Standard Command Interface
SCP	Safe Communication Protocol
SDI	Standard Diagnostics Interface
SDR	Safety Design Recommendation
SFE	Safe Front End
SH	Shunting
SIL	Safety Integrity Level
SL	Sleeping
SLC	System Level Constraints

SMI	Standard Maintenance Interface
SOC	Security Operations Centre
SoM	Start of Mission
SP	System Pillar
SPAD	Signal Passed At Danger
SR	Staff Responsible
SRE	Safe Rear End
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
SuC	System under Consideration
SysC	System Capability
SysF	System Function
TA	Trackside Assets
TACS	Trackside Asset Control and Supervision
TAF	Track Ahead Free
TBD	To Be Defined
TDS	Train Detection System
TIM	Train Integrity Monitoring
TIMS	Train Integrity Monitoring System
TMS	Traffic Management System
TRL	Technology Readiness Level
TTD	Trackside Train Detection
TU	Train Unit
UA	Unsupervised Area
UCA	Unsafe Control Action
UES	Unconditional Emergency Stop
URA	Usage Restriction Area
WP	Work Package
WSP	Wheel Slip Protection

GLOSSARY

Check: General procedure which ascertains if certain conditions hold (e.g., [check if] each end of a railway point is connected to a track section).

Configuration Data: Further information relevant for system operation that is not contained in topology, topography or infrastructure data (e.g., identifiers & connection parameters for object controllers and parameters for safety checks.)

Static Speed Profile: A static speed profile that is dynamically calculated by MBS and subsequently provided to the relevant train onboard unit.

Hazard: A hazard is defined as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" [1].

Infrastructure data: Additional information not contained in the topography but necessary for physical train operations (e.g., static speed profiles, cant, ...)

Loss: Within STPA, a loss is defined as an unacceptable event which harms "something of value to stakeholders." [1]. Typical values to protect include human life (loss of life), system function (loss of mission), the environment (loss of environment), etc.

Movement Authority: Permission for a train to run to a specific location within the constraints of the infrastructure [19].

Movement Permission: Request from PE to MBS to grant a defined MA for a certain train.

Safety Design Recommendation: Exported less stringent "recommendation" regarding the findings in this document versus more stringent "safety requirements" that may result from a later generation of this analysis.

Safety Requirement: A requirement based on findings from a safety analysis (see safety design recommendation).

Safety Responsibility: Defined responsibility with regards to safety functions of individual actors, systems or sub-systems.

Topography: Refers to geographical map information regarding the features of the terrain that correctly represent physical reality (geographical position, elevation, ...).

Topology: Subset of topography with linked track sections and identified track elements.

Unsafe Control Action: "An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard" [1].

System Level Constraints: "A system-level constraint specifies system conditions or behaviours that need to be satisfied to prevent hazards (and ultimately prevent losses)" [1].

Validation: "Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled."[3] This means validation is intended to ensure that the MBS meets the operational needs of the user.

Verification: "Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled."[3] This means verification is intended to check that the MBS meets its set of design specifications.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

This present document constitutes the technical contribution from Task 13.3 “Safety Analysis” to the Deliverable D13.1 “Moving Block Specifications applying a train-centric approach” in the framework of WP13, of FP2 R2DATO.

“The objective of this task was to work collaboratively to analyze the impact of System Pillar activities and Tasks (13.1 Definition/13.2 Specification) to develop a Moving Block Safety Analysis considering also the S2R results.” /R2DATO Grant Agreement/

To move a step beyond what was previously done in S2R (e.g., in-depth analysis of relevant scenarios) a novel method – called System Theoretic Process Analysis (STPA) - shall be applied to the matter. This STPA focuses on “unsafe control actions” in control and feedback loops within complex systems. An advantage over previous methods is the potential to identify emergent risks stemming from the interaction between those (sub)systems, which are often overlooked.

The subject of this analysis is the “Moving Block System” (MBS) that is being defined and specified in WP13. The figure below shows its localization within the planned Moving Block Demonstrator (MBD) from WP44/45. In this preliminary architecture it is foreseen that the MBS receives its topology model (Domain Data) from an entity designated as Digital Register (DR). Various commands and requests (e.g., requests to move a point/request to grant a movement permission) come from the Plan Execution (PE) that executes the operational plan from the Traffic Management System (TMS). On the other side, MBS facilitates communication with and also commands the Onboard-Units (OBU) and Trackside Asset Control & Supervision (TACS) – aka trackside object controllers.

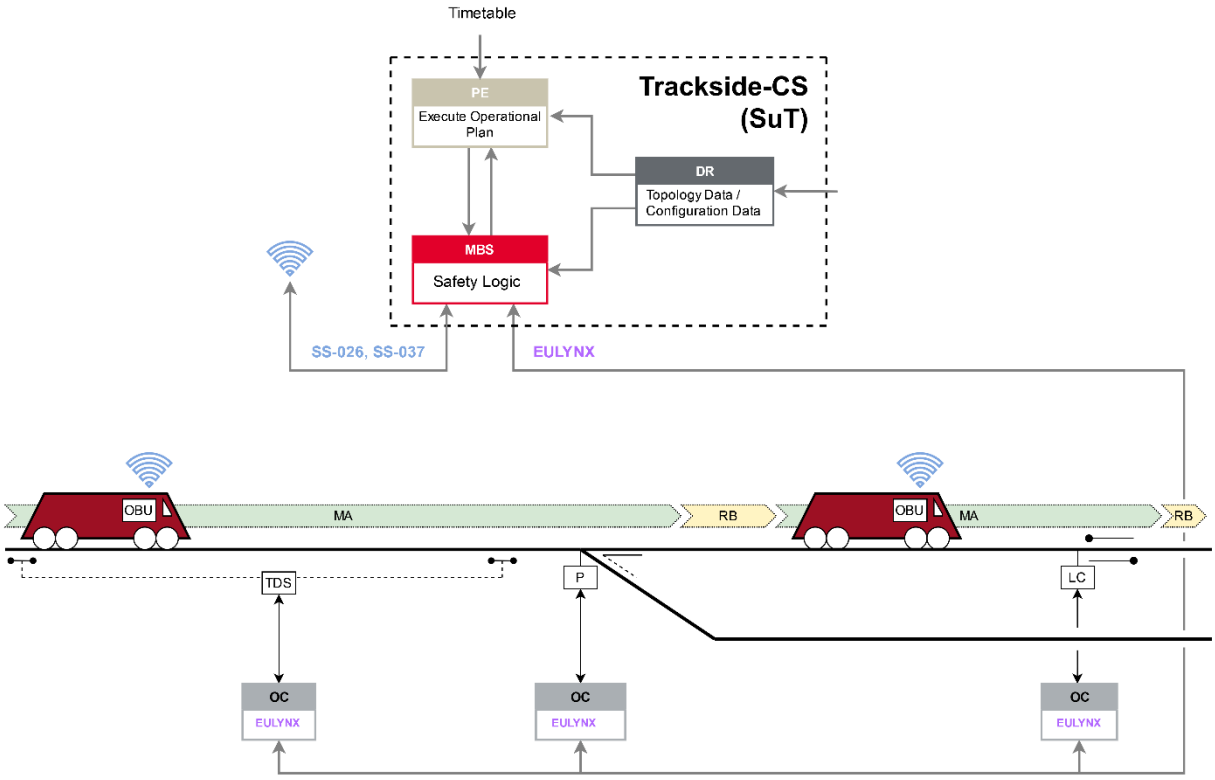


Figure 1: Localization of MBS within a simplified view of “moving block” trackside CS

The approach is “train-centric” in the sense that the physical train itself is considered as the main business object instead of indirectly deriving information about the train only by monitoring track occupations. Since we apply “moving block principles”, movement authorities can therefore be issued up to any point on the track, and trains can safely follow each other in absolute braking distance without being bound to wait for the next block section to become free. However, the system shall still be able to utilize information from previously installed Train Detection Systems (TDS) to complement and improve localization information where applicable (e.g. if receiving a OBU radio transmission takes longer than receiving occupation information from the TDS), and/or for migration purposes. Some advantages of the new system are:

- potential performance gains due to smaller train headway times.
- reduced efforts for TDS and obsolete lineside signals (cab side signaling).
- the merger of interlocking and RBC functionality, that enables the MBS system to even consider physical trains (since traditional IXL was only concerned about securing routes).
- the concentration of safety related functions into as few “safety-critical” components as possible (thereby reducing the SIL requirement for other components).
- the (envisaged) capability of runtime configuration updates.
- (envisaged) improved supplier independence due to open/fully defined interfaces.

MBS is thus by design “the component performing safety related functions” within this novel trackside CS. The implications of this approach on overall system safety are of great interest.

Previous investigations were focused on train localization (performance), radio communication (performance and availability), cold movement detection, as well as train length- and train integrity data. Ideally, the safety requirements from there can be mapped to the new results. However, a focus of this analysis are the control (inter-)actions and feedback between the adjacent systems (e.g., what are the main hazards that emerge from command and feedback loop between MBS and a safety operator panel).

2 SCOPE

The analysis for the Task 13.3 details the results of the safety analysis with focus on the MBS and its interfaces to the other internal and external systems, as depicted in Figure 2 - MBS System Boundary. It is based on the STPA analysis method for the current safety analysis and considers the result from the former X2Rail project. The STPA analysis proved to be the most suitable method at a time, when the system requirements and the system design were still subject to significant changes. Like in traditional safety methods, the efforts involved are highly dependent on the level of depth to which the STPA shall be conducted, and since the task resources are limited (due to overall WP allocation as well as due to the number of active authors) an adaptive approach is applied. While the whole system-stack involved in “command control & signaling” shall be covered at a high abstraction level, certain points of interest (e.g., where valuable information for feedback to the specification task can be generated) can be investigated on a lower abstraction level, down to individual control/feedback telegrams.

The analysis does not provide all the evidence to obtain certification or to fulfil the mandatory requirements or design standards (e.g.: EN50126-1 and -2, EN50128, EN50129, EN50159, ...). However, it will define safety related design recommendations which shall be considered during the development of the MBS and may be mapped to safety requirements in a later stage.

The overall analysis of the whole Moving Block Demonstrator (MBD) as depicted in Figure 1 below is covered in WP44/45 (Task 45.5.).

2.1 SYSTEM BOUNDARY

As briefly described in the introduction, the system boundary of MBS is defined through interfaces within the Moving Block Demonstrator (MBD) (e.g., I_PE, I_DR) and also to the outside of the MBD (e.g., I_TACS, I_TACS). Even though similar definitions have already been produced within Task 13.1, 13.2 and 44.3 we decided to reproduce (copy/update/rewrite) such a section here – at least until the documents from these tasks are in a stable version. Within this section there is also a description of all the subsystems depicted in the drawing below. Relevant Interface descriptions can be found in chapter 6 Interface Criticality together with a preliminary analysis of the interface criticality. The handover to neighboring systems is out of scope for this analysis.

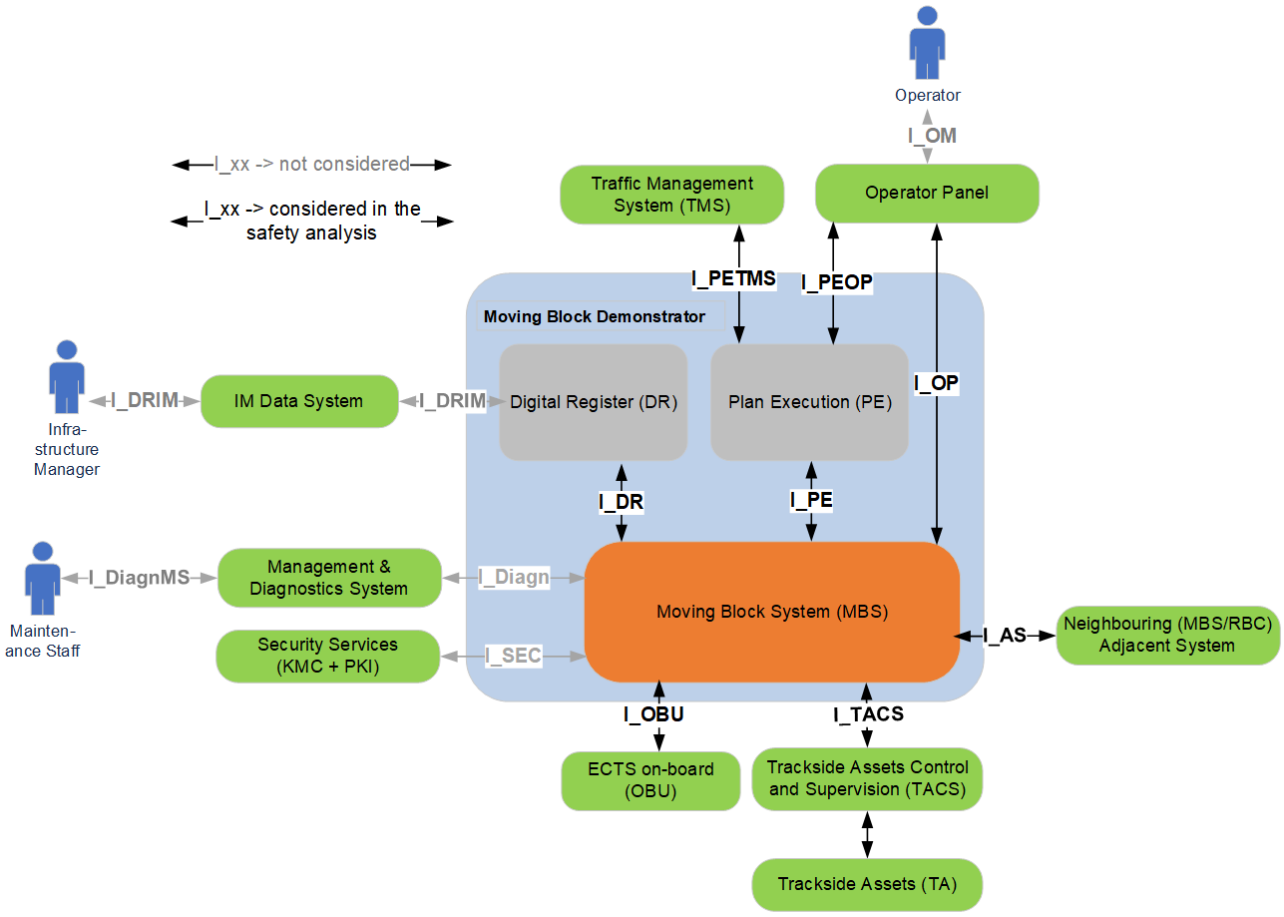


Figure 2 - MBS System Boundary

2.2 CONNECTED SYSTEMS

This chapter provides an actual description of the systems the MBS interacts- or has dependencies with, as shown in the system boundary figure above. The description itself is based on the system definition in WP44 Task 44.3.

2.2.1 Neighbouring (MBS/RBC) System

Attribute	Content
Name	Neighbouring (MBS/RBC) System [Adjacent System in 13.1/13.2]
Description	A neighbouring System can be either another MBS, a different radio-based ETCS related neighbouring system (e.g., RBC) or e.g., an RBC/IXL combination with traditional route logic. The interface to a radio-based ETCS related neighbouring system allows trains to pass the border to/from a neighbouring Level 2 area without changing the driver responsibility and the cab-signalling.

	The interface to a neighbouring system not related to radio-based ETCS allows trains to pass the border to/from an area not equipped with Level 2. The cab-signalling is replaced by optical signals and vice versa.

Table 1 – Neighbouring System Definition

2.2.2 Diagnostics System

Attribute	Content
Name	Management & Diagnostics System
Description	The Diagnostics system monitors the state of the MBS and logs parameters of interest. For this purpose, MBS transmits log, status, and diagnostic data to the Diagnostic system for status evaluation and analysis.

Table 2 – Diagnostics System Definition

2.2.3 Digital Register

Attribute	Content
Name	Digital Register
Description	The Digital Register (DR) provides reliable (meaning complete, accurate, current, consistent, verified and validated), interoperable and accessible infrastructure information as a critical enabler for safety-related and non-safety-related functions. The Digital Register includes static infrastructure information (static speed profile, gradients, cant, etc.) and configuration data, which are approved after the engineering process. The interface between the DR and the MBS is used to update the data in the MBS.

Table 3 – Digital Register Definition

2.2.4 ETCS on-board

Attribute	Content
Name	ETCS on-board
Description	The ERTMS/ETCS on-board (OBU) equipment is a computer-based system that supervises the movement of the train to which it belongs, on basis of information exchanged with the MBS. Its system requirement specification is defined in UNISIG subset 26 [2]

Table 4 – ETCS on-board Definition

2.2.5 Operator Panel

Attribute	Content
Name	Operator Panel
Description	The Operator Panel is a system that provides the human-machine interface with the Operations Manager in order to provide status information on the operation of the railway system and accept input for the resolution of degraded situations.

Table 5 – Operator Panel Definition

2.2.6 Plan Execution

Attribute	Content
Name	Plan Execution
Description	The PE operationalizes the “operational plan” or “timetable” as received from TMS via the I_OP interface. The functional split between PE and MBS is along a virtual SIL-boundary (allowing PE to be classified as SIL-basic integrity only). PE actually conceives the Movement Permissions and the individual commands for trackside assets, while MBS is a “gatekeeper” that validates (safety logic) and forwards commands and Movement Authorities to trackside assets and trains. The MBS only acts upon dedicated emergency patterns and provides the *Operational State* to the PE.

Table 6 – Plan Execution Definition

2.2.7 Security Service

Attribute	Content
Name	Security Service
Description	The Security Service summarises all technological systems that are necessary to manage and provide the cryptographic artefacts (e.g., keys or certificates) to ensure the confidentiality, authenticity and integrity (Information Security Triad) of the communication between subsystems.

Table 7 – Security Service Definition

2.2.8 Trackside Asset Control and Supervision

Attribute	Content
Name	Trackside Asset Control and Supervision

Description	The Trackside Asset Control and Supervision (TACS) reports the state of the *Trackside Asset*s (TAs). The MBS mainly uses this interface to trigger setting the state of a TA, e.g., moving a point, and to receive status information from TAs (e.g., occupancy information from TDS)

Table 8 – Trackside Asset Control and Supervision Definition

2.2.9 IM Data System

Attribute	Content
Name	Infrastructure manager (IM) Data System
Description	Infrastructure Manager Data System describes the body or firm responsible for the management of all relevant infrastructure data, traffic management, and control-command and signalling in alignment with key term definition in Directive 2012/34/EU.

Table 9 – IM Data System Definition

2.2.10 Traffic Management System

Attribute	Content
Name	Traffic Management System (TMS)
Description	Traffic Management System provides functionality for preparing and optimising the entire schedule within an Area of Control. This schedule will be represented by operational plans for each individual Train Unit. This operational plan is provided to the PE where it is operationalized into specific commands and movement permissions. PE provides the current operation state to TMS as feedback.

Table 10 – Traffic Management System Definition

3 INPUTS

The documents, project outputs, open standards as well as documents from tasks within R2DATO that are relevant to the work here are listed and briefly described in this chapter.

3.1 SYSTEM PILLAR INPUTS

System Pillar provided an envelope for the ERJU activities within the “common business objectives”- and the “operational visions” documents. Relevant passages have been cited below and shall be e.g., used as a benchmark for concluding remarks (in a later stage of the document).

3.1.1 CBO ([6], p.18) - Optimize safety strategies and standards

- Safety critical elements of a system should be optimized and simplified through design by moving away from bespoke solutions. The development of these parameters facilitates a common approach to safety and security. (simplified standard safety components)
- Simulation and modelling tools are needed to accurately calculate and validate the performance of systems with an incorporated robust PRAMSS framework controlling for the development process and the RAMSS change impact analysis for changes inside of the life cycle. (validated system performance) (robust PRAMSS framework)
- The safety logic shall have a generic approval and authorization in which it is proven that it just needs a reliable input of topology information and train information and will assure safety on this basis. {safety logic with generic safety approval}
- The exchange of components or connection of new subsystems under production shall happen without a new safety case or preparation processes. {seamless and selective exchange of components under production}
- An authorized vehicle can be operated everywhere on compliant infrastructure without local integration test. {vehicle is interoperable without local integration test}

3.1.2 Operational Vision ([7], p.20) - Enhanced safety assurance process

- Because of a high architecture quality, safe integration of components to a whole safe application is just done by a centralized (online) compliance test (certificate), that is done once (strategy “modular safety”).
- The quality of validation/testing and practical risk assessment for components and “system of systems” reaches a quality level, that allows to simplify bureaucratic development processes of today.
- Independent/redundant/stable safety monitoring systems and actor advisory systems allow a more dynamic change of systems and diversity of configurations and support a continuous improvement process.

