

Rail to Digital automated up to autonomous train operation

D8.1 - Safety analysis for automating functions

Due date of deliverable: 30/09/2025

Actual submission date: 30/09/2025

Leader/Responsible of this Deliverable: < Stephan Griebel, Siemens Mobility GmbH>

Reviewed: Y/N

Document status		
Revision	Date	Description
01	10/07/2025	First issue
02	30/09/2025	Release for TMT review
03	16/01/2026	Amendment based on ERJU review

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

Start date: 15/06/2023

Duration: 27 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
Angel Fernandez Gago	ADIF	Safety analysis and safety review for specific hazards
Angelo Viacava	SBB	Safety analysis and safety review for specific hazards Chapter 4.4, 4.5, 4.6, 5 Annex E – Explicit risk evaluation Review of final delivery
David Fernandez Gay	CAF Signalling	Safety analysis and safety review for specific hazards Chapter 4.4, 4.5, 4.6 Review of final delivery
Diego Garcia Vaquero	ADIF/RENFE	Safety analysis and safety review for specific hazards Chapter 6 Review of final delivery
Emre Buyukakincak	Alstom	Safety analysis and safety review for specific hazards Review of final delivery
Guy Larbat	Alstom	Safety analysis and safety review for specific hazards
Lukáš Kacar	AŽD Praha	Safety analysis and safety review for specific hazards Chapter 4.4 Review of final delivery
Konstantin Szengel	GTSD	Safety analysis and safety review for specific hazards Chapter 4.4 Annex A - Hazard log Annex B – Hazard list Review of final delivery

Name	Company	Details of Contribution
Markus Korb	Siemens Mobility	Safety analysis and safety review for specific hazards Chapter 4.4, 4.5, 4.6 Review of final delivery
Stephan Griebel	Siemens Mobility	Task leader Safety analysis and safety review for specific hazards Review of final delivery
Stephanie Löbig	Siemens Mobility	Deputy task leader Safety analysis and safety review for specific hazards Chapter 1, 2, 3, 4.1, 4.2, 4.3, 4.4, 6, 7 Review of final delivery Final editing of final deliverable
Thidarat Panthong	DB Systemtechnik	Safety analysis and safety review for specific hazards Annex C – SB & SRACS Annex D – Final THR Review of final delivery
Thomas Heilke	DB InfraGO AG	Safety analysis and safety review for specific hazards Review of final delivery

Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author’s view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

EXECUTIVE SUMMARY

The main task of WP 8.1, "Safety Analysis for Automating Functions," was successfully conducted as stipulated by the Grant Agreement and thanks to fruitful collaboration with the other relevant work packages and team members.

Based on the outcomes of WP 5 (Use Cases) and WP 6 (System Requirements), WP 8.1 derived:

- the hazards related to automating functions and
- their safety requirements, namely the Tolerable Hazard Rates.

This was achieved by establishing a rigorous Risk Analysis Model aligned with the other WP8 tasks, which – together with the analysis of operational barriers and an agreed-upon Risk Acceptance Criterion – enabled the detailed documentation of the results achieved, see ANNEX F and ANNEX G.

These results were exchanged with the other WP 8 tasks and can serve as a baseline for further research projects, enabling concrete developments by determining open parameters such as the concrete operational environment, effective barriers, and relevant architectural constraints.

The working group established the necessary milestones at the outset and monitored them continuously, as detailed in the Deliverable Development Plan.

Through online and in-person meetings, offline work, and deep-dive sessions, the experts were able to achieve the necessary complex analysis objectives and technical compromises in a constructive manner.

The possible next steps to finalize the analysis are presented in chapter 6.

OVERVIEW

R2DATO has the challenging objective of improving the automation level for the railway system. Safety is a key element for any transportation system design. Drawing lessons from the autonomous car industry, where unresolved safety concerns have delayed widespread commercial deployment, R2DATO integrates safety considerations from the earliest design phases. This preventive strategy serves multiple purposes: protecting human life, avoiding development delays, and ensuring the credibility and practical applicability of both R2DATO and ER-JU outcomes.

Scope

This report constitutes the final deliverable of WP 8.1 within R2DATO, focusing on the identification of safety requirements for controlling hazards associated with Automating Functions. The analysis specifically addresses potential hazards with their mitigation factors which arise from Use Cases, requirements and functional specifications. The methodology of this analysis is explained in chapter 4.

Safety aspects of other R2DATO components are addressed in separate work packages. WP 8.2 covers the perception module, while WP 8.3 encompasses the Automated Driving Module (ADM), Automated Processing Module (APM), and Repository (REP). Remote driving capabilities are addressed within WP 8.4.

The safety analysis presented in this report is based on the deliverables “D5.1 - Documentation of use cases for automating functions” provided by WP 5.1 [1] and “D6.1 - Report on sets of non-functional and functional requirements (SRS) for automating functions” provided by WP 6.1 [2].

The conclusions of the analysis are presented in Chapters 5 and 6.

Safety analysis approach

Unwanted deviations from the Use Cases, e.g. due to failures within Automating Functions, may result in hazards with the potential for catastrophic accidents.

The Automating Functions operate within a complex railway environment that incorporates established safety solutions (safety barriers) designed to address specific hazards. The automatic train protection (ATP) system serves as an example of such a barrier, providing independent technical protection against train overspeeding.

Taking these existing barriers into account, the safety analysis allows to determine and quantify the tolerable hazard rate (THR) for the identified hazards and to derive needed additional barriers and safety related application conditions (SRACs). The methodology of this analysis is explained in chapter 4.

Main safety results

The safety analysis has produced three main results:

- 1) Comprehensive identification and documentation of possible hazards, listed in ANNEX A, ANNEX B and ANNEX F.
- 2) Assessment of the identified hazards and determination of applicable existing safety barriers within the railway system that can partially or completely mitigate these hazards, as documented in ANNEX C and ANNEX G.

- 3) Determination of the final Tolerable Hazard Rate (THR), Safety Integrity Level (SIL), derived Safety-Related Application Conditions (SRACs), and additional required barriers for each hazard, all presented in ANNEX C, ANNEX D and ANNEX G.

ABBREVIATIONS AND ACRONYMS

AC	Alternating Current
ADM	Automatic Driving Module
AI	Artificial Intelligence
APM	Automatic Processing Module
AS	Assumption
AT	Automatic Driving
ATO	Automatic Train Operation
ATOREQ	Requirements for ATO (from WP 6.1)
ATP	Automatic Train Protection
AUGT	Automated Urban Guided Transport (from IEC 62267 title)
BAMS	Braking and Adhesion Management System
BI	Basic Integrity
CCS	Control Command and Signalling (TSI)
CCTV	Closed-Circuit Television
CoP	Code of Practice
CSM-RA	Common Safety Method for Risk Assessment
CTC	Centralized Traffic Control
DC	Direct Current
DCU	Door Control Unit
DGUV	Deutsche Gesetzliche Unfallversicherung (German Social Accident Insurance)
DMI	Driver-Machine Interface
EB	Emergency Brake
EBO	Eisenbahn-Bau- und Betriebsordnung (German Railway Construction and Operating Regulations)
EMC	Electromagnetic Compatibility
EMU/DMU	Electric Multiple Unit / Diesel Multiple Unit
EN	European Standard
EOA	End of authority
ERTMS	European Rail Traffic Management System
ER-JU	European Railway – Joint Undertaking
ETCS	European Train Control System
ETCS-OB	ETCS On-Board

EuRail	European Railway
FA	Flagship Area/ Functional Area
FIS	Functional Interface Specification
FS	Full Supervision (ETCS mode)
GoA	Grade of Autonomation (e.g., GoA3, GoA4)
HazAna	Hazard Analysis
HAZOP	Hazard and Operability study
HVAC	Heating, Ventilation, and Air Conditioning
IEC	International Electrotechnical Commission
IM	Infrastructure Manager
IMS	Incident Management System
JP	Journey Profile
LOA	Limit of Authority
LOC&PAS	Locomotive and Passengers (TSI)
MA	Movement Authority
MP	Mission Profile
NBÜ/NBA	Notbremsüberbrückung / Notbremsanforderung (Emergency Brake Override / Emergency Brake Request)
OAS	On-board Automatic System
OBU	On-Board Unit
OCC	Operational Control Center
OPE	Operation (TSI)
PEA	Passenger Emergency Alarm
PER	Perception
PHA	Preliminary Hazard Analysis
ppm	Parts per million
R2DATO	Rail To Digital Automated Up To Autonomous Train Operation
RAM	Reliability, Availability and Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAP	Roll Away Protection
RBC	Radio Block Centre
REP	Repository
Ril	Richtlinie (German Guideline/Directive)

RiskAna	Risk Analysis
RU	Railway Undertaking
S2R	Shift2Rail
SB	Safety Barrier
SFE	Safe End
SH	Shunting (ETCS mode)
SHA	System Hazard Analysis
SIL	Safety Integrity Level (e.g., SIL2)
SP	System Pillar
SR	Staff responsibility (ETCS mode)
SRAC	Safety Related Application Conditions
SRS	System Requirement Specifications
StVO	Straßenverkehrs-Ordnung (German Road Traffic Regulations)
SUC	System Under Consideration
TBD	To be determined
TCC	Traffic Control Centre
TCMS	Train Control Management System
TFFR	Tolerable Functional Failure Rate
THR	Tolerable Hazard Rate
TIMS	Train Integrity Monitoring System
TMS	Traffic Management System
TSI	Technical Specification for Interoperability
TSI ENERGY	Technical Specification for Interoperability relating to the 'Energy' subsystem
TSI LOC&PAS	Technical Specification for Interoperability relating to the 'rolling-stock-locomotives and passenger rolling stock' subsystem
TSI OPE	Technical Specification for Interoperability relating to the "operation and traffic management" subsystem
UC	Use Case
UDMP	Unauthorised Direction Movement Protection
UNISIG	Union des Industries de Signalisation (Union of Signalling Industries)
WP	Work Package (e.g., WP 5.1, WP 6.1, WP 8.1, WP 8.2, WP 8.3, WP 8.4)
X2Rail4	Shift to Rail 4

TABLE OF CONTENTS

Acknowledgements.....	2
Report Contributors.....	2
Executive Summary	4
Overview	5
Abbreviations and Acronyms	7
Table of Contents.....	10
List of Figures	12
List of Tables	13
1. Introduction	14
2. Background.....	16
3. Implementation of Grant Agreement tasks	17
3.1. Scope of the Safety Analysis	17
3.2. Deliverable Description.....	17
3.3. Task Description.....	18
4. Methodology	19
4.1. Scope, Limits and interfaces of the safety analysis.....	19
4.2. Assumptions.....	21
4.3. System Definition.....	23
4.4. Hazard analysis.....	23
4.4.1. Hazard identification inputs.....	23
4.4.2. Hazard identification process.....	24
4.4.3. Hazard classification process.....	26
4.4.4. Identified hazards and related accidents.....	27
4.5. Risk analysis	27
4.5.1. Risk Acceptance Principles.....	27
4.5.2. Codes of Practice	27
4.5.3. Similar Reference Systems.....	35
4.5.4. Explicit Risk Estimation.....	35
4.6. Review of the Safety Analysis.....	39
5. Technical Conclusions	40
5.1. Automating Functions.....	41
5.2. Out of Scope Hazards	41