3.1.3 Operational Scenarios

Missing. Implicitly defined operational scenarios within the use- and test-cases from Task 44.2. will be analyzed instead until other information is available.

3.2 X2RAIL DOCUMENTATION

- Safety Analysis from X2RAIL-1 [9]
- Safety Analysis from X2RAIL-3 [10]
- Safety Analysis Update from X2RAIL-5 [11]

The safety requirements from the shift2rail projects (currently to be found in the mapping tables / xlsx / within the project folder) shall be discussed in chapter 7 in a later stage of the document.

3.3 RCA DOCUMENTS

The Reference CCS Architecture (RCA, version 1.0, [12]) is a relevant input in the specification work packages as well as to system pillar activities and shall – at least implicitly – be considered.

3.4 R2DATO DOCUMENTS

The following documents from other tasks within R2DATO WP13/14 and WP44/45 are to be considered for this analysis:

- Task 13.1 provides a high-level definition for the Moving Block System (MBS) [13]
- Task 13.2. provides the (current) specification of the Moving Block System (MBS). [14]
- Task 44.2 Use cases document. [17]
- Task 44.3. provides a high-level definition, as well as the (current) specification of the Moving Block Demonstrator (MBD). [15, 16]

4 SAFETY ANALYSIS METHODEOLOGY

This chapter describes the used safety analysis methodologies on a very high abstraction level. Even though some aspects of the larger demonstrator (MBD) architecture have to be taken into account, the target of this safety analysis is the Moving Block System (MBS). The analysis is partly based on outputs from predecessor projects, such as X2Rail and RCA, but it also relies on inputs from system pillar, as well as the results from connected tasks within R2DATO.

The envisaged goal for the demonstrator (MBD) is TRL (Technology Readiness Level) 6 [20]. At this stage, the complete safety analysis is qualitative only, not quantitative. Quantitative methods, such as fault trees to verify specific safety objectives, may be added in a later stage when a higher TRL shall be achieved.

Figure 3 shows the scope of the safety analysis in the so called “hourglass model” from CENELEC EN 50126-2.

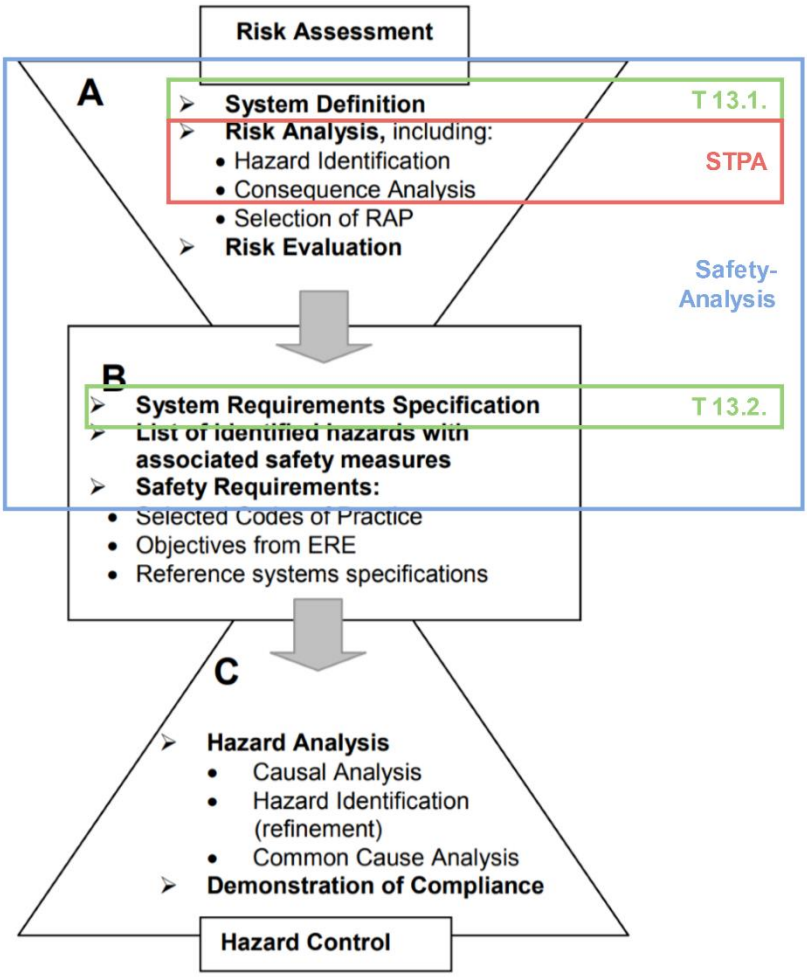


Figure 3 – Safety Analysis in Relation to the Hourglass Model

4.1 COMMON SAFETY METHODS

For safety-relevant changes to railroad systems (e.g., technical, operational, regulative or organizational changes), the risk assessment process in accordance with EU regulations 2015/1136 and 402/2013 (CSM-RA) must be applied.

However, technical changes to a system that are handled with the RAMS management process of the CENELEC standard EN 50126 (+128/129) are generally compliant with the CSM procedure.

4.2 CENELEC STANDARDS

Tasks 13.1 and 13.2 within work package 13 are developed along the relevant CENELEC standards. Thus, the following standards apply:

- EN 50126-1:2017: Generic RAMS Process
- EN 50126-2:2017: Systems Approach to Safety
- EN 50716:2023: Requirements for software development (supersedes EN 50128:2011: Software)
- EN 50129:2018: Electronic systems

They shall be applied as far as practicable for a TRL 6 system. This means that the standards will be taken as a major input for the development, but some requirements may be interpreted in a more relaxed way as it would be the case for a fully operational system.

4.3 STPA

The STPA handbook [1] describes the practical application of STPA in great detail. Here, we only provide a very short description and the reason why STPA was chosen.

STPA (System-Theoretic Process Analysis) is a method to identify hazards and related system constraints in complex systems, in order to identify (unsafe) control actions that lead to those hazards (and related losses). Mitigations to avoid these unsafe control actions can then be derived.

The reason why STPA was chosen is that it is geared towards large and complex systems with multiple interactions, where hazards do not necessarily only arise due to component failures, but also due to emergent behavior involving multiple components. The MBS (especially in combination with its interfaces and interactions with the environment) is a novel system, for which this method is believed to be of great value.

5 RISK ANALYSIS

This chapter details and documents the results of the conducted STPA analysis as described in chapter 4.3. The analysis focuses on the marked section of the “hourglass model” from CENELEC EN 50126-2 as shown in Figure 3 which is intended to derive the safety requirements from operator point of view. These requirements must be considered by the suppliers of an MBS system. The supplier’s safety analysis shall consider these requirements as their safety goals, that can be broken down into further sub safety goals and requirements.

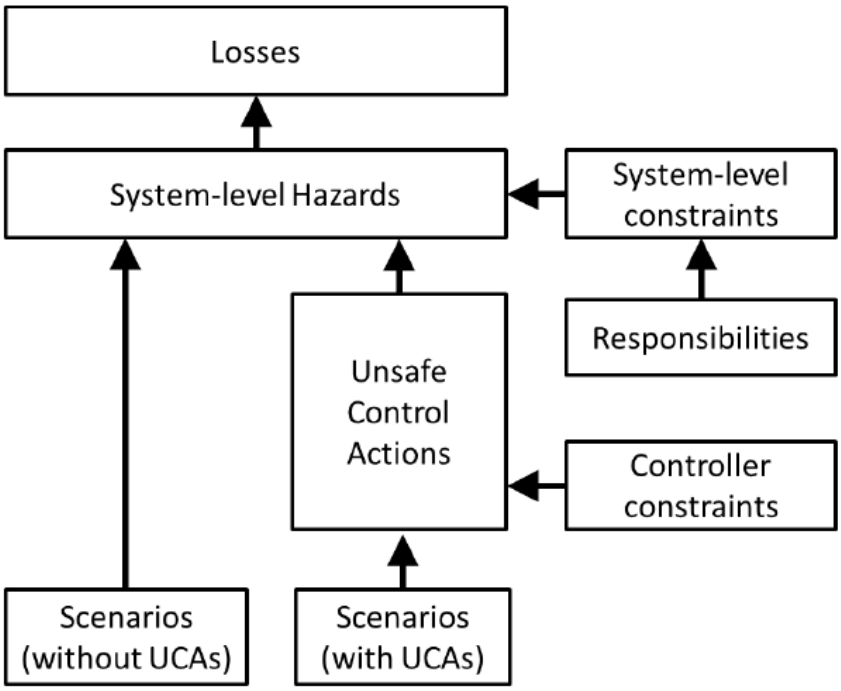


Figure 4: Traceability from STPA outputs from [1]

5.1 LOSSES

The first step of the STPA is to define which losses to consider for the analysis. The purpose of the analysis is to find possible causes for accidents. An accident is defined as an undesired or unplanned event that results in a loss. A loss always involves something of value to the stakeholder. Typical examples are loss of human life or injury, but also property damage, environmental pollution or loss of mission. [1] For this analysis, three main losses are considered:

Legend of the following table:

ID … a unique identifier

Name … a description of the loss

ID	Name
L-1	Loss of life or injury to people on the train (including injury because of incorrect braking technique without derailment or collision) • Passengers • Railway staff (crew on the train)

ID	Name
L-2	Loss of life or injury to people outside the train • Level crossing users (by any means of transportation or by foot) • People on the platform or neighbourhood of tracks • Railway workers • Trespassers (persons present on railway premises where such presence is forbidden)
L-3	Environmental loss (i.e. transport of dangerous goods)

Table 11 – Losses

Explicitly excluded from this analysis are loss of mission and loss of customer satisfaction, as our focus for this analysis is strictly on safety (e.g., a person's life).

5.2 HAZARDS

The next step of the analysis is to find the system level hazards. Within STPA, a hazard is defined as "a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss" [1]. Note that this definition differs from the classical definition of a hazard. It is essential that hazards are defined at system level instead of component level, as hazards may also arise from the interaction between components and cannot necessarily be assigned to a single component.

A system is defined as "a set of components that act together as a whole to achieve some common goal, objective, or end" [1]. It may contain subsystems and the analysis may be based higher or lower level of abstraction of individual subsystems as needed.

In order to identify system level hazards, it is therefore necessary to identify the system under consideration and the analysis boundary as defined in chapter 2.1 System Boundary. A useful way to define the analysis boundary may be to include only systems within the analysis boundary over which the system designers have some form of control.

To ease readability the hazards are described in a generic form. Each hazard may have multiple sub-hazards, further detailing the high-level hazard.

The hazards differentiate between losses in connection with other trains and hazards in connection with "other obstacles". For the purposes of this analysis, runaway trains are regarded as "other obstacles".

Legend of the following table:

ID … a unique identifier

Name … a description of the unsafe condition

ID Losses … associated losses

ID	Name	ID Losses
[H-1]	**Train does not maintain safe distance to other trains (front, back, flank)**	[L-1]
[H-1.1]	Train deceleration is insufficient	-

ID	Name	ID Losses
[H-1.2]	Train deceleration is too late	-
[H-1.3]	Train passes over point which has lost its end position (“Endlage”)	-
[H-1.4]	Train passes over point which indicates a wrong position	-

ID	Name	ID Losses
[H-2]	**Train does not maintain safe distance to other obstacles (obstacles include railway workers, vehicles on level crossings, end of line)**	[L-1, L-2]
[H-2.1]	Train deceleration is insufficient	-
[H-2.2]	Train deceleration is too late	-
[H-2.3]	Train passes over point which has lost its end position (Endlage)	-
[H-2.4]	Train passes over point which indicates a wrong position	-
[H-2.5]	Level crossing occupied by road vehicle or pedestrians	-
[H-2.6]	Railway workers on track or near track (might be dangerous at high speed)	-
[H-2.7]	Trucks and other construction trains	-
[H-2.8]	Runaway railway trains	-
[H-2.9]	Level crossing blocked longer than necessary	-

ID	Name	ID Losses
[H-3]	**Train leaves allowed/provisioned/allocated/reserved clearance gauge**	[L-1, L-2, L-3]
[H-3.1]	Train derailment and possibly collision with railway trains or other obstacles	-
[H-3.2]	Train violating clearance gauge due to e.g., overhanging cargo	-
[H-3.3]	Train violating clearance gauge due to running on two tracks simultaneously (“Gabelfahrt”)	-

ID	Name	ID Losses
[H-4]	**Train exposes passengers to high forces**	[L-1]
[H-4.1]	Train applies non-appropriate (excessive) braking technique	-
[H-4.2]	Train coupling with too high speed	-
[H-4.3]	Train overspeeding in curves	-

ID	Name	ID Losses

ID	Name	ID Losses
[H-5]	**Train exposes people outside the train to high forces (e.g., platform, level crossing, railway workers)**	[L-2]

ID	Name	ID Losses
[H-6]	**Train loses integrity of the train frame**	[L-1, L-2, L-3]
[H-6.1]	Environmental damage due to loss of dangerous goods	-
[H-6.2]	Runaway wagon (train integrity lost - train brakes apart)	-
[H-6.3]	Train frame damaged due to obstacle violating clearance gauge Note: This is currently not controllable	-

ID	Name	ID Losses
[H-7]	**Train enters an unsafe region (e.g., tunnel fire, landslide, avalanche, broken rails, storm, flooding, etc.) or train cannot leave unsafe region (e.g., tunnel fire) in acceptable time frame**	[L-1]

ID	Name	ID Losses
[H-8]	**Train violates utilization conditions of the infrastructure**	[L-1, L-2, L-3]
[H-8.1]	Train exceeds maximum allowed speed - overspeeding	-
[H-8.2]	Train not covered by allowed train types (axle load, track gauge, clearance gauge, emergency running characteristics, air-tight system, etc.)	-
[H-8.3]	Damage to infrastructure after temporary change of utilization conditions, which in consequence can cause derailment of following trains.	-

Table 12 – Hazards

5.3 SYSTEM LEVEL CONSTRAINTS

Legend of the following table:

ID … a unique identifier

Name … a description of the system level constraints

ID Hazards … a list of hazards associated with this system level constraints

5.3.1 Collision Avoidance

ID	Name	ID Hazards
[SC-1]	Trains must maintain a safe distance to other trains or obstacles.	[H-1, H-2]
[SC-1.1]	Areas reserved for train movement must not overlap.	[H-1]
[SC-1.2]	The permissible speed must be such that it is always possible to decelerate/brake the train in the area reserved for it.	[H-1.1, H-2.1, H-8.1]
[SC-1.3]	Conditions which limit the braking performance must be taken into account. (e.g. wet tracks or leaves on the track)	[H-1.1, H-2.1]
[SC-1.4]	The safety distance must be large enough so that the residual risk of a collision is acceptable even if the braking performance is worse than expected. (coupling of trains should still be possible –> “safe collision” of trains)	[H-1.1, H-2.1]
[SC-1.5]	The ability of trains to maintain the braking curve must be supervised, a violation must be detected and measures taken to prevent collisions. (e.g. emergency brake and/or deceleration of other trains, warning/closing of level crossings)	[H-1.2, H-2.2]
[SC-1.6]	If a point in an area reserved for train movement loses its end position, this must be detected and the train must be prevented from passing over it or at least the severity must be reduced by decelerating controlled trains and other vehicles.	[H-1.3, H-2.3, H-3.3]
[SC-1.7]	The current state of railway points must be correct with a very high probability. (MBS has no influence on this, except that certain safety application conditions can be required)	[H-1.4, H-2.4, H-3.3]
[SC-2]	If trains violate safe distances to other trains or obstacles, this violation must be detected and measures taken to prevent collision.	[H-1, H-2]
[SC-2.1]	Level crossings in an area reserved for train movement must be secured in a timely manner and other level crossing users must be warned in advance.	[H-2.5]

ID	Name	ID Hazards
[SC-2.2]	Trains must not pass level crossings too fast, depending on the local conditions (i.e. not completely secured level crossing).	[H-2.5]
[SC-2.3]	If it can be detected that a level crossing is occupied by some other level crossing users, then measures must be taken to reduce the risk of collision to a tolerable level.	[H-2.5]
[SC-2.4]	Railway workers must be warned in time when a train approaches a construction site.	[H-2.6]
[SC-2.5]	Trains must not pass railway workers (construction sites) too fast. (speed depends on the distance of the train to the railway workers)	[H-2.6]
[SC-2.6]	If trucks or other construction trains intersect an area reserved for a train movement, this must be detected and measures taken to prevent collision.	[H-2.7]
[SC-2.7]	Runaway railway trains must be detected (e.g. detection using TIMS, TTD, etc.) and measures taken to reduce the risk of collision to a tolerable level.	[H-2.8, H-6.2]
[SC-2.8]	Level crossings must not be blocked longer as necessary (i.e. barriers are to be opened as soon as the train has passed over the level crossing).	[H-2.9]

Table 13 – Collision Avoidance

5.3.2 Clearance Gauge – Derailment

ID	Name	ID Hazards
[SC-3]	Trains must stay within their reserved clearance gauge.	[H-3]
[SC-3.1]	Trains must be compatible with the infrastructure. (i.e. if axle load, track gauge, clearance gauge, minimum brake performance, … do not match or is not met, the train must not use this section of line)	[H-3.1, H-8.2]
[SC-3.2]	Trains must comply with the utilization conditions of the infrastructure. (i.e. the maximum permitted speed, which may depend on the actual train, must not be exceeded) Note: Here (SC-3.1 and SC-3.2) a distinction is made between the more static and the more dynamic conditions.	[H-3.1]
[SC-3.3]	If the utilization conditions are violated by a train, this must be detected and measures taken to reduce the risk of derailment.	[H-3.1]

ID	Name	ID Hazards
[SC-3.4]	If the clearance gauge is violated by a train, this must be detected (e.g. using checkpoint installations) and measures taken to reduce the risk of accidents. Note: checkpoint installations may be able to detect more issues like fire in the train, hot box, hot wheel, derailed axle.	[H-3.2]

Table 14 – Clearance Gauge

5.3.3 High Forces

ID	Name	ID Hazards
[SC-4]	Train must not expose passengers to high forces.	[H-4]
[SC-4.1]	Trains must not use excessive braking technique (i.e. emergency brake), if other measures are possible that reduce the risk of passenger injury to an acceptable value.	[H-4.1]
[SC-4.2]	Coupling of trains must be done at a speed so that the risk of passenger injury is acceptable.	[H-4.2]
[SC-4.3]	The speed of trains in curves must not expose passengers to an unacceptable risk. Note: This maximum speed depends on the radius of the curve, superelevation and tilting technology.	[H-4.3]
[SC-5]	Trains must not expose people outside the train to high forces.	[H-5]
[SC-6]	If train loses its train integrity, this must be detected and measures taken to prevent collision.	[H-6]

Table 15 – High Forces

5.3.4 Runaway Trains

ID	Name	ID Hazards
[SC-6.1]	If train loses its train integrity (i.e. runaway wagon), this must be detected and measures taken to reduce the risk of accidents. Note: This can be detected by monitoring train integrity (TIM), cold movement detectors or by TTD where available.	[H-6.2]
[SC-6.2]	If trains lose dangerous goods, this must be detected and measures taken to reduce the risk of environmental damage. Note: What measures are possible still needs to be investigated.	[H-6.1]

ID	Name	ID Hazards
[SC-6.3]	If the train frame is damaged, this must be detected and measures taken to reduce the risk of passenger injury. Note: Usually handled during inspections or through observant staff.	[H-6.3]

Table 16 – Runaway Trains

5.3.5 Unsafe Regions

Note: A unsafe region is not permanently unsafe (no train would be allowed to pass permanently unsafe regions). A region becomes unsafe due to events that cannot be planned, e.g., tunnel fire, landslide, avalanche, broken rails, storm, flooding, … Nevertheless, it is possible to detect these events with the use of sensors, or the operator (informed by e.g., the driver) manually instructs the system.