5.3.	Hazards partially analysed.....	42
5.4.	Hazards completely controlled by Code of Practice	42
5.5.	Hazards Partially controlled by Code of Practice	46
5.6.	Hazards not controlled by Code of Practice	56
5.7.	Hazards linked to other Hazards.....	59
6.	Conclusions	61
6.1.	Proposal of future work packages.....	62
6.2.	Opportunities for further development.....	63
6.3.	Gained insights.....	63
7.	References.....	65
7.1.	Input documents.....	65
7.2.	Safety Regulations and Safety Standards.....	65
7.3.	Technical regulations and standards	66
ANNEX A.	Hazard Log	69
ANNEX B.	Hazard List	70
ANNEX C.	External Safety Barriers and Safety related application conditions.....	75
ANNEX D.	Final THR for the Hazards	91
ANNEX E.	Explicit risk Evaluation – risk reduction	97
ANNEX F.	HAZOP	100
ANNEX G.	Risk Analysis	101

LIST OF FIGURES

Figure 1 - Methodology flow chart	15
Figure 2 - Safety analysis scope and limits within R2DATO WP 8	20
Figure 3 - Extract from the WP 8.1 HAZOP table - hazard identification for UC5.1-011, step 1, and related requirements	25
Figure 4 - Extract from the Hazard Log - backward traceability in column E (traceability from the Hazard Log to the HAZOP table).....	25
Figure 5 - Extract from the Hazard Log - forward traceability (traceability from the HAZOP table to the Hazard Log)	25
Figure 6 - Hazard log cells dealing with the hazard classification	26
Figure 7 - Hazards controlled by CoP	28
Figure 8 - Application of Code of Practice	34
Figure 9 - Relation Automating Functions and Hazards	38
Figure 10 - Possibilities of mitigation of the hazards.....	40

LIST OF TABLES

Table 1 - Grades of Automation high level description (source: subset - 125_v1.0.0)	16
Table 2 - Assumptions made in the risk analysis.....	21
Table 3 - Severity classification.....	26
Table 4 - Applied codes of practice	28
Table 5 - Harmonised design criteria from CSM-RA.....	36
Table 6 - Design criteria, extension to marginal and insignificant severity	36
Table 7 - SIL and TFFR according to EN50129 [6].....	39
Table 8 - Out of scope hazards	41
Table 9 - Hazards partially analysed	42
Table 10 - Hazards completely controlled by Code of Practice.....	42
Table 11 - Hazards partially controlled by Code of Practice	46
Table 12 - Hazards not controlled by Code of Practice	57
Table 13 - Hazards with no Code of Practice and no external safety barriers.....	58
Table 14 - Hazards linked to other hazards.....	59
Table 15 - Proposal for future Work Packages.....	62
Table 16 - Opportunnities for further development	63
Table 17 - Input documents	65
Table 18 - Legal safety framework	65
Table 19 - Safety standards – processes	66
Table 20 - List of referenced TSI.....	67
Table 21 - List of other referenced standard.....	68
Table 22 - Hazard list.....	70
Table 23 - List of applied Codes of Practice	75
Table 24 - List of applied existing safety barriers	86
Table 25 - List of proposed new safety barriers.....	87
Table 26 - List of derived Safety related application conditions (SRAC)	87
Table 27 - Final THR per hazard.....	92
Table 28 - Initial THR based on the harmonised design criteria from CSM-RA [2] and [3].....	97
Table 29 - Risk Analysis columns explanation	101

1. INTRODUCTION

This document is the deliverable of Working Group 8, Task 8.1, in the context of the R2DATO project. It contains information about the hazard log and the safety analysis regarding Automating Functions.

The Safety Analysis was based on Use Cases and ATO Requirements which were developed within WP 5, task 5.1 based on input from SP (System Pillar) and related Flagship Areas (FAs) (e.g. regarding demonstrators). [1] Additionally the functional System Requirements developed in WP 6, task 6.1 based on the use cases and operational parameters defined in WP 5 were also considered in this Safety Analysis. [2] The objective of this analysis is to provide an overview of operational hazards and their corresponding THR for future design, architecture and implementation activities.

Chapter 3, specifies how the tasks from the Grant Agreement are integrated. The Safety Analysis methodology is then described in Chapter 4. Thereafter, Chapter 5 presents the technical safety analysis conclusions and chapter 6 proposes subsequent working items.

Other main results of the task are:

- The list of operational hazards, documented in ANNEX B.
- The list of external safety barriers; they are the technical, organisational or operational measures which are outside of the System under Consideration (SUC) and completely independent on the SUC. They can reduce or eliminate the probability that a hazard evolves into an accident or reduce the accident consequences. The identified technical, operational and human safety barriers are intended as requirements which are expected to be fulfilled by systems outside of the SUC, i.e. as SRAC (safety related application conditions). They are documented in ANNEX C.
- The list of the final THR for each hazard, listed in ANNEX D.
- The List of applicable Code of Practices containing relevant safety requirements in chapter 4.5.2 and included in the safety analysis in ANNEX G.

The main steps of the safety analysis are documented and explained in Chapter 4. The outlined processes help clarify how the safety results were achieved and are illustrated in Figure 1 as follows:

- Systematically identify the hazards through a HAZOP
- Identify the hazard severity, based on the hazard consequences (accidents)
- Identify whether the hazard could be completely controlled by codes of practice or similar reference system and document the applicable related safety requirements
- If a hazard could not be completely controlled by codes of practice or similar reference systems, then:
 - Allocate an initial THR to the identified hazards; the initial THR is based on the unmitigated hazard severity.
 - Detect external safety barriers which can mitigate the risk related to the hazard and thus the THR.
 - Calculate a final THR for each hazard; the final THR considers the mitigation provided by the external safety barriers.

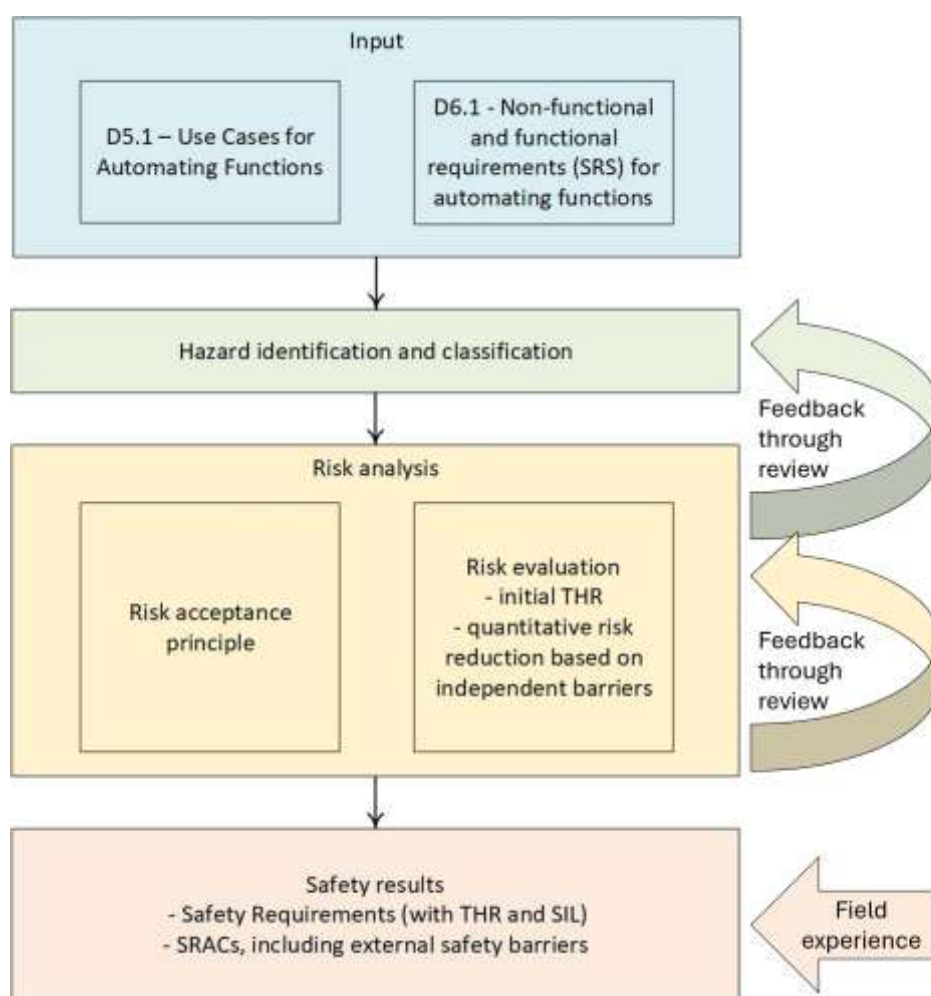


Figure 1 - Methodology flow chart

2. BACKGROUND

The European Railways are currently in the process of implementing ERTMS. A further step in achieving improved capacity, on-time performance and opportunities to realise energy efficiency improvements is to develop and implement ERTMS/ATO.

ERTMS/ATO covers a wide range of applications from manually assisted to fully automated train operation. Possible actual operation depends on the desired grade of automation (GoA) and the automation level supported by IM on a specific route.

The definition of GoA arises from apportioning responsibility for the given functions of railway operations between operational staff and involved technical railway systems. The Table 1 below defines the operation principles for each GoA level.

The safety analysis documented in this report focuses on GoA3 and GoA4.

Table 1 - Grades of Automation high level description (source: subset - 125_v1.0.0)

GoA	GoA Name	Train Operator	Description
GoA1	Non automated train operation	Train driver in the cab	The train is driven manually; but protected by automatic train protection (ATP). This GoA can also include providing advisory information to assist manual driving.
GoA2	Semi-automated train operation	Train driver in the cab	The train is driven automatically, stopping is automated but a driver in the cab is required to start automatic driving of the train, the driver can operate the doors (although this can also be done automatically), the driver is still in the cab to check the track ahead is clear and carry out other manual functions. The driver can take over in emergency or degraded situations.
GoA3	Driverless train operation	Train attendant on-board the train	The train is operated automatically including automatic departure, a train attendant has some operational tasks, e.g. operating the train doors (although this can also be done automatically) and can assume control in case of emergency or degraded situations.
GoA4	Unattended train operation	No staff on-board competent to operate the train	All functions of train operation are automatic with no staff on-board to assume control in case of emergencies or degraded situations.

3. IMPLEMENTATION OF GRANT AGREEMENT TASKS

The Task 8.1 focused on Safety and covered the following subjects regarding automating function:

- Hazard identification,
- Hazard Log and
- Safety Management Report

The scope of the analysis is described in the following chapter 3.1, together with the deliverable description in chapter 3.2 and the task description from the Grant Agreement [3] in chapter 3.3.

3.1. SCOPE OF THE SAFETY ANALYSIS

The safety analysis identifies hazards linked to the Automating Functions, based on the Use Cases provided by WP 5.1 [1] and on the requirements provided by WP 6.1 [2].

This safety analysis presents the hazard identification, mitigations, risk evaluation, and the final Tolerable Hazard Rate (THR) per hazard after the mitigations have been applied.