ID	Name	ID Hazards
[SC-7]	Trains must not be exposed to unsafe regions.	[H-7]
[SC-7.1]	Trains must not enter unsafe regions.	[H-7]
[SC-7.2]	Trains must leave unsafe region in acceptable time frame (e.g. tunnel or bridge, where safe passenger egress is not possible (i.e., non-stopping area)).	[H-7]

Table 17 – Unsafe Regions

5.3.6 Utilization Conditions

ID	Name	ID Hazards
[SC-8]	Trains must not violate the utilization conditions of the infrastructure.	[H-8]
[SC-8.1]	The utilization conditions must model the infrastructure in a way that compliance with these utilization conditions results in a tolerable risk of train movements. Note: This condition results in a requirement for data quality.	[H-8.1, H-8.2]
[SC-8.2]	Temporary change or degradation of the infrastructure must be incorporated in the utilization conditions modelling the restrictions on how the infrastructure can be used with a tolerable risk.	[H-8.3]

Table 18 – Utilization Conditions

5.4 HIERARCHICAL CONTROL STRUCTURE (HCS)

The hierarchical control structure models the system using functional components called controllers. Higher level controllers may enforce constraints on the controlled system by using control actions. Additionally, controllers may receive information from other controllers as feedback. Together the controllers form feedback control loops, shaping the overall behavior of the system.

Which actions a controller performs is determined by its control algorithm, representing the decision-making process. The information available to the controller at decision time is represented by the process model. A simple case of a control feedback loop is illustrated in Figure 5.

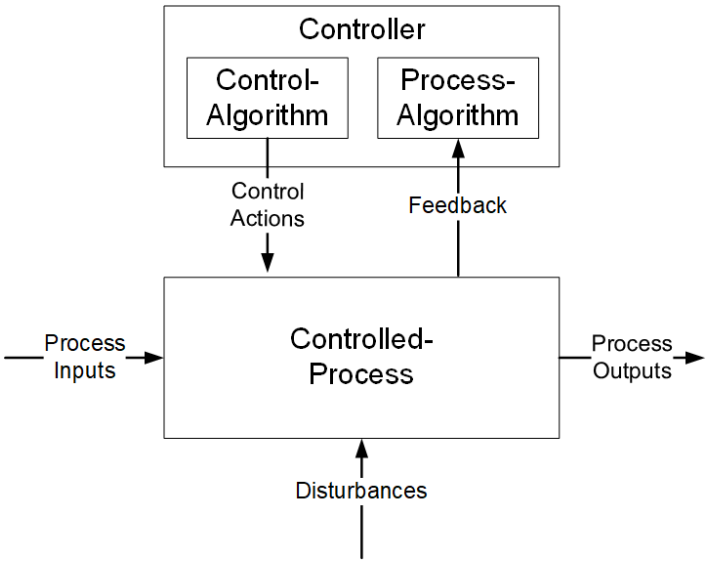


Figure 5 - Simple control-loop

The controller in the hierarchical control structure (HCS) is a functional representation, which may represent a single system or multiple system. A controller may be a human as well as a technical system. The control structure may be represented using multiple levels, where system details for lower levels are added as needed for the analysis.

A very high-level control structure for the CCS system is shown in Figure 6.

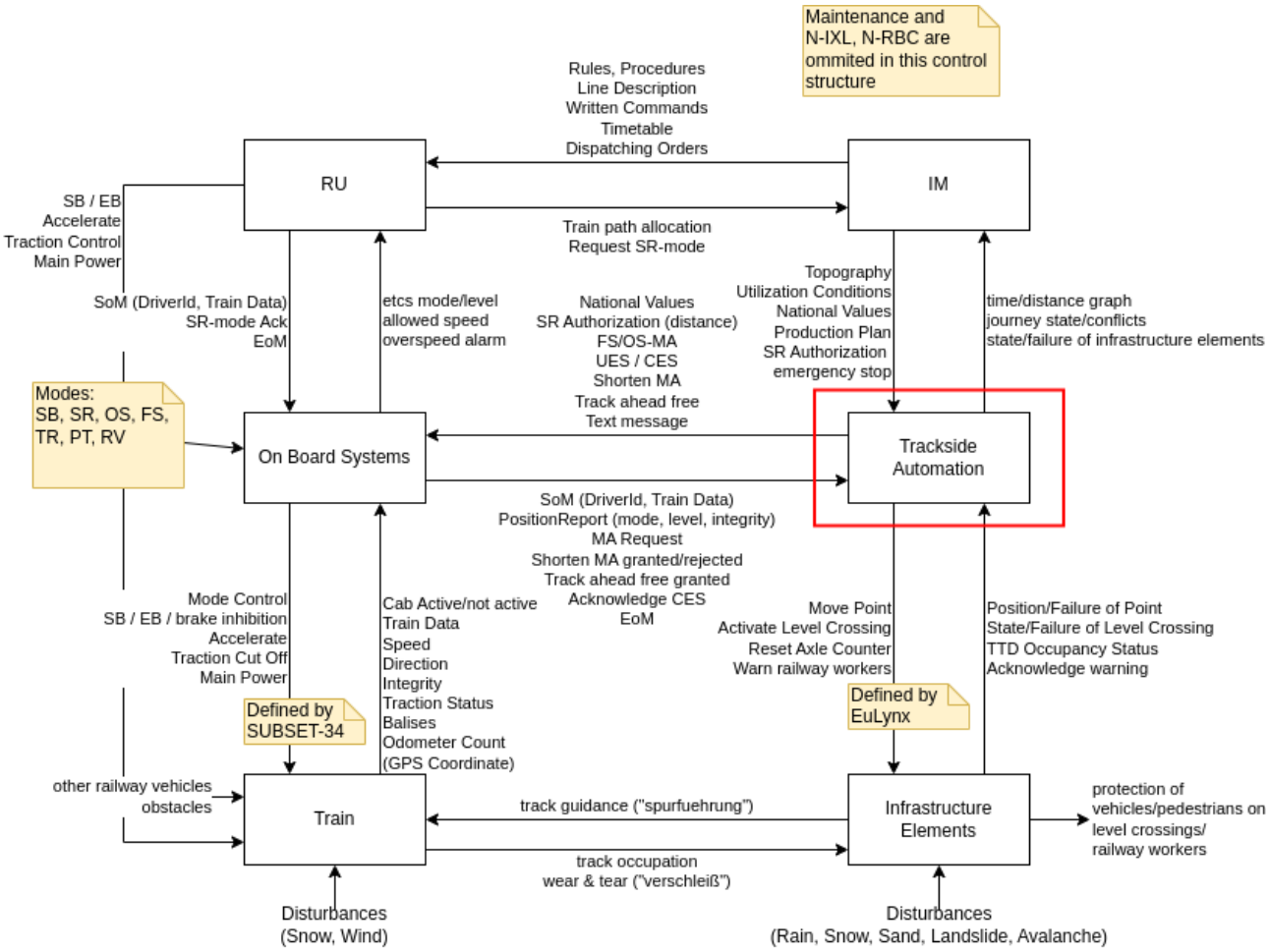


Figure 6 - High level control structure of the CCS system. The red rectangle highlights the controller containing the MBS system

Further detail is shown in Figure 7. The hierarchical control structure from Figure 6 is further decomposed to highlight the interaction of the moving block subsystem with other controllers.

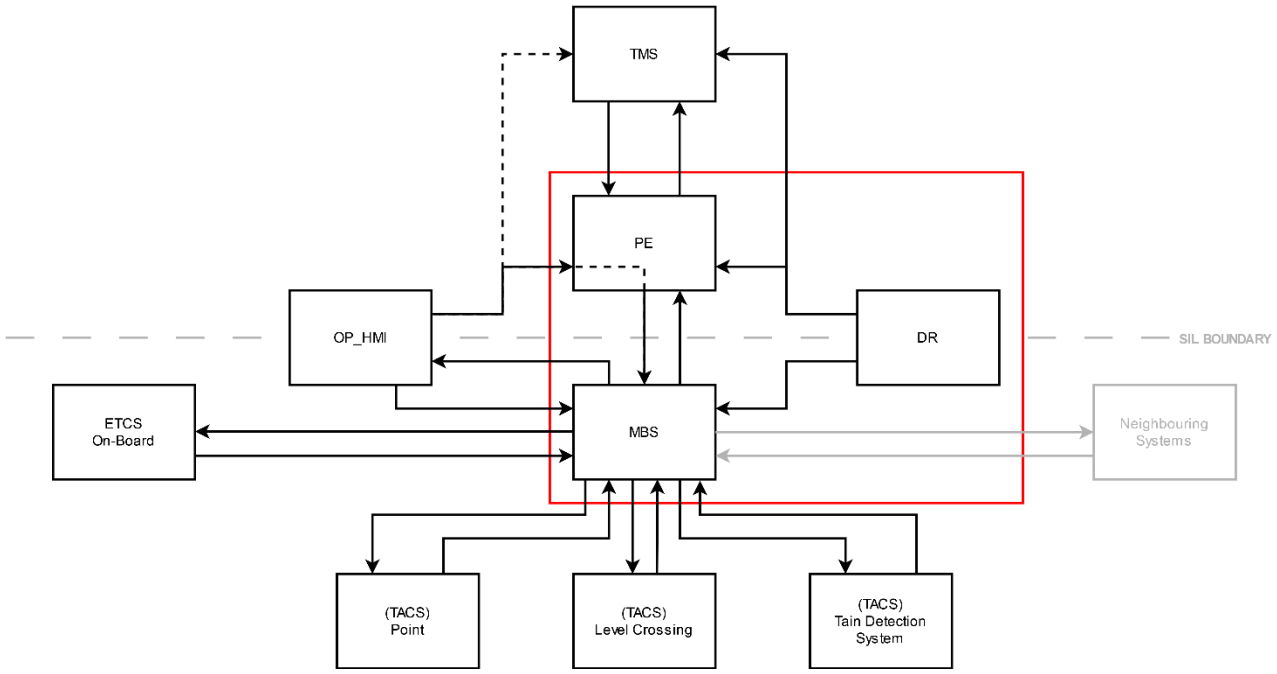


Figure 7 - Schematic second level control structure with focus on the trackside automation system. The red rectangle highlights the Moving Block Demonstrator (MBD)

Further below, in chapter 5.7 the MBD will be broken down into individual control loops between MBS and its adjacent systems.

5.5 ASSUMPTIONS

When analyzing a (not yet fully specified) system, a number of assumptions about its environment and internal operations are needed. Assumptions from the WP13 System Definition (as recorded in [17]) are used where they are directly relevant for the safety analysis. The corresponding System Description IDs are referenced at the end of the assumptions in square brackets where applicable.

Legend of the following table:

ID … a unique identifier

Name … a description of the assumption

ID Overall … a list of overall mitigation associated with these assumptions

ID	Name	ID Overall
[ASM-1]	MBS communicates using standardized interfaces with the field elements (Eulynx).	[I4]

ID	Name	ID Overall
[ASM-2]	MBS receives position information from the trains OBU and uses the train position information to derive movement authorities (train centric approach).	[G1]
[ASM-3]	Only ETCS Level 2 (previously Level 2/3 or R) equipped trains are supported by the MBS during normal operation. Trains without TIMS are supported for migration scenarios, when TTDs are available.	[G2]
[ASM-4]	MBS does not require TTDs but supports them for migration scenarios.	[G3]
[ASM-5]	MBS aims to have as little manual intervention (e.g. by the operator) as possible.	[G4]
[ASM-6]	MBS operation assumes trains are equipped with a TIMS (Train integrity monitoring system). However, in degraded modes and for migration purposes operation without TIMS is supported as well.	[G5]
[ASM-7]	MBS is responsible for safety control and should contain a generic and simple safety logic. The operational commands are generated by other systems.	[A2]
[ASM-8]	Train length and train integrity confirmation are relevant for a SIL 4 functions and therefore have to be provided with appropriate correctness guarantees for these functions.	[T0]
[ASM-9]	The train length reported by the OBU represents the maximum train length (e.g. after stretching).	[T1]
[ASM-10]	Changes in the communication technology to the Trains will neither affect the content of the messages defined in the ETCS Definitions nor the transit time (TBD s) of the messages between the Moving Block System and the trains.	[T2]
[ASM-11]	MBS functionality does not change whether the train is operated by a human driver or ATO.	[T3, T4]
[ASM-12]	MBS requires that the cold movement of trains is detected. This could be performed e.g. by a cold movement detection device (CMD device).	[T7]
[ASM-13]	The Train OBU and the infrastructure elements/OCs are SIL-4 systems.	-
[ASM-14]	The PE can be a SIL Basic Integrity safety related and non-safety related system.	-

ID	Name	ID Overall
[ASM-15]	The integrity of communication between the train OBU and MBS is ensured by a SIL-4 system.	-
[ASM-16]	The integrity of communication between the train infrastructure elements/OCs and MBS is ensured by a SIL-4 system.	-
[ASM-17]	Object controllers are correctly installed and configured. This can be checked by operational procedures with optional automated support (e.g. flagging the configuration as correct after multiple successful train passings) (i.e. the position reported by a railway point will not be incorrect due to wrong wiring of the 4-wire-bus).	-
[ASM-18]	Every train is identified by a unique and unchangeable identifier.	-
[ASM-19]	MBS assumes that the train is declared compliant („zugelassen“) with the tracks by the IM.	-
[ASM-20]	A train must be able to stop before the EoA/danger point. The braking curve is supervised by the trains OBU.	-
[ASM-21]	Safety Related text messages will not be sent by the operator. Instead, such message should be generated by automated systems (e.g., MBS).	-
[ASM-22]	Interaction between the operator and MBS only involves safety related information.	-
[ASM-23]	Other interactions of the operator with the system are done via the PE or the TMS.	-
[ASM-25]	All information received from the operator panel is relevant for one AoC only. This implies that it is not necessary to exchange this information between MBS and neighbouring systems.	-
[ASM-26]	The received information about the infrastructure (geographical position of tracks, points, etc.) correctly represent physical reality. An external controller is responsible for the data validation process. Rationale: MBS safety functions depend on this input but cannot verify the input independently.	-
[ASM-27]	When train integrity is lost, the main reservoir pipe is vented and the train emergency breaks engage.	-
[ASM-28]	Operator informs the MBS, about all regions where a train movement has been manually authorised by the operator. This also includes situations, where the radio connections to the OBU is lost.	-

Table 19 – Assumptions

5.6 SAFETY RESPONSIBILITIES

The following chapter provides an overview for the safety related responsibilities of MBS and its adjacent systems (MBD components).

Legend of the following table:

ID … a unique identifier

Name … a description of the safety responsibilities

ID SLC … a list of system level constraints associated with this safety responsibility

5.6.1 Moving Block System (MBS)

The responsibilities of MBS essentially comprise the following areas:

- Assess risk of commands for trains and infrastructure elements. Reject commands, which will result in an unsafe situation. Forward or process safety-validated commands.
- Intervention if risk of railway accidents is not tolerable (e.g., point in reservation area loses its end position, train moving too fast, runaway trains, …).
- Safe communication with trains and field elements
- Provide an up-to-date, reliable and consistent system view of trains, infrastructure and other relevant parties (e.g., level crossings)

They are described in more detail below:

ID	Name	ID SLC
Collision Avoidance:		[SC-1, SC-2]
[Resp-MBS-1]	Calculate the intersection of the area of movement permissions requested by the PE with other areas reserved for train movements (and the area of trains itself). Movement permissions which intersect or have insufficient distance shall be rejected.	[SC-1.1]
[Resp-MBS-2]	Provide speed restrictions, gradients and national values defined by the IM to the OBU.	[SC-1.2, SC-3.3]
[Resp-MBS-3]	Provide adhesion factor profile based on information of the operator, automatic detection (e.g. WSP) or weather forecast.	[SC-1.3]

ID	Name	ID SLC
[Resp-MBS-4]	Check the dynamically (within MBS) generated static speed profile of trains, taking into account the train properties, the utilization conditions and the national values of the infrastructure.	[SC-1.2, SC-1.4]
[Resp-MBS-5]	Verify that the safe distance between the EoA and other authorizations, trains or obstacles is big enough (depends on the mode: SR, OS, FS).	[SC-1.4, SC-3.3]
[Resp-MBS-6]	Verify that the max permitted distance for a train that runs in SR mode is clear of other authorizations, trains or obstacles.	[SC-1.4]
[Resp-MBS-7]	Check the location (and speed) reported by the trains and provide emergency stop command to the OBU, if the probability for leaving the reservation area is too high (or the permitted speed is violated).	[SC-1.5, SC-3.3]
[Resp-MBS-8]	Monitor location/speed reported by trains and in case that they will probably leave the area reserved for their movement protect and warn the affected environment.	[SC-1.5]
[Resp-MBS-9]	Supervise required point positions (in areas reserved for movement) and in case a point loses its end position and perform safety reaction.	[SC-1.6]
[Resp-MBS-10]	Support checking the infrastructure after maintenance (e.g., allowing the first train only to pass in OS mode after track maintenance).	[SC-1.7]
[Resp-MBS-11]	Prohibit usage of malfunctioning infrastructure elements (e.g., set a usage restriction for a malfunctioning point reported by a train driver to the operator).	[SC-1.7]
[Resp-MBS-12]	Detect malfunctioning infrastructure elements (e.g., train takes wrong direction passing a point) and report those to the operator.	[SC-1.7]
[Resp-MBS-13]	Check and monitor that level crossing in areas reserved for train movement are secured in a timely manner.	[SC-2.1]
[Resp-MBS-14]	Check that the speed of trains passing over not completely secured level crossings is not too high. Note: this restriction is already part of the static speed profile of movement permissions.	[SC-2.2, SC-5]
[Resp-MBS-15]	If obstacles are detected on a level crossing that is/was secured for train movement perform safety reaction.	[SC-2.3]

ID	Name	ID SLC
[Resp-MBS-16]	Register/remove warning areas for construction sites (including location on the tracks) reported by the railway worker warning systems.	[SC-2.4]
[Resp-MBS-17]	Check that the warning system for railway workers is activated in a timely manner, in case a train is approaching the warning area.	[SC-2.4]
[Resp-MBS-18]	Check that the speed of trains passing construction sites is not too high (e.g. TSR, This is part of the static speed profile of movement permissions and depends on the distance of the train to the railway workers).	[SC-2.5, SC-5]
[Resp-MBS-19]	If construction trains or other obstacles occupy the tracks of a construction site perform safety reaction.	[SC-2.6]
[Resp-MBS-21]	Warn the operator if runaway trains or other obstacles are detected.	[SC-2.7, SC-6.2]
[Resp-MBS-22]	Supervise secured state of level crossings (in areas reserved for movement) and perform safety reaction in case the level crossing loses its secured state.	[SC-2.1]
[Resp-MBS-23]	Report level crossings which are behind areas reserved for movements and did not open in reasonable time to the operator.	[SC-2.8]
[Resp-MBS-45]	Increase train location accuracy by combining train position reports with TTD occupancy information.	[SC-1, SC-2]
Communication with trackside infrastructure elements:		[SC-1, SC-2]
[Resp-MBS-46]	Receive the current position of all railway points.	[SC-1, SC-2]
[Resp-MBS-47]	Command the throw over a railway point.	[SC-1, SC-2]
[Resp-MBS-48]	Receive the current occupancy status of all trackside train detection systems (TTDs).	[SC-1, SC-2]
[Resp-MBS-49]	Receive the current status of all level crossings.	[SC-1, SC-2]
[Resp-MBS-50]	Command the opening/closing of level crossings.	[SC-1, SC-2]
Train Handover with neighbouring regions:		[SC-1, SC-2]
[Resp-MBS-39]	When a train approaches the border of the controlled region, inform the neighbouring system (MBS or interlocking (N-IXL)) and perform a handover.	[SC-1.1]
[Resp-MBS-40]	When a train approaches the border of the controlled region, inform the neighbouring system (MBS or RBC (N-RBC)) and perform a handover.	[SC-1.1]

ID	Name	ID SLC
[Resp-MBS-41]	Continue monitoring the train until its rear end has left the arear of control .	[SC-1.1, SC-2]
[Resp-MBS-42]	When an N-RBC announces a train entering the controlled region, check that the risk of the new train is acceptable and – if so – accept the handover from the N-RBC.	[SC-1.1]
[Resp-MBS-43]	When an N-IXL announces a train entering the controlled region, check that the risk of the new train is acceptable and – if so – accept the handover from the N-IXL.	[SC-1.1]
[Resp-MBS-44]	Start supervision of the train once it has entered the controlled region.	[SC-1.1, SC-2]
Clearance Gauge - Derailment:		[SC-3]
[Resp-MBS-24]	Before authorizing a movement permission for a train, check if the infrastructure properties are compatible with the properties of the train.	[SC-3.1]
[Resp-MBS-25]	Check the consistency of train properties reported by the train itself and provided by the DR/TMS/Operator.	[SC-3.1]
[Resp-MBS-26]	Before authorizing a movement permission for a train, verify if the utilization conditions are respected by the movement permission.	[SC-3.2, SC-5]
[Resp-MBS-27]	If utilization conditions for a requested movement permission are violated, the movement permission shall not be authorized.	[SC-3.3]
[Resp-MBS-29]	If a violation of utilization conditions (e.g., violation of the clearance gauge, hot box, hot wheel, fire on board, derailed axle, …) is reported perform safety reaction.	[SC-3.4]
Unsafe Regions:		[SC-7]
[Resp-MBS-32]	Inform the operator about conditions of regions which prevent a safe passage of trains.	[SC-7.1]
[Resp-MBS-33]	If movement permissions are requested which enter unsafe regions, this movement permissions shall not be authorized.	[SC-7.1]
[Resp-MBS-34]	If conditions of unsafe regions are detected in the area reserved for train movement perform safety reaction.	[SC-7.1]
[Resp-MBS-35]	Ensure that the risk of reversing trains entering emergency propelling areas is tolerable.	[SC-7.2]
Utilization Conditions:		[SC-8]
[Resp-MBS-37]	Before new topography data is used for production, plausibility checks (topological properties, e.g., like	[SC-8.1]

ID	Name	ID SLC
	connectivity) shall be performed. May be delegated to a different controller.	
[Resp-MBS-38]	Temporary changes in utilization conditions of infrastructure elements shall be taken into account when assessing whether a risk is tolerable.	[SC-8.2]

Table 20 – Moving Block System Safety Responibilities

5.6.2 Infrastructure Manager (IM)

The infrastructure manager is responsible for providing a production plan containing the journey timetable. He is also responsible to provide a description of the topology, topography and infrastructure (including axle load, track gauge, clearance gauge, traction system, etc.). The quality of the topography description shall be such that safety-critical decisions can be based on it. This includes guaranteed limits for accuracy and specifying confidence intervals for numerical values. In addition, changes (temporary or permanent) of the topography description shall be provided to the system in a timely manner. This includes emergency measures and other interventions from the operation personnel.

ID	Name	ID SLC
Collision Avoidance:		[SC-1, SC-2]
[Resp-IM-1]	Provide national values which are compliant with the requirements of static risk assessment.	[SC-1.2, SC-4.1]
[Resp-IM-2]	Instructions for operators and drivers concerning low adhesion factor conditions.	[SC-1.3]
Clearance Gauge - Derailment:		[SC-1.2, SC-4.1]
[Resp-IM-3]	Provide topography, topology, configuration- and infrastructure data. (e.g. axle load, track gauge, clearance gauge, traction system, static speed profile, etc.).	[SC-3.1, SC-4.3, SC-5]
Utilization Conditions:		
[Resp-IM-5]	The quality of data from [Resp-IM-3] shall be such that safety-critical decisions can be based on it. This includes guaranteed limits for accuracy and specifying confidence intervals for numerical values.	[SC-1.3]
[Resp-IM-6]	Changes (temporary or permanent) of the topography description shall be provided to the system in a timely manner.	[SC-8.1, SC-8.2]

Table 21 – Infrastructure Manager Safety Responibilities

5.6.3 Operator

Concerning the operator, we reiterate two important assumptions here:

- interaction between the operator and MBS only involves safety related information [ASM-22]
- other interactions of the operator with the system are done via the PE or the TMS [ASM-23]

The reason for these assumptions is that the PE and TMS implement the operational processes and MBS acts as a gatekeeper that monitors if the risk is tolerable and forwards safe commands/authorities.

ID	Name	ID SLC
Collision Avoidance:		[SC-1, SC-2]
[Resp-OP-1]	Inform Train about track conditions lowering the adhesion factor.	[SC-1.3]
[Resp-OP-2]	Setup/Revoke areas with low adhesion factor.	[SC-1.3]
[Resp-OP-3]	Setup/remove usage restriction areas for malfunctioning infrastructure elements (e.g., set a “Befahrbarkeitssperre” for a malfunctioning point reported by a train driver).	[SC-1.7]
[Resp-OP-4]	Setup/remove warning areas for construction sites (together with the Picop and provide further information of warning time, max allowed speed, …).	[SC-2.4, SC-2.5, SC-5]
[Resp-OP-5]	Inform MBS about runaway trains, including location on the tracks (and their assumed direction and speed).	[SC-2.7]
Clearance Gauge - Derailment:		[SC-3]
[Resp-OP-6]	Optionally provide missing train properties.	[SC-3.1]
Unsafe Regions:		[SC-7]
[Resp-OP-8]	Inform MBS about conditions of regions, which prohibit a safe passage of trains.	[SC-7.1]
[Resp-OP-9]	Prepare emergency propelling areas for reversing trains in unsafe regions.	[SC-7.2]
[Resp-OP-10]	Command trains to leave unsafe regions.	[SC-7.2]
Utilization Conditions:		[SC-8]
[Resp-OP-11]	Inform MBS about temporary changed utilization conditions of infrastructure elements.	[SC-8.2]

Table 22 – Operator Safety Responibilities

5.6.4 Driver

The train driver is responsible for operating the train, this includes e.g.,

- start up the train, perform brake test
- monitor OBU and train status
- selection of the ETCS operation mode
- control traction and brakes
- manually control the train in on-sight mode and decide the speed according to the dispatching orders from the dispatcher
- report emergency information
- take into account journey information from dispatcher to keep the train safe
- provide information to dispatcher when requested to do so
- enter validated train data (i.e., train length)

ID	Name	ID SLC
Collision Avoidance:		[SC-1, SC-2]
[Resp-DRV-1]	Inform Operator about track conditions lowering the adhesion factor.	[SC-1.3]
[Resp-DRV-2]	Adjust adhesion factor manually.	[SC-1.3]
[Resp-DRV-3]	Decelerate train to respect the permitted speed and distance to run.	[SC-1.4, SC-1.5, SC-5]
[Resp-DRV-4]	Report malfunctioning infrastructure elements, when checking is required (e.g., checking point position in OS mode).	[SC-1.7]
[Resp-DRV-5]	Check if the level crossing is free and warn other level crossing users. EB if tracks occupied by obstacles or level crossing users.	[SC-2.2, SC-2.3]
[Resp-DRV-6]	EB if construction site is occupied by railway workers, construction trains or other obstacles.	[SC-2.6]
[Resp-DRV-x]	Check that the track is clear/free (TAF), if required.	[SC-1]
Clearance Gauge - Derailment:		[SC-3]
[Resp-DRV-7]	Enter the correct train properties (validated train data).	[SC-3.1, SC-8.1]
High Forces:		[SC-4, SC-5, SC-6]
[Resp-DRV-8]	Coupling of trains shall be done at a speed so that the risk of passenger injury is acceptable.	[SC-4.2]

ID	Name	ID SLC
[Resp-DRV-10]	If loss of dangerous goods is detected, this shall be reported to the operator.	[SC-6.2]
[Resp-DRV-11]	If a damage of the train frame is apparent, this shall be reported to the operator.	[SC-6.3]
Unsafe Regions:		[SC-7]
[Resp-DRV-12]	Report conditions which prohibit a safe passage of trains.	[SC-7.1]
[Resp-DRV-13]	If leaving unsafe regions, keep the train movement inside the received distance to run.	[SC-7.2]

Table 23 – Driver Safety Responibilities

5.6.5 On Board Unit (OBU)

The DMI displays to the Driver the current allowed movement authority by using cab signaling (if not an ATO train). The OBU also supervises the speed and ensures that the train does not violate its movement authority. Further it will send the current position as a "train position report" to the MBS.

ID	Name	ID SLC
Collision Avoidance		
[Resp-OBU-1]	Calculation of the dynamic speed profile, taking into account the running/braking characteristics of the train and the track conditions/adhesion factor (specified in the UNISIG-26)	[SC-1.2, SC-1.3, SC-1.4, SC-5]
[Resp-OBU-2]	Trip the train, if train speed exceeds the permitted speed/ceiling speed or authority is overrun (distance)	[SC-1.2, SC-1.4, SC-1.5]
[Resp-OBU-3]	Cab signalling - display train speed, permitted speed, target distance, target speed to the driver	[SC-1.4, SC-1.5, SC-5]
[Resp-OBU-4]	Supervise movement against running in the direction opposite to the train orientation (reverse movement protection)	[SC-1.5]
[Resp-OBU-5]	Trip the train (apply emergency brake) if commanded by MBS	[SC-1.5, SC-1.6, SC-2.3, SC-2.6, SC-2.7]
[Resp-OBU-6]	Inform the driver when OS mode entered and request an acknowledgement from the driver	[SC-1.7]
[Resp-OBU-7]	Inform the driver when approaching a level crossing	[SC-2.2, SC-2.3]

Clearance Gauge - Derailment		
[Resp-OBU-8]	Provide the train properties (validated train data)	[SC-3.1, SC-8.1]
[Resp-OBU-9]	Periodically send position reports (interval parameters requested/configured by the track-side or national values; including position, direction, speed and the accurracy of this values)	[SC-3.3]
High Forces		
[Resp-OBU-10]	The driver shall be supported in coupling activities so that the risk of passenger injury is acceptable. (e.g. measure distance, display it and issue distance warnings)	[SC-4.2]
Unsafe Regions		
[Resp-OBU-11]	Supervise movement in reversing mode (distance and ceiling speed)	[SC-7.2]
Utilization Conditions		
[Resp-OBU-12]	Provide and check the system version	[SC-8.1]

Table 24 – On Board Unit Safety Responibilities

5.6.6 Maintenance workers

The maintenance workers are responsible for the upkeep of the infrastructure. They perform scheduled maintenance work as well as on-demand maintenance when infrastructure elements fail or report abnormal behavior.

ID	Name	ID SLC
Unsafe Regions:		[SC-7]
[Resp-MNT-1]	Inform operator of conditions of infrastructure elements on-site.	[SC-7.1]
[Resp-MNT-2]	Determine on-site whether train passage over infrastructure element is safe.	[SC-7.1, SC-1.6]
[Resp-MNT-3]	Repair damaged infrastructure elements and restore drivability of such elements.	[SC-7.1]

Table 25 – Maintenance Workers Safety Responibilities

5.6.7 Digital Register

The Digital Register (DR) is responsible for the compilation, versioning, validation and distribution of topology, topography, infrastructure- and configuration data.

ID	Name	ID SLC
Utilization Conditions:		[SC-7, SC-8]
[Resp-DR-1]	Validates that the topology and topography data is consistent with physical reality.	[SC-8.1]
[Resp-DR-2]	Verifies that the topology and topography data meet the data engineering and validation rules.	[SC-7.1, SC-8.1]
[Resp-DR-3]	Provides validated topology and topography data to PE, MBS and OBU relevant for their region of control.	[SC-8.1]
[Resp-DR-4]	Ensures synchronized activation of new data versions in PE, MBS and OBU.	[SC-7.1, SC-8.2]

Table 26 – Digital Register Safety Responibilities

5.7 CONTROL LOOP ANALYSIS

In the following, relevant control and feedback loops are considered across the most important interfaces. Later in the analysis, these can be explored in greater depth or the respective systems can be broken down into smaller controllers/actors.

A subset of the unsafe control actions was selected for further scenario generation. This was done due to the focus on changes system design, where the behavior of the moving block system differs from traditional fixed block systems.

Legend of the following tables:

Controllers …	modules involved in this analysis
Control Actions …	list of possible control actions to the controlled item
Feedbacks …	list of possible feedbacks from the controlled item
Process Model …	controlled process that fulfils a defined action
Control Algorithm …	a defined function that controls the process
Remarks …	a comment field for additional optional comments or remarks
[UCA-] ...	unsafe control action
[SDR-] ...	safety design recommendation

5.7.1 I_OP Interface

Operator Panel <-> MBS

Controllers	• Operator Panel: • MBS:

Control Actions:	• OP -> MBS:
	  ○ Set known infrastructure state
	  ○ Setup/revoke temporary Usage Restriction Area
	  ○ Emergency Text Messages to Driver (seldomly used)
	  ○ Conditional/Unconditional emergency Stop
	  ○ Command confirmation (command dependent)
	  ○ Setup/revoke warning areas for construction sites

Feedbacks:	• MBS -> OP:
	  ○ Command Received/Rejected
	  ○ Safety/Operational implications
	  ○ Request command confirmation (command dependent)
	  ○ Operation Succeeded/Failed + Reason

	○ Operational State
Process Model	• MBS ○ Operational State • OP ○ Panel: Request state/Command state ○ Operator: TMS/PE System View / Operational knowledge / Real world knowledge
Control Algorithm	• MBS ○ Semantic/Syntactic command check ○ Determine safety implications ○ Confirmation loop (command dependent) ○ Forward command and/or update known infrastructure state. ○ Provide feedback • OP ○ Operational Rules ○ Operational state from MBS ○ Known state of real world from other sources ○ Mental model of command implications.
Remarks	Operator shall be able to conduct temporary safety related interventions and enact temporary infrastructure restrictions. Only safety related commands are considered via the I_OP interface. Non-critical/standard commands can be sent via PE and subsequently I_PE.

Unsafe Control Actions:

	Hazardous when		
Control action	**Provided**	**Not Provided**	**Provided too late/early**
Set known infrastructure state	UCA-OP-1: Operator provides known infrastructure state when set state does not match reality [H1, H2]	UCA-OP-2: Operator does not provide a known infrastructure state when that known state is worse in reality than the operational state of MBS [H-8.1, H-8.3]	UCA-OP-3: Operator provides a known infrastructure state too late when that state is worse in reality than the operational state of MBS [H-8.1, H-8.3]

Setup/revoke temporary Usage Restriction Area	UCA-OP-4: Operator provides temporary usage restriction when usage restriction has excessive limits (too high-speed limit) [H-8.1, H-8.2] UCA-OP-5: Operator provides revocation of temporary usage restriction area when the usage restriction should still be applied [H-8.1, H-8.2]	UCA-OP-6: Operator does not provide temporary usage restriction area when conditions (for this area) are worse than depicted in the operational state of MBS [H-8.1, H-8.2]	UCA-OP-7: Operator provides temporary usage restriction area too late where conditions are worse than depicted in the operational state of MBS [H-8.1, H-8.2] UCA-OP-26: Operator provides revocation of temporary usage restriction area too early when the usage restriction should still be applied [H-8.1, H-8.2]
Conditional/Unconditional emergency Stop	UCA-OP-14: Operator provides emergency stop command for wrong train [H-4.1] UCA-OP-15: Operator provides conditional emergency stop command with wrong stopping position [H-1, H-2] UCA-OP-16: Operator provides conditional emergency stop command where an unconditional emergency stop command is required [H-1, H-2]	UCA-OP-17: Operator does not provide safety related conditional/unconditional emergency stop [H-1, H-2]	UCA-OP-18: Operator provides safety related conditional/unconditional emergency stop too late [H-1, H-2]
Command confirmation (command dependent)	UCA-OP-19: Operator provides command confirmation for the wrong train/	UCA-OP-21: Operator does not provide command confirmation (any of the unsafe	UCA-OP-22: Operator provides command confirmation too late (any of the unsafe

	infrastructure element / message [H1, H2, H7, H8] UCA-OP-20: Operator provides command confirmation without consideration of safety implications for other trains [H1, H2, H7, H8]	actions above) [H1, H2, H7, H8]	actions above) [H1, H2, H7, H8]
Setup/revoke warning areas for construction sites	UCA-OP-23: Operator provides command to revoke warning are for construction site when the railway workers are still on site. [H-5]	UCA-OP-24: Operator does not provide setup command for area of construction site before the construction begins. [H-5]	UCA-OP-25: Operator provides command to revoke warning are for construction site to early when the railway workers are still on site. [H-5]

Scenarios for unsafe control actions:

[S1-UCA-OP-1]: Two railway points P1 and P2 report a lost end position and are unable to execute throwover commands by the operator. As the railway points are within close proximity, a single maintenance team is dispatched to investigate the two points. The maintenance team is able to fix the position of P1 and reports work completed this to the Operator. The operator mistakenly believes the team also fixed the position of point P2, which the team was also tasked to investigate. As a result, the operator provides an infrastructure state not matching reality to MBS [UCA-OP-1]

=> [SDR-1]: Provide an operational rule set which explicitly determines to which infrastructure item a completed (safety related) intervention refers/referred to.

[S2-UCA-OP-2]: When passing a protected level crossing, the train driver notices that the bars on one side are not fully closed and reports this to the operator. As this particular level crossing had problems in the past, the operator mistakenly believes that this was already entered into the operator panel. As a result, a required URA is not applied to the MA [UCA-OP-2].

=> [SDR-2]: When changes to the operational state are reported by personnel, the operator shall always check if they are already entered in the operation state of MBS, even if the operator believes this has already been done in the past
=> [SDR-3]: The operator panel shall provide easily accessible information on all currently manually entered infrastructure state with the required confidence for a safety related function.

[S3-UCA-OP-3]: A construction team is in the field upgrading multiple railway points. The construction is scheduled sequentially so that the impact on the railway traffic is minimized. Due to unforeseen problems on site, the construction order of the points is switched and this is reported to the operator. As the operators shift ends shortly and the change only affects the next shift, he leaves a note for the next shift. When the next shift starts, an operational disturbance keeps the operator

busy. As a result, the note concerning the construction schedule is read only after construction has already begun and the operator reports the known operational state to MBS too late [UCA-OP-3]

=> [SDR-4]: The interface for the operator shall allow to pre-schedule usage restriction areas.
=> [SDR-5]: The operator shift handover shall include either an operational process or digital means that prevent a loss of (safety related) information during the handover.

[S4-UCA-OP-4]: Due to construction work, a temporary usage restriction area with a speed reduction shall be established. When entering the speed restriction, the operator makes a typo leading to a usage restriction area with an excessive speed limit [UCA-OP-4].

=> [SDR-6]: The operator panel should implement procedures to verify the entered usage restriction data, before the entered data is passed to the MBS system.

[S5-UCA-OP-5]: A maintenance team performs work on two tracks T1 and T2 closely located to each other. When the team reports that it has completed its work for T1, the operator mistakenly believes that the work on both tracks has been completed. As a result, the operator revokes the usage restriction area for T1 and T2 when it still should be applied for T2 [UCA-OP-5].

=> See [SDR-1] and [SDR-3]

[S6-UCA-OP-6]: The operator receives a report from a train driver that there are leaves on the track reducing braking performance. The operator knows a corresponding usage restriction has already been entered by the previous shift. However, this usage restriction has since expired. The operator mistakenly believes the usage restriction is still applied and as a result does not provide the usage restriction to the operational state of MBS as needed [UCA-OP-6].

=> See [SDR-2] and [SDR-3]

[S7-UCA-OP-7]: An operational disturbance requires the operator to manually manage a large number of trains. As the timetable should be upheld as much as possible, the operator is under time pressure. In this situation a construction team reports that it will begin constructions on track T1 in half an hour. The operator takes note and is immediately occupied with train management again. Due to time pressure, the operator only follows up on the note after the construction has already begun. As a result, the operator provides the usage restriction area for the construction site too late to MBS [UCA-OP-7].

=> [SDR-7]: Entering usage restriction areas shall take priority over the regular management of running trains
=> see also [SDR-4]

[S8-UCA-OP-26]: The operator receives a report from the construction team that construction will be completed in half an hour. However, unforeseen difficulties on the construction site cause the operation to take longer. Emerged in their work the construction team does not report this delay to the operator. The operator mistakenly believes that the team has finished their work as planned and revokes the usage restriction area too early [UCA-OP-26].

=> [SDR-8]: The operator shall always verify with the construction team on site that the work has actually been completed before removing the corresponding usage restriction area.

[S9-UCA-OP-14/17/18]: Similar reasoning to [S7-UCA-OP-9] (handling of commands under time pressure, selecting the wrong train) [UCA-OP-14, UCA-OP-17, UCA-OP-18]

[S10-UCA-OP-15]: The Operator wants to stop a train before a danger point. The interface requires that the operator enters the stopping position manually. While entering the stopping position, the operator makes a typo. As a result, the operator provides a conditional emergency stop command with the wrong position. As the train has already passed this position, the command is ignored by the OBU [UCA-OP-15].

=> [SDR-9]: The operator panel shall be designed to support the operator with contextual information when executing operator commands. I.e. the operator shall be able to select the stopping position based on an interface with information about the physical elements/trackside assets and select a stopping position based on the physical elements position.