3.2. DELIVERABLE DESCRIPTION

	Deliverable description from Grant Agreement [3]	Output of deliverable
Deliverable 8.1	<p>“Safety Analysis for automating functions”</p> <p>This deliverable will contain information about the safety analysis (e.g., PHA, SHA), safety management and hazard log</p>	<p>The safety analysis to be found in ANNEX F and ANNEX G</p> <p>The Hazard Log is to be found in ANNEX A</p>

3.3. TASK DESCRIPTION

	Task definition from Grant Agreement [3]	Output of deliverable
Task 8.1	In relation to the ongoing development a continuous examination regarding safety aspects must be done. Therefore, the preliminary hazard identification process for each use case and operational scenario must be done, inclusive safety risk assessment for each requirement, function, task.	<p>A safety analysis, including the hazard identification/ analysis and the risk assessment, has been carried out.</p> <p>The safety analysis is based on the requirements, functions, tasks (e.g. outcomes and steps) outlined in document "D5.1" delivered by WP 5.1, [1] and the system requirements detailed in document "D6.1" provided by WP 6.1 [2]</p> <p>Task 8.1 resulted in a comprehensive risk assessment that evaluates the identified hazards, describes safety barriers, and determines final safety classifications through detailed calculations.</p>

4. METHODOLOGY

The safety analysis aims to identify the final Tolerable Hazard Rate (THR) for hazards associated with Automating Functions. This analysis has been executed in two distinct stages.

The first stage comprises the hazard identification and classification, which is based on the Use Cases for Automating Functions provided by WP 5.1 [1] and the System Requirements delivered by WP 6.1. [2]

The second stage involves a comprehensive risk assessment, during which safety barriers were identified and evaluated. These measures serve to mitigate both the consequences and probability of accidents resulting from the identified hazards.

External and already existing safety barriers, independent of ATO, have been identified and evaluated. They can be technical, operational or organisational safety measures. The external safety barriers have not been developed specifically to manage ATO risks; they nevertheless exist in the railway environment and can help mitigate ATO risks as well, with complete independence on ATO. An example of an external safety barrier is ATP: although not designed with ATO in mind, an ATP with continuous speed supervision is a sufficient safety measure to handle hazards related to overspeed, even if caused by Automating Functions.

External safety barriers have thus been considered to avoid overestimating the safety requirements necessary for ATO. Some external safety barriers are explicitly documented within Codes of Practice.

In case external safety barriers prove insufficient to reduce risks to tolerable levels, additional safety requirements are needed to allow a safe operation with Automating Functions.

External safety barriers have been documented as SRACs, i.e. as necessary safety relevant preconditions that the systems outside ATO need to fulfil. If, for a specific application, the SRACs are not complied with, the risks need to be re-evaluated at a specific application level.

The analysis flow is pictured in Figure 1.

4.1. SCOPE, LIMITS AND INTERFACES OF THE SAFETY ANALYSIS

This safety analysis addresses hazards that may arise from the Use Cases regarding Automating Functions as defined by WP 5.1 [1], while incorporating System Requirements provided by WP 6.1 [2] for hazard identification.

The hazard identification process employs a top-down approach based on the Automating Functions, their Use Cases, and the System Requirements. This systematic approach ensures comprehensive identification of potential hazards at both system and operational levels while maintaining traceability to functional requirements.

The subsequent sections and the Figure 2 detail specific exclusions from this WP 8.1 safety analysis:

- No bottom-up analysis based on the detailed ADM, APM and REP functions
 - WP 8.1 does not cover the bottom-up analysis for the ADM, APM and REP functions
 - WP 8.3 performed a bottom-up analysis, starting from each of the ADM, APM and REP logical functions, evaluating the impact on safety of their failures. On the contrary, WP 8.1 provided a top-down, high level operational safety analysis based on the deviations from the expected operational behaviour (as defined in the Use Cases from WP 5.1) and from the high-level system requirements (as defined by WP 6.1).
- No detailed analysis of the PER Use Cases and requirements
 - WP 8.1 does not cover the detailed PER safety analysis.
 - WP 8.2 performed the detailed safety analysis related to the specific PER Use Cases (as defined within D5.2) and requirements (as defined within D6.3).
- No remote driving hazards
 - WP 8.1 does not cover functions and hazards related to remote driving. The safety analysis covering the remote driving is planned to be performed by WP 8.4.
- No final safety results for the overall R2DATO WP 8 scope
 - The overall safety results for the whole R2DATO WP 8 scope require a harmonization and consolidation of the results produced by the WP 8.1, WP 8.2, WP 8.3 and WP 8.4 safety analysis. This consolidation and harmonization task is outside the scope of WP 8.1.