[S11-UCA-OP-16]: The operator receives information that part of a track has become unexpectedly occupied. A train currently has a valid MA over the obstructed portion of the track. The operator believes the train is still at a large distance from the obstructed portion and issues a conditional emergency stop. However, the train position report was outdated and the train is already past the stopping position for the conditional emergency stop. As a result, the operator fails to provide the required unconditional emergency stop command. [UCA-OP-16]

=> [SDR-10]: The operator shall receive a (visual) indication about the reported train position age. (e.g., information outdated longer than for a defined threshold should be indicated).

[S12-UCA-OP-19/20/21/22]: Similar to [S5-UCA-OP-5] and [S5-UCA-OP-7]. [UCA-OP-19, UCA-OP-20, UCA-OP-21, UCA-OP-22]

[S13-UCA-OP-23]: Similar to [S1-UCA-OP-1] and [S1-UCA-OP-5]. [UCA-OP-23]

[S14-UCA-OP-24]: Similar to [S6-UCA-OP-6]. [UCA-OP-24]

[S15-UCA-OP-25]: Similar to [S8-UCA-OP-26]. [UCA-OP-25]

5.7.2 I_OBU Interface

MBS -> OBU

Controllers	• MBS • OBU
Control Actions:	• MBS -> OBU:[1] ○ Configuration Values (National values) ○ SR Authorization (distance) ○ FS/OS Movement Authority ○ Conditional/Unconditional Emergency Stop (CES/UES) ○ Shorten MA
Feedbacks:	• OBU -> MBS:[2] ○ MA Request ○ Train Position Report ○ Validated Train Data ○ Acknowledge CES
Process Model	• OBU ○ Static and dynamic properties of train ○ Current train position (including uncertainties) ○ Current train speed ○ ETCS mode ○ Train Data (train length, running number, etc.) • MBS ○ Operational state ▪ Reported train location ▪ Reported track occupations ▪ Granted MAs ○ Infrastructure state ▪ Topography and geometry ▪ State of infrastructure elements ▪ Utilization conditions

[1] Subset-026 ch.8.7

[2] Subset-026 ch.8.6

	▪ Temporary speed restrictions ○ National Values
Control Algorithm	• OBU ○ Supervise train braking curve ○ Supervise train speed ○ Service break ○ Emergency break • MBS ○ Safety Logic before granting MA ○ Command conditional/unconditional emergency stop ○ Updating operational state expanded process model ○ Handover to neighboring systems

Unsafe Control Actions:

	Hazardous when		
Control action	**Provided**	**Not Provided**	**Provided too late/early**
Configuration Values (National values)	[UCA-MBS-6] MBS provides national values to OBU when these values are not conforming to the risk analysis [H-1.1, H-2.1, H-8.1]	[UCA-MBS-1] MBS does not provide national values to OBU when these values are more restrictive than default values [H-1.1, H-2.1, H-8.1] [UCA-MBS-2] MBS does not provide temporary speed restrictions to the OBU [H-2.6, H-5, H-8.3] [UCA-MBS-3] MBS does not provide track gradients to the OBU [H-1.1, H-2.1]	

		[UCA-MBS-4] MBS does not provide inhibition of defined type of brake to the OBU [H-1.1, H-2.1] [UCA-MBS-5] MBS does not provide the adhesion factor to the OBU when the adhesion conditions are worse than normal [H-1.1, H-2.1]	
FS/OS Movement Authority	[UCA-MBS-7] MBS provides MA to the OBU when train type/properties are not compatible to infrastructure [H-3.1, H-8.2] [UCA-MBS-8] MBS provides MA to the OBU when the MA is intersecting a reservation area of another train [H-1]. [UCA-MBS-9] MBS provides MA to the OBU when the MA has a too small safety distance to other potential obstacles [H-1.1, H-2.1, H-3.1] [UCA-MBS-10] MBS provides FS/OS MA		[UCA-MBS-18] MBS provides MA too early for OBU when not all infrastructure elements along the MA are secured and passable for the train movement [H-1.4, H-2.4, H-3.3]

	to the OBU and not all infrastructure elements (points, level crossings, etc.) are prepared and secured for the running path of the train [H-1.4, H-2.4, H-3.3] [UCA-MBS-11] MBS provides FS MA passing over a not completely secured level-crossing [H-2.5, H-5] [UCA-MBS-12] MBS provides MA to OBU when the MA is directing into an unsafe area [H-7]. [UCA-MBS-13] MBS provides FS MA to OBU when coupling trains [H-4.2] [UCA-MBS-14] MBS provides MA to OBU when the MA speed profile exceeds the most restrictive speed profile for this train given the running path [H-4.3, H-8.1] [UCA-MBS-15] MBS provides MA to OBU when the MA is ending within a		

	non-stopping area [H-7] [UCA-MBS-16] MBS provides FS MA to OBU when the area reserved for train is not clear of other trains or obstacles [H-1.1, H-2.1] [UCA-MBS-17] MBS provides MA to OBU when other train or obstacles have insufficient distance from the flank of the area reserved for train movement [H-1.1, H-2.1, H-2.8, H-3.1]		
SR Authorization	[UCA-MBS-19] MBS provides SR authorization with a too long permitted distance, or into the wrong direction [H-1.1, H-2.1] (Note: this is used only if the position of the train is not known)		
Conditional/Unconditional Emergency Stop (CES/UES)		[UCA-MBS-20] MBS does not provide UES to OBU when the train leaves the area reserved for its movement [H-1.2, H-2.2, H-3.1]	
Shorten MA		[UCA-MBS-21] MBS does not provide	

		shorten MA to OBU when the train is approaching a point which lost its end position or indicates the wrong position [H-1.3, H-2.3, H-3.1] [UCA-MBS-22] MBS does not provide shorten MA command, if train is approaching a level crossing which is not secured anymore [H-2.5, H-5]	

Scenarios for selected unsafe control actions:

The unsafe control actions [UCA-MBS-16] and [UCA-MBS-17] were selected, as they are closely associated with the running path protection, which may be handled differently between fixed block and moving block systems.

[S1-UCA-MBS-16] Train T1 is a train composed of two consists, T1a and T1b, with one OBU per consist. The train is initially at standstill, and both consists are unpowered and coupled and no TTDs are located at the track. The consists T1a and T1b are uncoupled while the train is powered off. The driver enters the cab of T1a, opens the desk and enters the validated train data. He mistakenly believes that T1b is still coupled and inputs the total of T1a and T1b as train length into the DMI. As the consist T1a is still integer, the TIMS reports integrity confirmed. When PE requests an MA for T1a from MBS, MBS mistakenly believes that a train with a length of T1 is moved, while in reality train T1b is still standing on the tracks. As a result, after releasing the MA behind T1a, MBS grants another train T2 a MA into the region where T1b is still standing, leading to a collision [UCA-MBS-16]

=> [SDR-11]: MBS shall always be aware when a change of train length is expected (i.e. due to splitting and joining).

[S2-UCA-MBS-16] Train T1 with length LEN1 is initially at standstill and located on track TR1. T1 is not equipped with a functioning TIMS and no TTDs are available for TR1. The driver opens the desk and enters the validated train data. Due to operational changes, additional cars have been added to the train. The driver enters a too short train length LEN2, because he is not aware that the train is longer than during normal operations. As he is already behind schedule and there are visual obstructions blocking his view to the end of the train, the driver confirms the train integrity without seeing the last train cars. Therefore, MBS mistakenly believes T1 has length LEN2, which is shorter than the real train length LEN1, and grants an MA to T1 based on LEN2. As a result, after releasing the MA behind T1, MBS grants another train T2 a MA into the region where T1 is still standing, leading to a collision [UCA-MBS-16]

=> [SDR-12]: If MBS is aware of the expected train length (i.e. by transmitting the expected train length together with the train running number from the PE) it shall compare the expected train length with the reported train length in the validated train data and require addition confirmation if the two lengths differ.

[S3-UCA-MBS-16] Train T1 is initially at parked and located at L1, near the bottom of a valley. The train is powered down and no TTDs are available for this section of the track. After applying the parking brakes, the railway personal does not add the brake shoes below the wheels. Therefore, after the air pressure is no longer sufficient to keep the train at standstill, T1 starts to move towards the bottom of the valley and is now located at L2. MBS mistakenly believes that T1 is still located at its last known location L1. As a result, MBS grants another train T2 a MA into L2, leading to a collision [UCA-MBS-16]

=> [SDR-13]: In regions where the parking of vehicles is expected, methods for detecting the presence of trains independent of train position reports shall be available (i.e. installing TTDs in these regions)

[S4-UCA-MBS-16] Train T1 is initially at standstill and located at L1. T1 is in no power mode and no TTDs are available. The driver opens the desk and enters the validated train data. The OBU does not know the current train position. The driver therefore tells the operator the train position, and requests a staff responsible movement authorization. However, as the driver cannot see the track kilometer board due to visual obstructions, he mistakenly reports the wrong train position L2 to the operator. The operator permits a train movement based on a L2, while the train is in reality located at L1. As a result, MBS grants another train T2 a MA into L1, leading to a collision [UCA-MBS-16]

=> [SDR-14]: When moving a train based on a train position transmitted by the driver, the operator shall perform additional validity checks from a second source (i.e. planned start location of the train) before granting a SR authorization.

[S5-UCA-MBS-16]: Light Maintenance vehicle M1 is powered off and located at L1 on track TR1. TR1 is equipped with a track circuit TTD1, which is unable to detect the maintenance vehicle M1. At MBS initialization, TTD1 is reported as clear. Therefore, MBS is unaware of the presence of M1 at L1. As a result, MBS grants another train T1 a MA into L1, leading to a collision [UCA-MBS-16]

=> [SDR-15]: When the presence of maintenance vehicles is expected, track circuits alone should not be sufficient to clear the track, if these circuits can miss occupations by some vehicle types (i.e. light maintenance vehicles). Note: This may adversely impact operational performance at system startup or when clearing areas previously occupied by maintenance vehicles.

[S1-UCA-MBS-17] Train T1 is at standstill and located at the left track of railway point P1. The reported train length of LEN1 or T1 is shorter than the physical train length LEN2. Therefore, MBS mistakenly assumes that T1 is outside the fouling point of P1. As a result, MBS grants another train T2 a MA over P1, leading to a flank collision between T1 and T2 [UCA-MBS-17]

=> see [SDR-12]

[S2-UCA-MBS-17] Unsupervised area UA1 is reachable via the left track of railway point P1. Train T1 is located in UA1, and neither the UA1 nor the tracks of P1 are equipped with TTDs. Due to degraded braking performance, T1 skids outside the region UA1, and beyond the fouling point of P1. As a result, MBS grants another train T2 a MA over P1, leading to a flank collision between T1 and T2 [UCA-MBS-17]

=> [SDR-16]: Between controlled region and unsupervised region, the movement of non-communicating trains shall be detectable, i.e. using TTDs, or preventable using a point/derailer (similar to [SDR-13])

[S3-UCA-MBS-17] Maintenance vehicle M1 located within worksite W1 on track TR1 and equipped with a movable crane arm. Track TR2 runs parallel to TR1. If fully extended, the crane arm of M1 can reach into the maximum permitted clearance gauge TR2. Because worksite W1 is located on TR1, MBS mistakenly believes this worksite cannot affect trains running on TR2. As a result, an MA for another train T2 running on TR2 is granted while the crane arm of M1 is extended into TR2, leading to a clearance gauge violation [UCA-MBS-17].

=> [SDR-17]: The effects of Maintenance on neighboring tracks shall be taken into account (conceptionally, e.g., as function in MBS or as additional TSR with the URA from planning data or operator input) when granting a MA.

[S4-UCA-MBS-17] Train T1 performs end of mission on side Track TR1 which is connected to the main track TR2 via point P1. Due to an operational error the train was not protected against roll-away. After some time, the pressure in the brake tanks drops and the train starts to roll toward P1. In the mean-time another MA was granted for Train T2 on the main track TR2 leading over P1. Since MBS cannot detect the unexpected occupation on P1 nor the unexpected vacancy of the TTD on T1 in time, train T1 collides with train T2 leading to a flank collision.

=> [SDR-18] Simple detection of track occupation is not sufficient to prevent flank collisions in all cases. Technical means to secure a sufficiently large vacant area before the fouling point is required.

[S5-UCA-MBS-17] A side-track TR1 is equipped with TTD and via the point P1 connected to the main track TR2. Train T1 and train T3 are both located in the same TTD are on track TR1. Both trains have performed end of mission. Due to an operational error train T1 was not secured against roll-away. After break tank pressure drops, the train T1 rolls toward P1.

=> [SDR-18]

5.7.3 I_TACS Interface

MBS <-> TACS (SCI-XX.PDI, SCI-P, SCI-LC, SCI-TDS)

Controllers	• MBS • TACS

Control Actions:	• MBS -> TACS:
	  ○ Manage PDI connection[3]
	  ○ Move point (SCI-P) [4]
	  ○ Open/close/isolate level crossing (SCI-LC)[5]

[3] Eu.Doc.93, Eu.Doc.119

[4] Eu.Doc.38, Eu.Doc.36

[5] EU.Doc.109, EU.Doc.108

	○ Reset track occupancy status (SCI-TDS)[6]
Feedbacks:	• TACS -> MBS: ○ Manage PDI connection ○ Report point state (SCI-P) ○ Report level crossing state (SCI-LC) ○ Report track occupancy state (SCI-TDS) ○ Heartbeat [RASTA Protocol]
Process Model	• MBS ○ Operational State • TACS ○ TACS configuration / parameters ○ TACS state ○ TA state
Control Algorithm	• MBS ○ Safety Logic ○ Supervise TACS heartbeat ○ Determine safety implications of commands ○ React to safety related events ○ Establish communication with TACS ○ Forward commands to OBU ○ Sensor fusion • TACS ○ Provide heartbeat ○ Compare between TACS state and TA state ○ Obstacle detection (only LC/LX) ○ Command new state (for switchable TAs) ○ Report state update (incl. timeout, degraded states and obstacles)
Remarks	Most of this is regulated in the EULYNX Specification.

[6] Eu.Doc.44

Unsafe Control Actions

	Hazardous when			
Control action	**Provided**	**Not Provided**	**Provided too late/early**	**Stopped too soon**
Manage connection				
Move point	[UCA-TACS-1] MBS provides move point command when a train is passing over [H-1.3, H-2.3, H-3.3]. [UCA-TACS-2] MBS provides move point command when the point is already reserved/locked for another train's movement [H-1.3, H-2.3] [UCA-TACS-3] MBS provides move point command to wrong direction when preparing reservation area [H-1.4, H-2.4, H-3.1, H-4.3] [UCA-TACS-4] MBS provides move point command when the new point position endangers the reservation area of other trains [H-1.4, H-2.4, H-3.1]	[UCA-TACS-5] MBS does not move point to required direction when preparing a reservation area [H-1.4, H-2.4, H-3.1]. [UCA-TACS-6] MBS does not provide move point when a runaway wagon is to be diverted [H-2.8]	[UCA-TACS-7] MBS provides move point command too late (after MA has already been sent to the train) when preparing a reservation area [H-1.4, H-2.4, H-3.1, H-3.3, H-4.3] [UCA-TACS-8] MBS provides move point command too late (after the wagon has already passed the point) when a runaway wagon is to be diverted [H-2.8]	[UCA-TACS-9] MBS stops the supervision of the moved point too soon when the point is still required for a reserved area and the point loses its end position. [H-1.3, H-2.3, H-3.1, H-3.3, H-4.3].

Open/close level-crossing	[UCA-TACS-10] MBS provides open level crossing command while the level crossing is still reserved for train movement [H-2.5] [UCA-TACS-11] MBS provides close level crossing command when the level crossing is not required for train movement [H-2.9]	[UCA-TACS-12] MBS does not provide close level crossing command when the level crossing needs to be closed for train movement [H-2.5] [UCA-TACS-13] MBS does not provide the open level crossing command when the level crossing is no longer required for train movement [H-2.9]	[UCA-TACS-14] MBS provides close level crossing command too early when a train is approaching [H-2.9]. [UCA-TACS-15] MBS provides close level crossing command too late when a train is approaching [H-2.5]. [UCA-TACS-16]: MBS provides open level crossing command too early when a train is still within the level crossing [H-2.5] [UCA-TACS-17]: MBS provides close level crossing command too late when a train is already within the level crossing [H-2.9]	[UCA-TACS-18] Supervision of closed level crossing is stopped to soon when still required for train movement [H-2.5].
Reset track occupancy state	[UCA-TACS-19] MBS provides reset track occupancy command while a train inside the track occupancy section [H-1, H-2, H-6.2]	/ Note: this may reduce availability but is not related to safety	[UCA-TACS-20] MBS provides reset track occupancy command too soon while a wagon is still inside the track	[UCA-TACS-21] MBS stops the supervision of the track occupancy state too soon while a supervision is still required for train

			occupancy section [H-1, H-2, H-6.2]	movement [H-1, H-2]

The loss scenarios for trackside assets occur together with unsafe control actions on the I_OBU interface (e.g. granting an MA) and the I_OP interface (e.g., manually reseat a TDS). Often, the state of the trackside assets constitutes the context under which control actions to the OBU or the operator panel becomes unsafe. These loss scenarios are not repeated here, as details on them are already listed in the previous section.

5.7.4 I_DR Interface

MBS <-> DR

Controllers	• DR • MBS
Control Actions:	DR -> MBS • Provide validated topology and topography data. • Provide utilization restrictions (e.g., URA) for topology change. • Activate validated data version (Note: this assumes a new data version was previously provided) • Request currently used validated data version (Note: not safety related)
Feedbacks:	MBS -> DR • Confirm data reception • Confirm/reject activation of utilization restriction • Confirm/Reject activation of new data version • Report currently used data version (Assumption: not safety related)
Process Model	• MBS ○ Current operational state (includes utilization restriction) ○ Current active data version ○ Currently inactive data versions ○ Data verification & validation signatures • DR ○ Topology and Topography data ○ Usage restrictions required for activation ○ Data verification & validation signatures
Control Algorithm	• MBS

	○ Check if received data is malformed (Note: syntactic check only) ○ Check if new data version is compatible with current operational state before activation ○ Verify data signatures ○ Verify required usage restrictions for topology change are active. • DR ○ Validate data input against physical reality (or export responsibility to other entity ->[ASM-26]) ○ Verify data against data engineering and validation rules ○ Compile data version relevant for region of control ○ Distribute data to consuming systems. ○ Activate new data version synchronously for all recipients
Remarks	-

Unsafe Control Actions

	Hazardous when			
Control action	**Provided**	**Not Provided**	**Provided too late/early**	**Stopped too soon**
Provide validated topography data	[UCA-DR-1] DR provides topography data to MBS which has not been verified. [H-8] [UCA-DR-2]: DR provides topography data to MBS which is malformed. [H-8] [UCA-DR-3]: DR provides topography data to MBS which has not been validated against physical reality. [H-8]	[UCA-DR-4] DR does not provide a new version of topography data to MBS when the infrastructure is changed (i.e. construction work) [H-8.1]	[UCA-DR-5] DR does provide a new version of topography data to MBS too late when changes to the infrastructure have already been made. [H-8.1]	[UCA-DR-6] DR does not resend new topography data to MBS if the previous transmission failed. [H-8] (e.g. not checking that the data reception was confirmed)

Activate validated data version	[UCA-DR-7] DR provides activation of a data version to MBS when the data version to activate is not contained in the inactive data versions of MBS [H-8] [UCA-DR-8] DR provides activation of a data version to MBS when the activated data version does not match physical reality [H-8] [UCA-DR-13] DR provides activation of a data version for which MBS has not activated the required usage restriction. [UCA-DR-14] DR provides activation of a data version for which MBS has activated a wrong or insufficient usage restriction.	[UCA-DR-9] DR does not provide activation of a new data version to MBS when current data version is more permissive than physical reality [H-8.3] (i.e. due to construction work)	[UCA-DR-10] DR provides activation of a data version to MBS too late when the activated data version is more restrictive than the current data version [H-8.3] (e.g. speed restriction due to construction work) [UCA-DR-11] DR provides activation of a data version to MBS too early when the activated data version is more permissive than physical reality [H-8] (e.g. raising the speed limit before infra upgrade has been completed)	[UCA-DR-12] DR does not retry activation of a data version to MBS when the previous activation was rejected. [H-8] (e.g. not checking that the activation was confirmed)

Note: this design may add new UCA to MBS (e.g. performing safety checks against inactive data versions, activating a data version which endangers trains with granted movement permissions, not activating new data version, not verifying data signature, …)

Scenarios for selected unsafe control actions:

[S1-UCA-DR-1/2] DR provides a new set of domain data to MBS which has not been verified to comply with the given engineering rules, or which is malformed in other ways. Since no further checks are applied on MBS side a data type for the configuration of railway point P1 is misinterpreted such that point position “left” actually corresponds to point position “right”. MBS then allows the movement of train T1 over point P1 leading to collision or derailment on a side track.

-> [SDR-25] DR shall include a set of verification functions that ensure that processed data follows the required engineering rules and is not malformed.

[S1-UCA-DR-3] DR provides a new set of domain data to MBS, however the distance between railway point P1 and railway point P2 in the data is longer than in reality. MBS is thus not aware that the Train T1 is actually reaching over P1 and allows P1 to be switched under T1 leading to a derailment.

-> [SDR-19] There shall be a "safety responsible" entity which is in a valid position to verify the correctness (correspondence to the physical reality) of the input data for MBS with a certainty corresponding to a SIL-4 function.

[S2-UCA-DR-3] DR provides a new set of domain data to MBS that was originally validated by a safety responsible according to [SDR-19], however the data was altered in and intermediate processing step such that the distance between railway point P1 and railway point P2 is now longer than in reality. MBS is thus not aware that the Train T1 is actually reaching over P1 and allows P1 to be switched under T1 leading to a derailment.

-> [SDR-20] MBS shall include a function that ensures that the input data (here Domain Data) received corresponds exactly to what has been verified and validated by the above (in UCA-DR-1) mentioned safety responsible (e.g. by means of a dedicated signature or safety code).

[S1-UCA-DR-4/5] Construction work to shorten a side track was scheduled for a certain date. Due to operational changes the actual construction work starts early, and a URA for work site protection is created together with the dispatcher. After the construction work is finished, the dispatcher lifts the worksite URA, although the topography and configuration data in MBS was not yet updated to reflect a shorter track. As a result, a train is authorized to enter the side track and collides with the buffer stop.

-> [SDR-21] An operational rule may be required, that ensures that any infrastructure changes have to be preceded by a (sufficiently large & restrictive) URA, and that this URA may only be lifted if the changes have been updated in the topography & configuration data of MBS.

[S1-UCA-DR-11] For some reason it was decided that domain data should be updated before the actual construction work on the tracks took place. To secure the area where track changes will occur a URA was foreseen. However, MBS was not commanded to activate this URA before the following topology/domain data update. Since MBS has no means of deciding if such a URA would have been required it activates the new domain data version right away. Subsequently. MBS allows a train to move into the site with a higher velocity than allowed for safe operation. .

=> [SDR-24] If an URA for safe activation of new set of domain data is required the domain data shall include the reference for this URA (e.g. by means of a dedicated safety code).

[S1-UCA-DR-12] As in [S1-UCA-DR-11] but MBS received a URA from a Non-SIL system where an undetected error occurred that led to the URA being wrong/too small/too unrestrictive.

=> [SDR-22] There shall be a “safety responsible” entity which is in a valid position to define a (sufficiently large & restrictive) URA which covers the area in said AoC which is about to change during the upcoming data (Domain Data) update. Again, with a certainty corresponding to a SIL-4 function.

[S2-UCA-DR-12] As in [S1-UCA-DR-12] but the undetected error occurred during transmission and led to the URA being wrong/too small/too unrestrictive.

=> [SDR-23] MBS shall include a function that ensures that the received URA corresponds exactly to what was defined by the aforementioned safety responsible (e.g. by means of a dedicated safety code).

5.7.5 I_PE Interface

MBS <-> PE

Controllers	• PE • MBS

Control Actions:	PE -> MBS
	• Connection
	  ○ Domain Data Version Check
	  ○ Synchronization Complete
	  ○ Close Connection
	• Command Change DPS state
	• Request Movement Authority
	• Revoke Movement Authority
	• Heartbeat

Feedbacks:	MBS -> PE
	• Connection
	  ○ Domain Data Version Check
	  ○ Synchronize Operational State
	  ○ Close Connection
	• Share operational state
	  ○ Report TACS State
	  ○ Report Train Object State
	• Reject command/request
	• Accept command/request
	  ○ Allow/grant command/request
	  ○ Deny command/request

Process Model	• PE
	  ○ Operational State
	  ○ Safety Logic (needs to be aware what SL will do/grant)
	  ○ Operationally synchronized timetable
	• MBS
	  ○ Operational State
	  ○ Safety Logic

Control Algorithm	• MBS
	  ○ Check command/request validity
	  ○ Check command/request safety
	  ○ Incident/Emergency Routines
	  ○ Supervise heartbeat
	• PE
	  ○ Sequence Movement Authorities according to plan
	  ○ Command changed DPS state according to plan
	  ○ Request Movement Authority according to plan
	  ○ High-level Incident/Emergency Routines/Optimization
	  ○ Provide heartbeat

Remarks	Since PE performs only functions with SIL basic integrity, all commands from PE have to be checked by MBS an associated risk to safety in order to be suitable for SIL 4 functions.

6 INTERFACE CRITICALITY

This chapter details the results of the safety analysis of the MBS safety boundary analysis and the related interfaces. The aim of this analysis is to identify safety related connections and systems relating to the MBS. The MBD shall support different modes of operation. This chapter analysis these modes for the impact to the MBS.

6.1 SYSTEM SAFETY BOUNDARY

The system boundary is given through the “system definition” from task 13.1 and was further analyzed from the safety perspective. The following figure classifies the sub systems of the MBD into safety related and non safety related controllers.

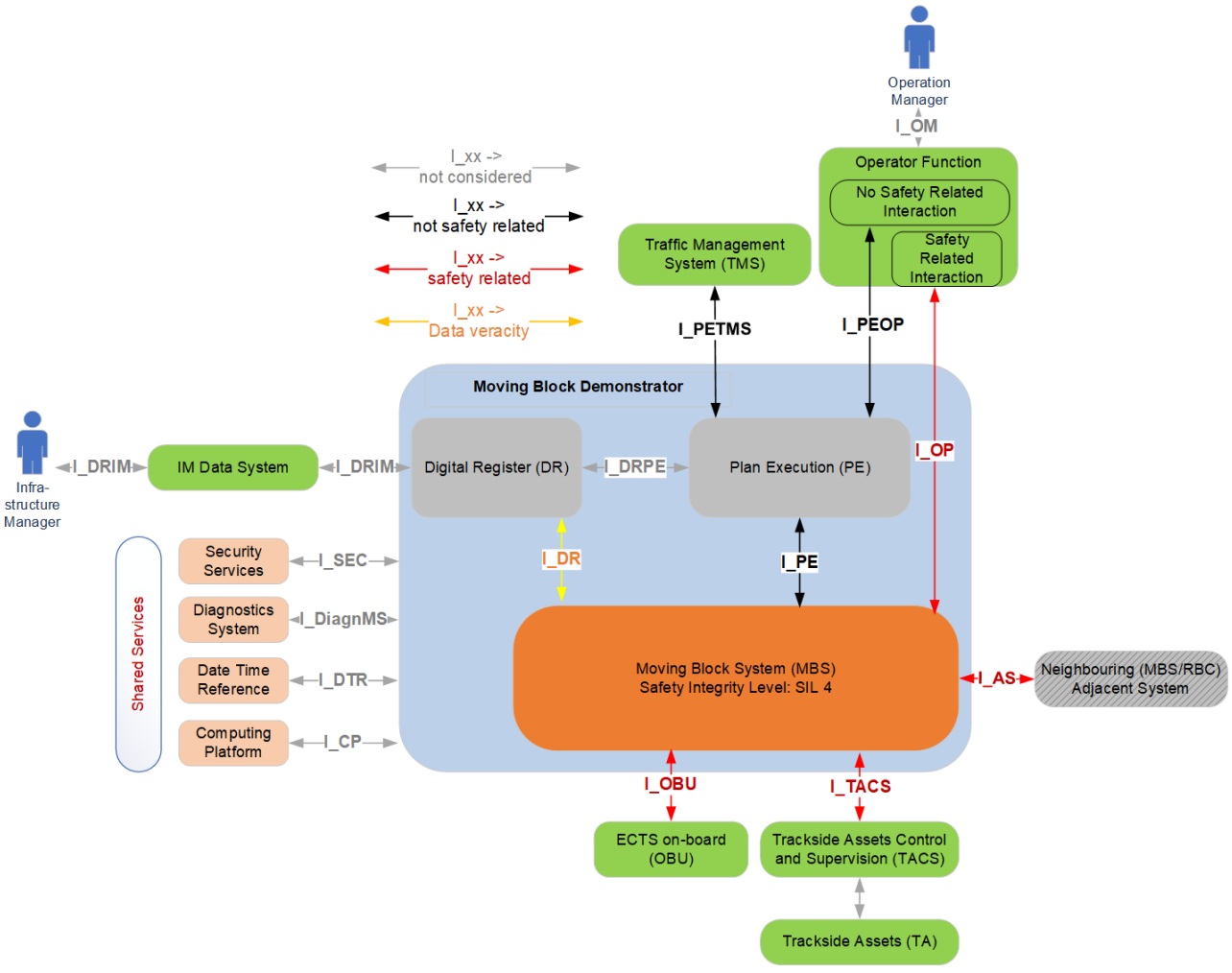


Figure 8 - MBS System Boundary and Interface Definition

6.2 INTERFACE TABLES

From the MBS module perspective, the following interfaces are analysed according to their safety relevance to determine which of the interfaces are safety related. The interfaces are further analysed about the kind of communication (unidirectional or bidirectional). This classification shall help to reduce the development effort for such kind of interfaces which are connecting the MBS to non-safety related systems.

Legend of the following table:

Interface Name … the name of the interface

Interface Description … a short description of the interface

Connection … defines both connection entities of the interface

Communication … classifies the connection into unidirectional or bidirectional

Safety related … a classification, whether the interface is safety related (Yes) or not (No)

Remarks … a comment field for additional optional comments or remarks

6.2.1 I_AS

Interface Name	**I_AS**
Interface description	This interface represents the connection between the MBS and the neighbouring systems (MBS/RBC). The communication is done according to the specification of the ERTMS/ETCS SUBSET-037 and ERTMS/ETCS SUBSET-039.
Connection	Moving Block System (MBS) <-> Neighbouring (MBS/RBC) System Adjacent System
Safety related	Yes
Remarks	MBS <-> MBS/RBC handover not in scope of this analysis.

Table 27 – I_AS Interface Definition

6.2.2 I_DR

Interface Name	**I_DR**	
Interface description	This interface represents the connection between the DR and the MBS. DR provides updates of existing and new data to the MBS by using a standardised data format.	
Connection	Digital Register (DR) <-> Moving Block System (MBS)	
Safety related	Overall system safety depends on data veracity but not e.g., on interface availability.	
Safety implication	Safety measures	Comment
Interface integrity (MBS needs information to be unmodified)	Integrity could be verified by using a data/bulk checksum.	Technical/Operational considerations required
Correctness of data (MBS needs information to represent the correct state)	Ensured through dependable external system/actor signature, e.g., if data is pre-validated.	Technical/Operational considerations required
Availability of connection (relevant for MBS safety function)	No safety related implications.	Already set / Not critical
Remarks	-	

Table 28 – I_DR Interface Definition

6.2.3 I_OBU

Interface Name	**I_OBU**	
Interface description	This interface represents the connection between the MBS and the ETCS on-board unit (OBU). The communication is done according to the specification of the ERTMS/ETCS SUBSET-026 and ERTMS/ETCS SUBSET-037.	
Connection	Moving Block System (MBS) <-> ECTS on-board (OBU)	
Safety related	Yes	
Safety implication	Safety measures	Comment
Interface integrity (MBS needs information to be unmodified)	Integrity already ensured through SS-026/SS037.	Already set / Not critical
Correctness of data (MBS needs information to represent the correct state)	Correctness already ensured through SS-026/SS037.	Already set / Not critical
Availability of connection (relevant for MBS safety function)	Monitoring of continuous connection already ensured through SS-026/SS-037.	Already set / Not critical
Remarks	-	

Table 29 – I_OBU Interface Definition

6.2.4 I_OP

Interface Name	**I_OP**	
Interface description	This interface represents the connection between the MBS and the operator position with the intend to exchange operation relevant information for SIL-2 functions (e.g.: railway point lock).	
Connection	Moving Block System (MBS) <-> Operator Position	
Safety related	Yes	
Safety implication	Safety measures	Comment
Interface integrity (MBS needs information to be unmodified)	Integrity shall be verified by using a protocol checksum.	Technical/Operational considerations required
Correctness of data (MBS needs information to represent the correct state)	Correctness shall be verified by using an appropriate protocol e.g., with a signature.	Technical/Operational considerations required
Availability of connection (relevant for MBS safety function)	The operator/role must have the means to interact/influence MBS at any time (e.g., react to safety incident). Appropriate safety reaction may be required if connection is lost.	Technical/Operational considerations required
Remarks	-	

Table 30 – I_OP Interface Definition

6.2.5 I_PE

Interface Name	**I_PE**	
Interface description	This interface represents the connection between the MBS and the PE. For the data exchange between the MBS and the PE a standardised data format is used.	
Connection	Moving Block System (MBS) <-> Plan Execution (PE)	
Safety related	No	
Safety implication	Safety measures	Comment
Interface integrity (MBS needs information to be unmodified)	Not required	Already set / Not critical
Correctness of data (MBS needs information to represent the correct state)	Not required	Already set / Not critical
Availability of connection (relevant for MBS safety function)	Not required	Already set / Not critical
Remarks	As the MBS shall reject requests from PE which can result in an unsafe system state. This interface is not considered safety related, as unsafe requests are simply rejected.	

Table 31 – I_PE Interface Definition

6.2.6 I_TACS

Interface Name	I_TACS	
Interface description	This interface represents the connection between the MBS and the Trackside Assets Control and Supervision (TACS) according to the specification of the EULYNX standards.	
Connection	Moving Block System (MBS) <-> Trackside Assets Control and Supervision (TACS)	
Safety related	Yes	
Safety implication	Safety measures	Comment
Interface integrity (MBS needs information to be unmodified)	SCI-P / SCI-TDS / SCI-LC / SCI-LX /: Integrity already ensured via RaSTA protocol.	Already set / Not critical
Correctness of data (MBS needs information to represent the correct state)	SCI-P: Ensured through external SIL4 system. SCI-TDS: We can verify the correctness through a second source	[minor] operational considerations required
Availability of connection (relevant for MBS safety function)	Monitoring of continues connection already ensured via RaSTA heartbeat.	Already set / Not critical
Remarks	-	

Table 32 – I_TACS Interface Definition

6.2.7 I_PEOP

Interface Name	I_PEOP	
Interface description	This interface represents the connection between the plan execution (PE) and the operator position with the intent to exchange operation relevant information for none safety related functions.	
Connection	Plan Execution <-> Operator Panel	
Safety related	No	
Safety implication	Safety measures	Comment
Interface integrity	Integrity shall be verified by using a protocol checksum.	-
Correctness of data	No safety related implications.	-
Availability of connection	No safety related implications.	-
Remarks	Not further assessed, as it is assumed, that the data input is correct and completely provided and this interface has no direct communication to the MBS system.	

Table 33 – I_PEOP Interface Definition

6.2.8 I_PETMS

Interface Name	I_PETMS	
Interface description	This interface represents the connection between the PE and TMS and has no interface to the MBS.	
Connection	Plan Execution (PE) <-> Traffic Management System (TMS)	
Safety related	No	
Safety implication	Safety measures	Comment
Interface integrity	Integrity shall be verified by using a protocol checksum.	-
Correctness of data	No safety related implications.	-

Availability of connection	No safety related implications.	-
Remarks	Not further assessed, as it is assumed, that the data input is correct and completely provided and this interface has no direct communication to the MBS system.	

Table 34 – I_PETMS Interface Definition

7 MAPPING OF X2RAIL SAFETY ANALYSIS

This chapter covers the safety analysis results [X2RAIL-5] of the project X2RAIL to ensure that they are adequately considered in this analysis. This is done by analyzing each hazard from the X2Rail results and by providing a trace to different artefacts of this STPA analysis.

7.1 4.1 TRACK STATUS ERRONEOUSLY CLEARED

This section describes causes which result in a Clear Track Status Area by the L3 Trackside, when there is in fact an obstruction present

Hazard	4.1.1 Dispatcher interaction in L3 Trackside initialisation
Hazard headline	Track Status Area erroneously cleared during L3 Trackside initialisation by dispatcher leading to collision
Hazard description	At L3 Trackside initialisation, in addition to communicating trains there could be non-communicating trains (e.g. in modes SH, NP, etc.) or other obstructions such as vehicles not equipped with ETCS, work areas, etc. After initialisation (either in planned circumstances or as a consequence of a system fault) the Level 3 Trackside has to ascertain the Train Location of all vehicles and obstructions in the Area. If the L3 Trackside allows for a responsible person to declare Clear Track Status Areas, then it is critical that the area is only determined Clear when it is truly clear to avoid a Movement Authority into an Occupied Track Status Area, that could lead to a collision.
Trace to R2DATO	[UCA-OP-1], [SDR-1], [SDR-3].

Table 35 – 4.1.1 Dispatcher interaction in L3 Trackside initialisation

Hazard	4.1.2 Using invalid/outdated stored information for L3 Trackside initialisation
Hazard headline	Track Status Area erroneously cleared during L3 Trackside initialisation by system leading to collision
Hazard description	"At L3 Trackside initialisation, in addition to communicating trains there could be non-communicating trains (e.g. in modes SH, NP, etc.) or other obstructions such as vehicles not equipped with ETCS, work areas, etc. After initialisation (either in planned circumstances or as a consequence of a system fault) the Level 3 Trackside has to ascertain the Train Location of all vehicles in the Area. If the L3 Trackside utilises stored information to clear Track Status Areas, then it is critical that this information is correct to avoid a Movement Authority into an occupied area, that would lead to a collision. The information may no longer be correct and erroneously consider the track clear when it is still occupied."
Trace to R2DATO	Depends on specific implementation (utilizing previously stored data after initialization) and this is out of scope at this state of analysis.

Table 36 – 4.1.2 Using invalid/outdated stored information for L3 Trackside initialisation

Hazard	4.1.3 Deactivating Temporary Shunting Area
Hazard headline	Track Status Area erroneously cleared after deactivation of a Temporary Shunting Area leading to collision
Hazard description	The L3 Trackside considers the track status in an Active Shunting Area as Unknown Track Status Area, except for the Train Location of communicating trains. When deactivating a Shunting Area, responsible staff may have the possibility to clear any remaining Unknown Track Status Area. Doing this, an occupied area of track could be set to clear, leading to collision.
Trace to R2DATO	[out of scope]

Table 37 – 4.1.3 Deactivating Temporary Shunting Area

Hazard	4.1.4 Driver confirms train integrity
Hazard headline	Track Status Area erroneously cleared by driver confirming Train Integrity leading to collision
Hazard description	In case a train driver confirms Train Integrity after a part of the train has been lost, the lost part will be not detected (unless there is TTD), which could lead to collision with other trains approaching the area where the lost part is. This situation could occur when operating trains without TIMS or for a train with a failed TIMS.
Trace to R2DATO	[H-1] [SC-2.7] [SC-6.1] [ASM-3] [ASM-6] [ASM-8] [SDR-12] The analysis considers in the unsafe control actions of the I_OBU interface different scenarios about unknown train position.

Table 38 – 4.1.4 Driver confirms train integrity

Hazard	4.1.5 Recovery of a failed train
Hazard headline	Track Status Area erroneously cleared by TIMS device not being able to detect loss of train integrity after coupling trains leading to collision
Hazard description	"When a train is coupled with another train they should be considered as one train with a common train integrity. However, this depends on if the TIMS devices in the coupled trains are compatible or if the TIMS in the rear part is operational. In case the driver updates the train length to that of the coupled trains without knowing the status of the TIMS device in the rear part, a loss of integrity in the rear part will not be detected and reported by the TIMS in the front part of the train. This could happen in a rescue situation when there is need to pull out a failed train and lead to a collision if the track is cleared based on information which is not valid for the complete train and a part of it is lost without being detected."

Trace to R2DATO	[H-1] [SC-2.7] [SC-6.1] [ASM-3] [ASM-6] [ASM-8] The analysis considers in the unsafe control actions of the I_OBU interface different scenarios about unknown train position.