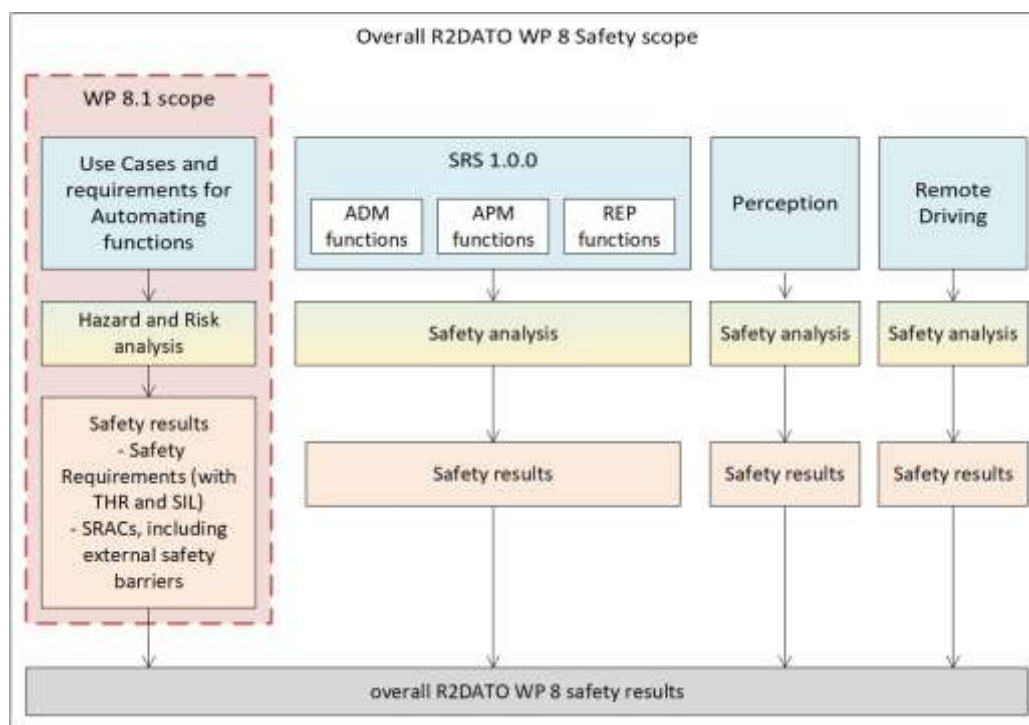


Figure 2 - Safety analysis scope and limits within R2DATO WP 8

4.2. ASSUMPTIONS

The Table 2 compiles the assumptions used in the safety analysis, encompassing general assumptions, hazard-specific assumptions, and items defined as outside the analytical scope.

Table 2 - Assumptions made in the risk analysis

Assumption ID	Assumption	Hazard ID
Overall assumptions		
AS_01	<p>this safety analysis covers the following operational mode:</p> <p>GoA3 and GoA</p> <p>ETCS FS Automatic Driving (AD)</p> <p>The safety results are not valid and not applicable for other operational modes</p>	General
Hazard specific assumptions made for the HazAna		
AS_02	Operation under ETCS Full Supervision/ ATP	H8.1-01-2 H8.1-01-3 H8.1-09 H8.1-13-4 H8.1-11-2
AS_03	<p>This analysis is valid for dual-mode vehicles. (two different electrical power supplies)</p> <p>This analysis is not covering the train going through a system/ phase separation with the pantograph raised.</p>	H8.1-02
AS_04	This analysis is about applying the parking brake. National parking brake requirements shall be followed while applying the parking brake.	H8.1-03-1
AS_05	If the Emergency brake is requested by a passenger, the request is transmitted to the OCC.	H8.1-03-3
AS_06	The door traction interlock is implemented as a SIL2 function on the vehicle	H8.1-05-2-c
AS_07	The door release inhibition at speed is implemented as a SIL2 function on the vehicle	H8.1-05-2-e
AS_08	<p>The analysis excludes hydraulic brakes.</p> <p>The analysis excludes battery powered train.</p> <p>The analysis excludes hydrogen powered train.</p>	H8.1-07

Assumption ID	Assumption	Hazard ID
AS_09	The analysis excludes dangerous cargo.	H8.1-07 H8.1-10-1
AS_10	In general, there are existing rules to pay attention in the near of rail track (in Germany for maintenance: Regulation for staff: "DGUV Verhalten bei Arbeiten im Gleisbett"/RIL 132.0118) and prohibition to access rail track (§ 62 EBO), Head lights/marker lights on vehicle side is standard.	H8.1-11-1
AS_11	The analysis considers two scenarios: train passing persons at platform and inside a tunnel.	H8.1-11-3
AS_12	All the preconditions independent on ATO for a safe evacuation are fulfilled. The analysis only deals with the following scenario: the evacuation cannot safely take place due to reasons directly or indirectly involving ATO. Every safe area or every place where the accident had happened has the same effect for the passengers (same infrastructure, same distance to hospital, doctors and fire brigade available). The Passenger Information System is not considered as a safety barrier as it is Basic Integrity.	H8.1-12-1
AS_13	GOA level is primarily managed by the APM for GOA3/4 and Driver for GOA0/1/2	H8.1-13-1-c
AS_14	The analysis is linked to the following scenario: A train not intended or authorised to operate in a specific ETCS mode is incorrectly placed or remains in that mode.	H8.1-13-3
AS_15	There are two scenarios for this hazard: lost train position or lost train communication. 1. Position Loss During Start of Mission (Train Wake-up) 2. Position/Communication Loss During Operation	H8.1-13-4
AS_16	For moving block TIMS is required.	H8.1-14
AS_17	The analysis depends on the kind of self-check; therefore WP 8.1 did not perform a detailed analysis for this hazard.	H8.1-16-1

Assumption ID	Assumption	Hazard ID
"Out of scope" assumptions		
AS_18	Adhesion factor related hazards cannot be determined as the implementation of it is considered not yet established	General
AS_19	Process related to driver changing from GoA3/4 to GoA2/1/0 although previously defined it has been considered out of scope as the process doesn't look completely defined.	General
AS_20	Bomb alarm is out of the scope of WP 8.1(security)	H8.1-07
AS_21	Out of scope	H8.1-08
AS_22	out of scope, because there are standards and tools which handle this	H8.1-13-2
AS_23	out of scope, need to be analysed by another WP	H8.1-13-3-b
AS_24	out of scope	H8.1-15-1
AS_25	out of scope	H8.1-15-2
AS_26	out of scope	H8.1-15-3

4.3. SYSTEM DEFINITION

The target system is an interoperable ERTMS/ATO system supporting multiple grades of automation. This document specifically addresses GoA3/4, representing an evolution toward autonomous trains. The system builds upon GoA2 functions specified in TSI 2022 while incorporating new functions required for GoA3/4. For detailed specifications, please refer to the SRS.

4.4. HAZARD ANALYSIS

This chapter illustrates the safety methodology for the hazard identification and classification and illustrates how the hazard identification is documented in the hazard log.