Table 39 – 4.1.5 Recovery of a failed train

7.2 4.2 ERROR IN TRAIN LOCATION

This section describes causes which result in the location of a train as recorded within the L3 Trackside being different from the true location of the train

Hazard	4.2.1 Confidence interval reduced at End of Mission
Hazard headline	Error in Train Location from reduced confidence interval at End of Mission leads to collision
Hazard description	"The L3 Trackside needs to determine the area that could be occupied by a train performing End of Mission (EoM) in order to protect it. To that aim, the L3 Trackside is expected to use the location information received from the train. However, as part of the ERA CCM Process an ambiguity in the specifications has been identified which makes it unclear how the ETCS On-board calculates the confidence interval reported at EoM. This is because linking information, including balise location accuracy used in the confidence interval, is deleted when changing to SB mode. If the location accuracy of the LRBG has a larger value than the National Value (Q_NVLOCACC) and the ETCS On-board uses the National Value in the EoM Position Report, this could lead to a collision if the Unknown Track Status Area for protecting the train is unduly shortened, not covering the whole length of the train."
Trace to R2DATO	[not applicable – described hazard results from a specific implementation]

Table 40 – 4.2.1 Confidence interval reduced at End of Mission

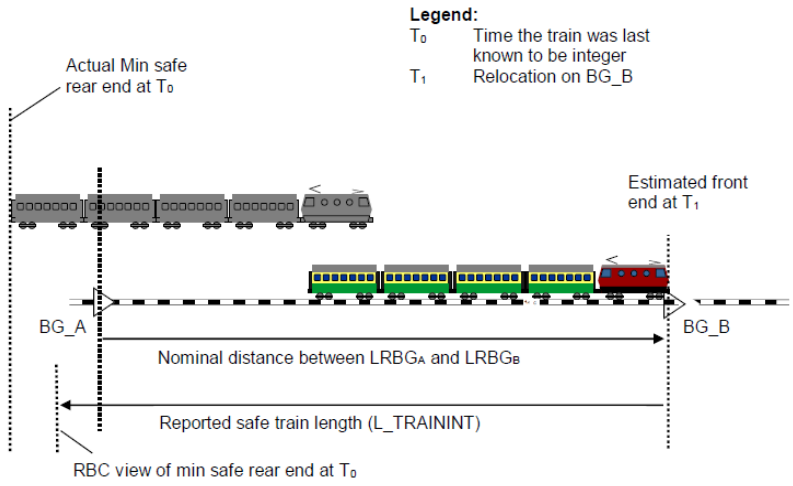
Hazard	4.2.1 Lack of linking information
Hazard headline	Error in Train Location from lack of linking information leading to collision
Hazard description	When relocation is done for a new balise group without linking information (Subset-026, 3.4.4 [BL3 R2]) the ETCS On-board uses the estimated distance travelled between the previous LRBG and the new LRBG. Next figure illustrates the potential issue that arises.  **Figure 1: On-board mSRE relocation in the absence of linking information** At time T0 (i.e. the time when the train was last known to be integer), the LRBG was BG_A. At time T1, BG_B is encountered, the ETCS On-board then relocates the Min Safe Rear end at T0 to the new LRBG. If linking information is not available or not used, the ETCS On-board then sends a position report to the L3 Trackside using the estimated distance between BG_A and BG_B when calculating the safe train length. If this estimate is shorter than the real distance between BG_A and BG_B, the L3 Trackside believes that the confirmed rear end is closer to BG_A than it actually is. This means that in case the train has been broken between time T0 and T1, but not yet detected by the TIMS device, there could be a part of the train in the section of track that was just cleared, but the L3 Trackside is not aware of this.
Trace to R2DATO	[currently unclear if hazard is still applicable since safe train length (in the lates UNISIG SS-26) is only sent if also confirmed]

Table 41 – 4.2.1 Lack of linking information

7.3 4.3 Error in Train Length

This section describes causes which result in the Train Length of a train as recorded within the L3 Trackside being different than the true length of the train

Hazard	4.3.1 Reported train length shorter than actual
Hazard headline	Train Length value shorter than the actual length leading to collision, derailment, or exceeding speed limits
Hazard description	"In case the Train Length given in the Validated Train Data to the L3 Trackside is shorter than the physical train length, this could result in: ▫ Another train being authorised beyond the rear of this train located in front, OR ▫ Infrastructure released (points moved) under the train, OR ▫ Train does not achieve calculated braking curves, OR ▫ Train permitted to accelerate earlier after speed restrictions. The error in Train Length could be caused by: ▫ Incorrect train length provided by an external system. ▫ Incorrect train length entered by the Driver at Start of Mission. ▫ Driver does not update the train length after joining."
Trace to R2DATO	R2DATO assumes in the [ASM-8] and [ASM-9] the correct reporting of the correct train length and train integrity. To show why these assumptions are needed, the analysis considers in [S2-UCA-MBS-16] the safety implications of a reported train length shorter than physical reality. This also results in recommendations regarding expected splitting and joining operations ([SDR-11] and [SDR-12])

Table 42 – 4.3.1 Reported train length shorter than actual

Hazard	4.3.2 Reported train length longer than actual
Hazard headline	Train Length value longer than the actual length leading to collision or exceeding speed limits
Hazard description	"In case the Train Length given in the Validated Train Data to the L3 Trackside is longer than the physical train length, this could result in a Track Status Area which is Occupied or Unknown being cleared while still occupied by another vehicle, or that the calculated braking curves are not met by the train. The error in Train Length could be caused by: ▫ Incorrect train length provided by an external system. ▫ Incorrect train length entered by the Driver at Start of Mission.

	▫ Driver does not update the train length after splitting."
Trace to R2DATO	R2DATO assumes in the [ASM-8] and [ASM-9] the correct reporting of the correct train length and train integrity. To show why these assumptions are needed, the analysis considers in [S1-UCA-MBS-16] the safety implications of a reported train length longer than physical reality. This also results in recommendations regarding expected splitting and joining operations ([SDR-11] and [SDR-12])

Table 43 – 4.3.2 Reported train length longer than actual

7.4 4.4 CMD Erroneously Validates Position

This section describes the result of a CMD system erroneously validating the location of a train

Hazard	4.4.1 Wrong side failure of CMD
Hazard headline	CMD erroneously validates a position which is incorrect leading to collision or derailment
Hazard description	"In case CMD validates the position of a train after being moved in NP mode, the L3 Trackside can give this train a Movement Authority based on the position at End of Mission while the train is now somewhere else. This may lead to derailment or collision. Note that some CMD equipment may allow for a short movement of a train whilst still reporting “no cold movement detected”. Potential mitigations: The following considerations could be taken as mitigation measures: • Hazardous failure rate for CMD to be considered. • Use linking reaction for the first expected Balise Group in the linking chain when authorising trains to move, which will brake the train if it is not found as expected. • Use TTD where trains start after NP mode. However, this is not enough on its own."
Trace to R2DATO	[S3-UCA-MBS-16] [S4-UCA-MBS-16] [mainly concerns the SIL classification of the CMD device]

Table 44 – 4.4.1 Wrong side failure of CMD

7.5 4.5 UNDETECTED MOVEMENTS

This section describes causes which result in undetected movement of a train

Hazard	4.5.1 Rollback after standstill
Hazard headline	Undetected backward movement after standstill leading to collision
Hazard description	If a train moves backwards after reaching standstill, it could compromise the authorisation for another train. It can take some time before the L3 Trackside can react on this potentially hazardous situation and try to prevent a collision.
Trace to R2DATO	[S3-UCA-MBS-16] [S4-UCA-MBS-17] [S5-UCA-MBS-17]

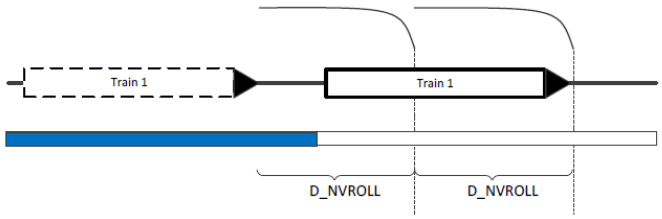
Table 45 – 4.5.1 Rollback after standstill

Hazard	4.5.2 Unreported Movement
Hazard headline	Unreported Train movement leading to collision or derailment
Hazard description	"If a non-communicating train is moved, the movement is not reported to the trackside, and therefore, the L3 Trackside has no knowledge of the movement, and may authorise a conflicting train movement."
Trace to R2DATO	[S3-UCA-MBS-16] [S4-UCA-MBS-17] [S5-UCA-MBS-17]

Table 46 – 4.5.2 Unreported Movement

Hazard	4.5.3 At entrance to Level 3 area
Hazard headline	Undetected movement entering the L3 area leading to collision
Hazard description	In degraded situations, it could occur that a train incorrectly enters the L3 Area when it is not authorised, and it is not detected by the L3 Trackside.
Trace to R2DATO	[ASM-4-v2]

Table 47 – 4.5.3 At entrance to Level 3 area

Hazard	4.5.4 After End of Mission
Hazard headline	Undetected movement after End of Mission leading to collision
Hazard description	If a train in SB mode rolls away, Standstill Supervision will result in a brake application once the train moves beyond the distance D_NVROLL. This results in the train being brought to a halt, after which the driver can acknowledge the standstill supervision, releasing the brake. There is no limit on the number of acknowledgements the driver is allowed to make, since this may inhibit Splitting operations. This functionality can enable the driver to use consecutive acknowledgements of the standstill supervision activation to move the train. Figure 3 illustrates the movement that could occur.  **Figure 3: Train exiting the Unknown protective area after EoM** This creates a risk where the train could move outside the Unknown Track Status Area created at EoM for protection, because ETCS does not prevent the use of

	consecutive roll away movements.
Trace to R2DATO	[ASM-4-v2]

Table 48 – 4.5.4 After End of Mission

Hazard	4.5.5 Loss of Train Integrity
Hazard headline	Undetected movement of a part of the train after loss of integrity leading to collision
Hazard description	In case train integrity has been lost and part of the train rolls backwards due to the gradient profile, this may result in a collision with other vehicles. In case of derailment, collisions can also occur on adjacent tracks.
Trace to R2DATO	[S3-UCA-MBS-16] [S4-UCA-MBS-17] [S5-UCA-MBS-17]

Table 49 – 4.5.5 Loss of Train Integrity

Hazard	4.5.6 Propelling train
Hazard headline	Undetected movement beyond the secured area for a propelling train leading to collision
Hazard description	"In case a train is pushing another train in front of it (propelling movement) there is a risk that the front of the propelled train overpasses the area reserved for this movement as the driver in the propelling train cannot see where the front is. This can happen if there is need to rescue a failed train from the rear. The rescue train will then be propelling a piece of rolling stock in front of it that cannot report its position. If the front of this movement overpasses the reserved area, a collision may occur as the L3 Trackside is not aware of the real ""front end"" (belonging to the failed train) and able to react on this situation to protect other movements. As mSFE and Train length doesn't match with the real train this could lead to a wrong track status."
Trace to R2DATO	[rescue train out of scope]

Table 50 – 4.5.6 Propelling train

Hazard	4.5.7 Shunting train
Hazard headline	Undetected movement out of an Active Shunting Area leading to collision
Hazard description	Shunting movements may unintentionally move beyond the border of an Active Shunting Area without the L3 Trackside being aware of this and therefore being unable to protect other movements in the vicinity of the Shunting Area.
Trace to R2DATO	[shunting out of scope]

Table 51 – 4.5.7 Shunting train

7.6 4.6 TTD ERRONEOUSLY INDICATES TRACK CLEAR

This section describes the result of a TTD which erroneously indicates a section of track as Clear Track Status Area

Hazard	4.6.1 Wrong side failure of TTD
Hazard headline	TTD erroneously indicates a Clear Track Status Area leading to collision or derailment
Hazard description	"If TTD is used to clear track irrespective of Train Locations, then: ▫ An Unknown Track Status Area could be cleared without being swept, ▫ Infrastructure could be released or moved under a train, ▫ Erroneously updating the CRE of the train in front, and consequently providing an MA to a following train that could result in a collision."
Trace to R2DATO	[according to assumption ASM-13 TTD is considered a SIL4 function]

Table 52 – 4.6.1 Wrong side failure of TTD

7.7 4.7 POINTS MOVED UNDER TRAIN

This section describes the result of moving a point after communications failure

Hazard	4.7.1 Points Moved After Communications failure
Hazard headline	A point is moved in an Unknown/Occupied/Reserved Track Status Area with a train over it, or when it is about to pass over it, leading to derailment

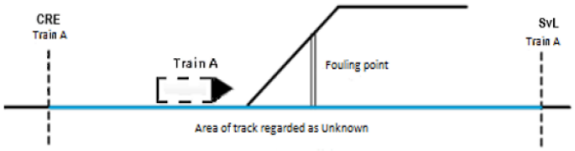
Hazard description	"The Dispatcher needs to move a train inside an Unknown, Occupied or Reserved Track Status Area to a new location. Figure 4 illustrates the situation with a train approaching a set of points inside an Unknown Track Status Area.  Figure 4: Unknown Track Status Area due a Communication failure The Dispatcher would need to move points so that the train can be moved to a siding. In the absence of TTD, moving a point could cause a derailment if moved when a train is over or about to pass it."
Trace to R2DATO	[ASM-4-v2]

Table 53 – 4.7.1 Points Moved After Communications failure

7.8 4.8 HAZARDS IDENTIFIED BUT PRESENT ALREADY IN ETCS L2

The hazards in this section were also identified by the work on ETCS Level 3, but after examination, were found to be already present in L2.

In some cases, there are additional mitigations possible in ETCS Level 3, which are given in the proposed mitigations.

Hazard	4.8.1 Mixed traffic
Hazard headline	Non-ETCS train erroneously enters a route for an ETCS L3 train leading to collision
Hazard description	"Drivers that operate both ETCS and non-ETCS fitted trains may mistakenly use a 'proceed for ETCS' aspect when operating a non-ETCS train due to confusion of ETCS and non-ETCS experience. Such a situation may result in a SPAD (Signal Passed At Danger) and a collision. This could happen at borders to the L3 Area but also inside an area with mixed traffic where L3 is used as an overlay to a conventional system with optical signals. This hazard is the same as in Level 2. It is the same situation as a non-ETCS train erroneously entering a route set for a Level 2 train in a mixed traffic area."

Trace to R2DATO	[assumption [ASM-3] – there are no non-ETCS trains with regular movements]

Table 54 – 4.8.1 Mixed traffic

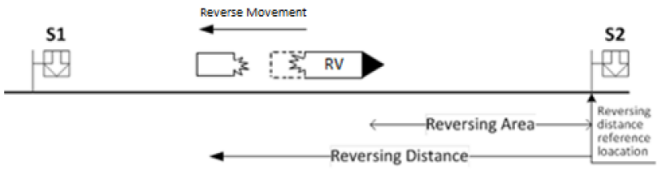
Hazard	4.8.2 Reversing
Hazard headline	Train moves backwards after loss of train integrity leading to collision
Hazard description	"In case a train needs to reverse after a loss of train integrity it may collide with the part of the train that was lost:  Figure 5: Train reversing after loss of integrity Figure 5: Train reversing after loss of integrity This hazard is the same as in Level 2, and in conventional signalling."
Trace to R2DATO	[reversing out of scope]

Table 55 – 4.8.2 Reversing

Hazard	4.8.3 Loss of train integrity
Hazard headline	Derailment after loss of train integrity causes obstruction in adjacent tracks leading to collision
Hazard description	"After a loss of train integrity, the lost part of the train could derail causing an obstruction in the adjacent track resulting in a collision. This hazard is the same as in Level 2, and in traditional signalling."
Trace to R2DATO	[S3-UCA-MBS-16] [S4-UCA-MBS-17] [S5-UCA-MBS-17]

Table 56 – 4.1.1 Dispatcher interaction in L3 Trackside initialisation

8 COMPILED DESIGN RECOMMENDATIONS

This chapter contains the compiled safety design recommendations for the analyzed control loops supplemented with rationale, guidance &/or example statements. Although these enriched recommendations should be self-explanatory, it might make sense to look up the linked (hypothetical) scenarios for each, that led to unsafe control actions in the chapters above.

8.1 UNSAFE CONTROL ACTIONS TOWARDS ON BOARD UNIT

=>[SDR-13]: In regions where the parking of vehicles is expected, methods for detecting the presence of trains independent of train position reports shall be available (i.e. installing TTDs in these regions)

Rationale Uncontrolled train movements, like runaway cars after parking, are not constrained by a movement authority. Such a scenario is described in [S3-UCA-MBS-16]

=> [SDR-16]: Between controlled region and unsupervised region, the movement of non-communicating trains shall be detectable, i.e. using TTDs, or preventable using a point/derailer (similar to [SDR-13])

Rationale Detecting or preventing the presence of uncontrolled trains out of unsupervised regions (e.g. at the borders of the region of control) is needed for assumption 2. A corresponding scenario is described in [S2-UCA-MBS-17].

=> [SDR-18] Simple detection of track occupation is not sufficient to prevent flank collisions in all cases. Technical means to secure a sufficiently large vacant area before the fouling point is required.

Rationale Even when the train presence is detected according to assumption 1., the reaction times can be insufficient to prevent a flank collision hazard, making further measures necessary:

=> [ASM-4-v2] MBS does not require TTDs for controlled train movement but supports them for migration purposes or systems where the chance of uncontrolled movement cannot be sufficiently controlled by other means.

Rationale The assumption that TTDs can completely be eliminated while still guarding against all loss scenarios found in our analysis is too strong. As long as uncontrolled train movement cannot be eliminated, their presence is still required.

=> [SDR-11]: MBS shall always be aware when a change of train length is expected (i.e. due to splitting and joining).

Rationale If the MBS detects an unexpected difference between the reported and expected train length, this could indicate a wrong data input (either by the driver or in the operation plan).

Example This can be done e.g. by informing the MBS that splitting or joining is performed via the plan execution.

8.2 Unsafe Control Actions towards Operator Panel

=> [SDR-1]: Provide an operational rule set which explicitly determines to which infrastructure item a completed (safety related) intervention refers/referred to.

Rationale Since safety functions of MBS directly depend on the correctness of its operational state, special care has to be taken where a human operator is allowed to issue safety related commands or settings.

=> [SDR-2]: When changes to the operational state are reported by personnel, the operator shall always check if they are already entered in the operation state of MBS, even if the operator believes this has already been done in the past

Rationale as above.

=> [SDR-3]: The operator panel shall provide easily accessible information on all currently manually entered infrastructure state with the required confidence for a safety related function.

Rationale The operator shall have a means to reproduce origin and the reliability of the presented data.

=> [SDR-4]: The interface for the operator shall allow to pre-schedule usage restriction areas.

Rationale In order to avoid secondary (possibly non-SIL systems) tools, or even pen & paper solutions the system shall include safe and transparent means for pre-scheduling.

=> [SDR-5]: The operator shift handover shall include either an operational process or digital means that prevent a loss of (safety related) information during the handover.

Guidance Ideally all relevant information as well as the handover- procedure itself are foreseen in the operator panel/system.

Example Whenever the operator confirms a (safety related) request from any other stakeholder, this confirmation shall contain a token (e.g., safety code) either from MBS or a trustworthy operator panel, guaranteeing that the said intervention is either already in place or dependably pre-scheduled.

=> [SDR-6]: The operator panel should implement procedures to verify the entered usage restriction data, before the entered data is passed to the MBS system.

Rationale Since the operator is still a human being, additional procedures to verify the inputs are recommended.

=> [SDR-7]: Entering usage restriction areas shall take priority over the regular management of running trains

Rationale E.g., a usage restriction that was issued to late is a safety risk.

Guidance Maybe an even more general prioritization of tasks could be implemented. The life-cycle of URAs -> is a design decision potentially influencing multiple systems.

=> [SDR-8]: The operator shall always verify with the construction team on site that the work has actually been completed before removing the corresponding usage restriction area.

Rationale Again, possibly safety related information from/through human beings needs to be re-checked by adequate processes and rules.

=> [SDR-9]: The operator panel shall be designed to support the operator with contextual information when executing operator commands. I.e. the operator shall be able to select the stopping position based on an interface with information about the physical elements/trackside assets and select a stopping position based on the physical elements position.

Rationale With processes that have a “human in the loop” also the feedback to this human – e.g., its readability and its correctness - may have safety implications.

=> [SDR-10]: The operator shall receive a (visual) indication about the reported train position age. (e.g., information outdated longer than for a defined threshold should be indicated).

Rationale Edge cases that result from timing interrelation (e.g., max. GSM-R signal roundtrip) in the greater system need to be – at least - visible to the operator.

8.3 Unsafe Control Actions towards Trackside Assests Control & Supervision

Those UCAs are either covered with measures defined in the EULYNX specification or are directly linked to moving trains - and thus covered by UCAs towards the onboard unit (8.1.).

8.4 UNSAFE CONTROL ACTIONS REGARDING DOMAIN DATA & UPDATES

=> [SDR-25] DR shall include a set of verification functions that ensure that processed data follows the required engineering rules and is not malformed.

Rationale as with [SDR-19].

=> [SDR-19] There shall be a “safety responsible” entity which is in a valid position to verify the correctness (correspondence to the physical reality) of the input data for MBS with a certainty corresponding to a SIL-4 function.

Rationale With the concept of a “generic” Safety Logic the functional behavior of MBS depends on the correctness (conformity with physical reality) of its input topography- and configuration data (here Domain Data) from an external source.

Guidance This is a nonnegligible advantage over past and current approaches (see Figure 9). For example, MBS allows for much greater flexibility with regards to setting MAs instead of relying on pre-defined routes. However, since MBS cannot verify that correspondence to physical reality by itself, an exported requirement demanding proof, as well as a clear path of responsibility shall be established.

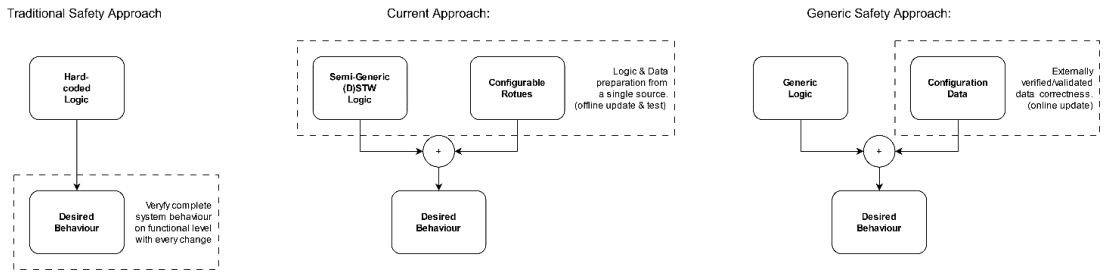


Figure 9: Generic Safety Logic

=> [SDR-20] MBS shall include a function that ensures that the input data (here Domain Data) received corresponds exactly to what has been verified and validated by the above (in UCA-DR-1) mentioned safety responsible (e.g. by means of a dedicated signature or safety code).

Rationale If there are intermediaries between the entity that validated the input data for MBS and MBS itself, then a method is required to assure that the data has not been altered/changed in between.

Example The following figure shows how such a tracing of the safety responsibility for new topography and configuration data could be implemented. In this case the responsibility lies with the engineering data supplier:

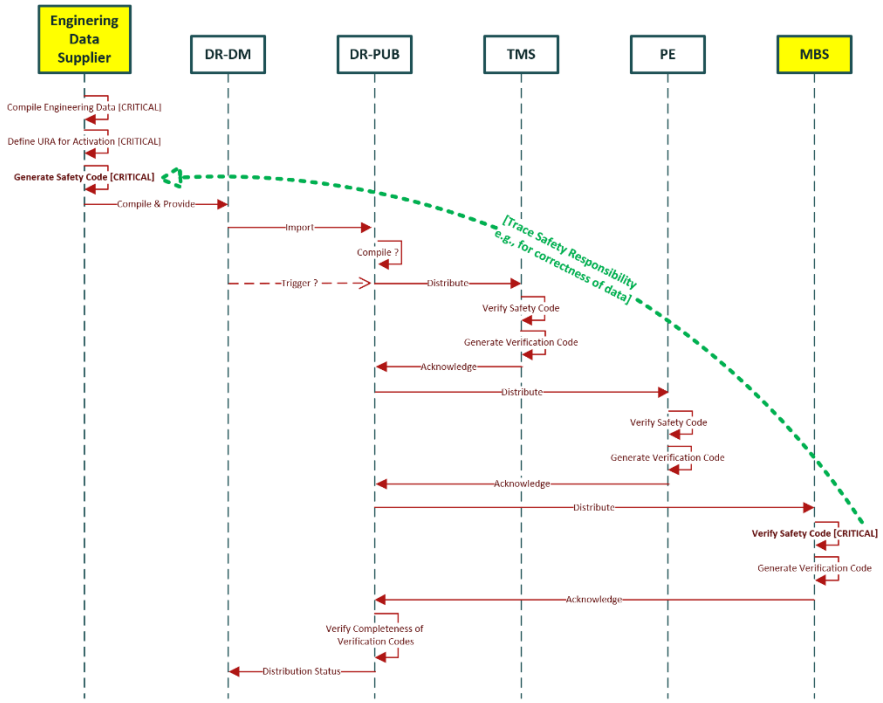


Figure 10: Example for tracing of safety responsibility for topography & configuration data

=> [SDR-21] An operational rule may be required, that ensures that any infrastructure changes have to be preceded by a (sufficiently large & restrictive) URA, and that this URA may only be lifted if the changes have been updated in the topography & configuration data of MBS.

Rationale MBS lacks the information to verify that the URAs are sufficiently restrictive for the infrastructure change to be safely performed. This verification must therefore be performed by other means, e.g. an operational rule.

=> [SDR-22] There shall be a “safety responsible” entity which is in a valid position to define a (sufficiently large & restrictive) URA which covers the area in said AoC which is about to change during the upcoming data (Domain Data) update. Again, with a certainty corresponding to a SIL-4 function.

Rationale Similar to the correctness of topography and configuration for normal operations, it is paramount that the URA covering the area that is about to change during an update (of Domain Data) is sufficiently large and correct.

Alternative MBS could have a capability that allows to derive the delta between the current and the uploaded new/next Domain data update. However, a separate (and safe) concept on how to derive a sufficiently large URA would be required.

=> [SDR-23] MBS shall include a function that ensures that the received URA corresponds exactly to what was defined by the aforementioned safety responsible (e.g. by means of a dedicated safety code).

Rationale If there are intermediaries between the entity that defined the URA and MBS itself, then a method is required to assure that the data has not been altered/changed in between.

Example Similarly, the engineering data supplier could also provide the extent/type of the required URA, even though it is then timed/initiated through TMS/PE:

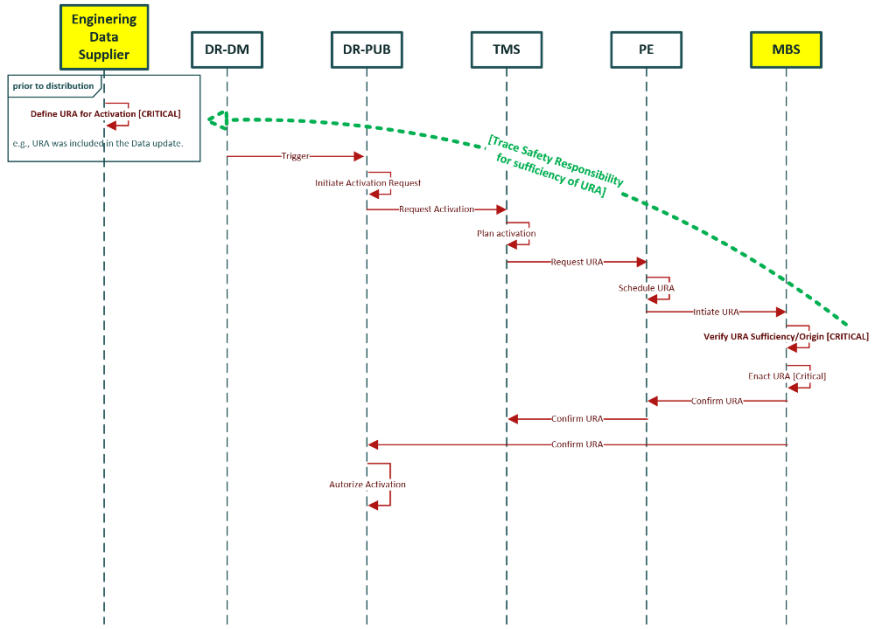


Figure 11: Example for tracing of safety responsibility for update URA

Finally, MBS would only have to check if the URA is in place before activating the update within itself:

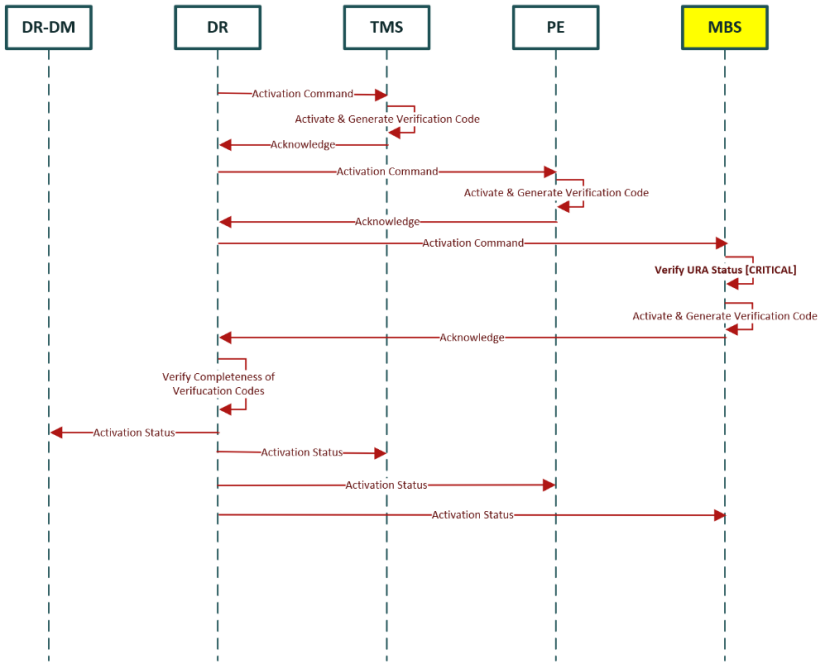


Figure 12: Example for verifying URA status.

=> [SDR-24] If an URA for safe activation of new set of domain data is required the domain data shall include the reference for this URA (e.g. by means of a dedicated safety code).

Rationale MBS (or DR if designed with sufficient SIL) shall be able to decide if the required precautions were taken before activating a new version of domain data.

9 SAFETY RESULTS & CONCLUSION

9.1 STRUCTURE OF THE RESULTS

The results of this document are presented in three separate chapters:

Chapter 6 “Interface Criticality” contains the analysis of the safety relevance of the interfaces connected directly to the MBS. The neighbouring system is specified in the name of the interface (e.g.: I_DR is the interface between the MBS and the DR). An analysis with respect to the correctness and integrity of the data as well as the availability of the connection was also conducted for each interface. The following interface are listed as safety related: I_AS, I_OBU, I_OP, I_TACS.

Chapter 7 “Mapping of X2Rail Safety Analysis” covers the safety analysis results [X2RAIL-5] of the project X2RAIL to ensure that they are adequately considered in this analysis. This is done by analyzing each hazard from the X2Rail results and by providing a trace to different artefacts of the STPA analysis. It can be stated that the X2RAIL results - where applicable (not bound to a S2R specific solution) - are fully covered by the artifacts (e.g. assumptions, design recommendations, interface analysis, ...) from this task.

Chapter 8 “Compiled Design Recommendations” contains the results of the risk analysis in Chapter 5 above, supplemented with rationale, guidance & example statements where applicable. Although these enriched recommendations should be self-explanatory, it makes sense to look up the linked unsafe control actions in the chapters above. They describe how such a hypothetical scenario could have occurred and form the background for the recommendations.

9.2 STARTING POINT

The basis for this analysis was the rough system architecture that is baked into the grant agreement as well as various sources from previous projects (see chapter 3). However, essential inputs from system pillar were not available at the time. Thus, an own list of assumptions (see chapter 5.5) was created, compared, mapped, and supplemented with a similar list from the system definition task (13.1). Similarly, the operational context was rather compiled and derived from state-of-the-art procedures in the participating railway companies than given from the normative side. Another factor shaping the work in this task, were the resources at hand, and the parallelized work structure given through the grant agreement.

9.3 Positioning and Objectives

Overall, the undertaking in this task can best be compared to step 3 in the classic V-Cycle from the CENELEC norms.

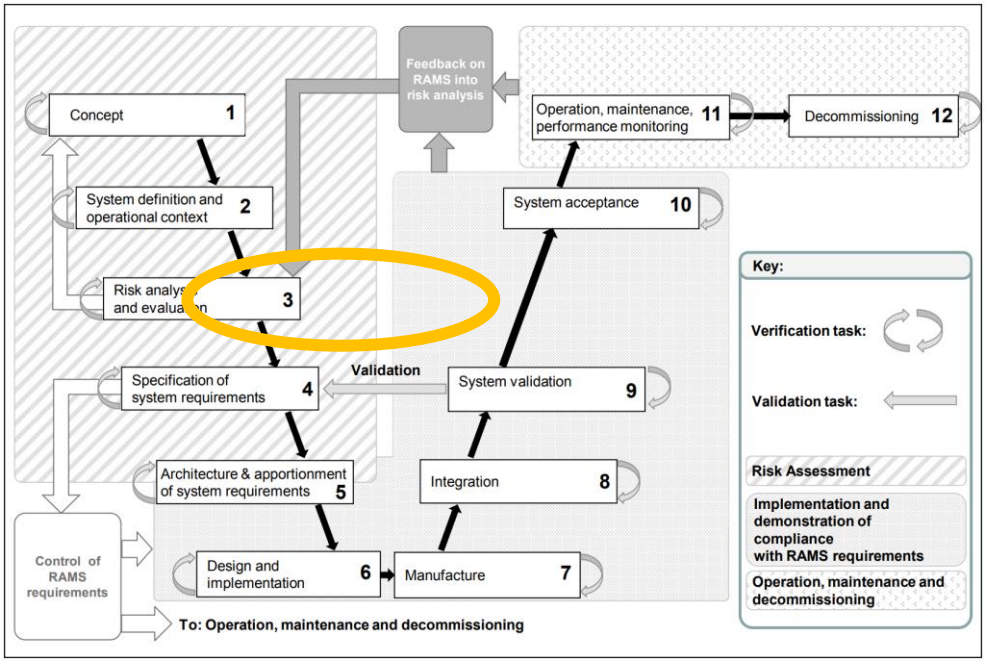


Figure 13: CENELEC V-Cycle

The first part of the original objectives stated in the grant agreement "a*nalysis of the impact of the system pillar inputs*" was not feasible due to a lack of the inputs regarding the concepts and the operational context. But the missing inputs were substituted from other sources as stated in 9.2. The results of this task can conversely serve as input for the ongoing discussion in the system pillar.

Due to limited time and resources, the authors decided to focus on system hazards, by analyzing the control interactions between the moving block system and the systems with which it interfaces directly. The chosen method is explained and exemplified in chapter 5.

We expect that the results can be utilized to update the system concepts, the system definition as well as the operational context and then further the system specification for the continuing innovation pillar work on the Moving Block Demonstrator. Some of the results can also be exported adjacent work packages, like WP27 where the Digital Register is being specified, or to the demonstrator work packages WP44/45 where operational concepts, and an operator console/workbench will come into play.

Even though a proof of completeness with respect to functional safety is not in part of this task, we were able to show that we cover the whole set of results from X2Rail safety work in chapter 7.

9.4 Discussion of Main Results

An advantage of the chosen approach was that it allowed to connect the beforehand stated assumptions with the relevant loss scenarios they affect. Some of the used assumptions were well established (e.g., the SIL classification of the OBU, OCs), while others were relatively novel (e.g.,

not requiring TTDs for detection of train presence). The safety analysis therefore provided an opportunity to validate or - if necessary - update these assumptions.

For example, under the assumption that TTDs are not required ([ASM-4]), we generated loss scenarios for the relevant unsafe control actions to see if the hazard could still be prevented. This is closely connected to two further assumptions about MBS:

1. Up to date knowledge of all (potential) train positions on the tracks
2. Ability to constrain all train movement within a known area (i.e., movement authority)

The respective set of loss scenarios (concerning runaway wagons, loss of communication, parking vehicles and so on) led to the specific design recommendations [SDR-13], [SDR-16] & [SDR-18]. The summary of those in turn leads to the conclusion, that the assumption that TTDs can completely be eliminated while still guarding against all loss scenarios found in our analysis is too strong. In short, if uncontrolled train movement cannot be eliminated, their presence is still required. Henceforth, [ASM-4] was updated to [ASM-4-v2] "*MBS does not require TTDs for controlled train movement but supports them for migration purposes or systems where the chance of uncontrolled movement cannot be sufficiently controlled by other means.*"

A second class of assumptions is concerned with the correspondence between reported data and physical reality. This includes assumptions about the reported train length ([ASM-8]) as well as the geographical position of infrastructure elements like points, tracks, etc. ([ASM-26]). For train length, partial validation is possible in the case of splitting or joining trains. However, the validation alone may not be sufficient to achieve the desired level of confidence required for a SIL 4 function (e.g., if two trains enter the same TTD section and maneuvers like joining, splitting, or turning take place). Thus [SDR-11] states that "*MBS shall always be aware when a change of train length is expected (i.e. due to splitting and joining)*."

The correctness of information on the geographical position of infrastructure elements is even more critical for MBS. Some controller constraints depend on geometrical information (e.g. ensuring that there are no intersections between movement authorities, [Resp-MBS-1]) which need the required level of precision to ensure that no intersections are undetected. MBS lacks the information to validate the provided information by itself, but depends on it for SIL-4 functions. Thus, the corresponding assumption [ASM-26] has the rank of exported requirement, provided in a higher level of granularity through the design recommendations [SDR-18] to [SDR-24].

The third class of results concerns the control loops where a human actor is involved. Several design recommendations in section 8.4 concern the Operator Panel, its ability to display safety related information, to re-verify human entered values, to schedule safety related commands, or more general operational procedures that could be linked to respective loss scenarios in our analysis.

9.5 Open Points and Future Work

Even though the major pain points were likely highlighted in this analysis, they are not yet verifiably settled or solved. In that regard, the design recommendations will have to be considered in the system definitions of MBS, DR and the Operator Panel - to be then re-checked/validated in a further

step of the safety analysis (e.g., protection against side-on collisions; domain data safety responsible entity).

Some of the assumptions defined at the beginning of the work packages simplified the analysis and might have to be re-opened in a later stage when extending the system scope (e.g., SIL of train length / train integrity information; handover to neighboring MBS- or legacy systems). Finally, there are some use-cases that were postponed to a later stage of the demonstrator (e.g., supervised shunting) that must be analyzed as soon as first concept drafts are available.

The results of the safety analysis review from D13.1 will be further developed and addressed within WP14. Regarding any form of proof of completeness, e.g., for a later certification will likely have to move to a possible second phase of the R2DATO project.

REFERENCES

[1] Nancy G. Leveson, John P. Thomas; STPA Handbook; March 2018, STPA Handbook (MIT-STAMP-001)

[2] UNISIG, Subset 026, ERTMS/ETCS System requirements specification, Issue 4.0.0, July 2023

[3] CENELEC, EN 50126-1:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[4] CENELEC, EN 50126-2:2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[5] CENELEC, EN 50129:2018, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling

[6] System Pillar Common Business Objectives, Version 1, 25/07/2022, (https://rail-research.europa.eu/wp-content/uploads/2022/10/SP-Common-Business-Objectives.pdf)

[7] System Pillar Operational Visions, Version 1, 11/07/2022, (https://rail-research.europa.eu/wp-content/uploads/2022/10/SP-CCS-TMS-CMS-Operational-vision.pdf)

[8] Common Safety Method for Risk Evaluation and Assessment, CELEX (EU) No 402/2013 (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32013R0402), CELEX (EU) 2015/1136 (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2015.185.01.0006.01.ENG).

[9] X2Rail-1, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

[10] X2Rail-3, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

[11] X2Rail-5, https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-5

[12] RCA, https://ertms.be/activities/target-archi-ccs-architecture

[13] R2DATO WP13 Task 13.1 System Definition

[14] R2DATO WP13 Task 13.2 System Specification

[15] R2DATO WP44 Task 44.3 System Definition

[16] R2DATO WP44 Task 44.3 System Specification

[17] R2DATO WP13 Task 13.1 System Definition - Assumptions

[18] R2DATO_WP13_SystemDefinition_Assumptions.xlsx (Work Package internal File)

[19] UNISIG, Subset 023, ERTMS/ETCS Glossary of Terms and Abbreviations, Issue 4.0.0, July 2023

[20] ISO 16290:2013-Space systems — Definition of the Technology Readiness Levels (TRLs) and their criteria of assessment