4.4.1. Hazard identification inputs

The hazard identification process (carried out with an approach based on the HAZOP technique) incorporates two primary sources: the operational Use Cases documented in "D5.1" from WP 5.1 [1], and the functional and non-functional System Requirements for Automating functions specified in document "D6.1" from WP 6.1. [2]

Deliverable "D5.1" [1] documents a total of 74 use cases and 29 operational scenarios. Following a 'day in the life of a train' approach, these scenarios and their corresponding use cases provide a comprehensive operational framework.

Given time constraints and delayed formal inputs from other tasks, WP 8.1 started their analysis based on the Use Cases from D5.1 [1] and then incorporated later the System Requirements from D 6.1 [2] in its analysis.

Regulations and Standards that have been considered to support the hazard identification re listed in chapter 7.2.

The results of previous Shift2Rail projects have been analysed and incorporated to the extent that they conform with the results of Work Packages 5 and 6.

The specific safety results from Shift2Rail4 have been fully implemented into Work Package 8.3. The results from TAURO were also considered.

4.4.2. Hazard identification process

The WP 8.1 utilized an approach based on the Hazard and Operability (HAZOP) study because it provides a highly structured and systematic approach to identify potential hazards and operability issues within its system. This methodology, conducted by a multi-disciplinary team, allowed the WP 8.1 to proactively scrutinize deviations from design intent by systematically applying guide words to process parameters. Its effectiveness lies in uncovering potential causes, consequences, and necessary safeguards.

The WP 8.1 started the hazard identification by systematically going through each Use Case from D5.1 [1]. Deviations from the Use Case expected outcomes and, where necessary, steps were investigated. Where necessary HAZOP guide words were used to support the analysis.

Hazardous deviations and failures (i.e. deviations which could results in harm to persons or loss of human life) were listed down and further analysed, identifying the related hazards and potential accidents.

Requirements from D6.1 [2] were linked to the corresponding steps of the Use Cases from D5.1 [1] and similarly analysed to identify additional hazardous deviations, hazards and accidents.

The HAZOP is documented in the HAZOP table, see ANNEX F. The HAZOP contains 1852 rows, with one or more rows for each outcome and step of each of the 74 Use Cases, integrated by additional rows for the system requirements (ATOREQ). The complete HAZOP table is found in ANNEX F and an extract is to be found in Figure 3. Although systematic and complete, the HAZOP table is not easily readable. It also includes many duplicated hazards, as several different deviations and failures could result in the same hazard.

A separate hazard log was therefore created to consolidate the hazard identification and the related information coming from the HAZOP. The Hazard Log has only 63 rows, with each row dedicated to a different, standardized hazard. Hazards from the HAZOP were linked to the standardized hazards in the hazard log. The hazard traceability is bidirectional (from the HAZOP to the Hazard Log and vice versa).

The performed hazard identification meets the applicable requirements from the European Regulation 402/2013 (CSM-RA) and the CENELEC EN50126-2.

4.4.3. Hazard classification process

Each hazard has the potential to lead to one or more types of accidents (e.g. a collision). A set of high-level accident categories has been defined, and hazards have been assigned to the relevant categories. These accident categories are further associated with their possible consequences, such as fatalities and weighted injuries. For example, accidents categorized as “collisions” or “derailment” involving passenger trains are considered “catastrophic”. Consequently, the classification of hazards is based on the severity of the accident category they may trigger (see also Figure 6). The performed hazard classification meets the applicable requirements from the European Regulation 402/2013 (CSM-RA) [2] and [3] and the CENELEC EN50126-2 [5].

The results of the hazard identification process have been documented within the hazard log, as shown in the following Figure 6.

Hazard		related UC	Accidents	Risk Evaluation without Safety B	
ID	description			Severity Category	Severity Justification
HB.1-01	vehicle movement				
HB.1-01-1	Vehicle untimely sets itself in motion by applying traction from standstill	UC5.1-007, UC5.1-012, UC5.1-015, UC5.1-017, UC5.1-025, UC5.1-027, UC5.1-028, UC5.1-028, UC5.1-032, UC5.1-033, UC5.1-057, UC5.1-066, UC5.1-070, ATOREQ.38, ATOREQ.39, UC5.1-012, UC5.1-018	Train-train collision	Catastrophic	Derailment due to possible flank collision leading to several injuries or death and high damage on infrastructure

Figure 6 - Hazard log cells dealing with the hazard classification

Hazard severity

Hazards are described and classified according to the severity classification of the potentially associated accidents. The severity categories meet the applicable requirements from the European Regulation 402/2013 (CSM-RA) and the CENELEC EN50126-2.

Table 3 - Severity classification

Severity category	Consequences to persons
Catastrophic	Affecting a large number of people and resulting in multiple fatalities and/or multiple severe injuries and/or major damage to the environment resulting from an accident
Critical	Affecting a very small number of people and resulting in at least one fatality
Marginal	No possibility of fatality, at most one severe injury or multiple minor injuries only
Insignificant	Possible one minor injury

4.4.4. Identified hazards and related accidents

The complete hazard identification results are documented in the Hazard Log, which can be found in ANNEX A. An overview on the hazard management, including the complete list of identified hazards, can be found in ANNEX B.

4.5. RISK ANALYSIS

4.5.1. Risk Acceptance Principles

The risk acceptance principles have been selected in accordance with the European regulation 402/2013 (CSM-RA) [2] and [3] and the CENELEC EN 50126-2 [7]:

- Codes of practice
- Similar reference systems
- Explicit risk estimation

The risk evaluation criteria and the process to derive the safety requirements are presented separately for each of the risk acceptance principle in the following sections.

4.5.2. Codes of Practice

Whenever possible, Codes of Practice (CoP) have been applied to manage the related applicable WP 8.1 hazards. As Automating Functions are an innovation for railways, no Codes of Practice are available to completely and specifically control the hazards linked to Automating Functions. At the same time, Codes of Practice developed for other systems can be applicable to completely or partially control selected WP 8.1 hazards.

For instance, deviations from the Use Cases and system requirements for Automating Functions might result in overspeed. Technical solutions independent on Automating Functions, as ETCS FS or class B systems with ATP are available and documented in the related technical literature (CoP). Such solutions can control the “overspeed” hazard, independently on its cause, be it a failure of an Automating functions or a different reason.

As the Codes of Practice apply to systems outside the Automating Functions, they usually cannot be used as Safety Requirements for the Automating Functions, but rather as SRACs (Safety Relevant Application Conditions), i.e. a set of preconditions that systems outside the scope of the Automating Functions need to fulfil, to allow the safe operation with the Automating Functions.

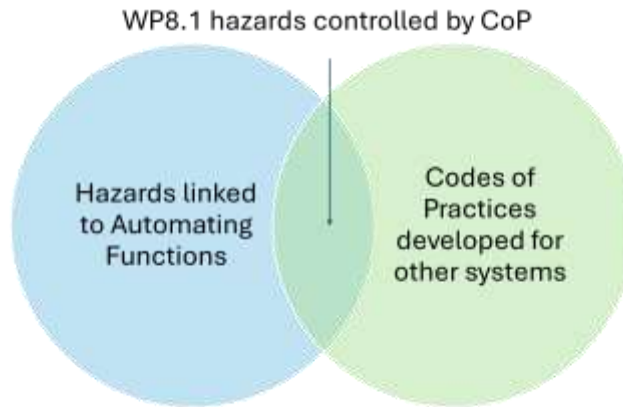


Figure 7 - Hazards controlled by CoP

The following codes of practice were deemed applicable to completely or partially control specific hazards in the GoA3 and GoA4 context:

Table 4 - Applied codes of practice

Code of Practice	Specific function or general description	Managed hazards
Subset-026 Set of specifications 3 (ETCS B3 R2 GSM-R B1) - System Requirement Specification	<p>This subset is the requirement specification for ERTMS/ETCS equipment. Additionally, Subset-91 indicates the SIL level of some of the safety related functions of the SS026.</p> <p>The main functionalities of defined in the SS026 are related to train distance and speed supervision.</p>	<p>H8.1-01-1-a Vehicle untimely sets itself in motion by applying traction from standstill</p> <p>H8.1- 01-3 excessive speed</p> <p>H8.1- 01-2 Vehicle travels in the wrong direction</p> <p>H8.1-03-1, Parking brake force reduced or not given</p> <p>H8.1- 13-4 Train location</p> <p>H8.1-05-1-a, Doors are released on the wrong side or outside of a safe area for the passenger exchange</p> <p>H8.1-05-2-a, unexpected train movement while people are boarding or leaving the train - rolling backward</p> <p>H8.1-09, Hazard due to two trains approaching each other with excessive speed</p>

Code of Practice	Specific function or general description	Managed hazards
		<p>H8.1-13-1-a, hazard due to wrong JP</p> <p>H8.1-13-1-b, hazard due to wrong MP</p> <p>H8.1-13-3, hazard due to wrong ETCS mode</p> <p>H8.1-13-4, hazard due to lost train location or train communication</p> <p>H8.1-13-4, hazard due to lost train location</p>
Subset-034 Train interface FIS, section 2.4.6 "Station platform"	The subset specifies the functional interface between the ERTMS/ETCS on-board equipment and the train.	H8.1-05-1-a, Doors are released on the wrong side or outside of a safe area for the passenger exchange
Subset-036 Eurobalise FFFIS	The subset specifies the interface between the ERTMS/ETC equipment and the Eurobalises.	H8.1-05-1-a, Doors are released on the wrong side or outside of a safe area for the passenger exchange
Subset-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 and 2	The subset defines the generic high-level quantitative safety requirements for ETCS operating in either Level 1 or Level 2	H8.1-14, loss of train integrity
Subset-125 ERTMS/ATO System Requirement Specification- System Requirements Specification for ERTMS/ATO	<p>The subset specifies the system requirements that must be fulfilled in order to provide an interoperable solution for ERTMS/ATO (GoA2)</p> <p>This subset is not safety-related it is meant to be used together with Subset 026.</p>	<p>H8.1-13-1-a, hazard due to wrong JP</p> <p>H8.1-13-1-b, hazard due to wrong MP</p> <p>H8.1-05-1-a, Doors are released on the wrong side or outside of a safe area for the passenger exchange</p>

Code of Practice	Specific function or general description	Managed hazards
		H8.1-13-3, hazard due to wrong train ETCS mode
TSI LOC&PAS Technical Specification for Interoperability relating to the 'rolling-stock-locomotives and passenger rolling stock' subsystem of the rail system in the European Union.	This TSI provides information on the application of the Technical Specification for Interoperability for the 'Conventional Rail Locomotives and Passenger Rolling Stock' subsystem	<p>H8.1-03-3, Passenger emergency brake request fails</p> <p>H8.1-04, Insufficient track guidance, track guidance fails, derailment</p> <p>H8.1-05-1-b, Persons trapped in the external door frame</p> <p>H8.1-05-1-d, Persons fall in the gap between the platform and the train</p> <p>H8.1-05-2-c, unexpected train movement while people are boarding or leaving the train - traction applied by the train</p> <p>H8.1-05-2-a, unexpected train movement while people are boarding or leaving the train - Scenario: train rolling backward</p> <p>H8.1-06, Ignition and Fire (partially)</p> <p>H8.1-10-3, Hazard to passengers due to unexpected, excessive train movements during travel</p> <p>H8.1-12-3, Insufficient availability of vehicle functions required in an emergency</p> <p>H8.1-12-4, passenger get nervous/ panic</p> <p>H8.1-05-1-a, Doors are released on the wrong side or outside of a safe area for the passenger exchange</p> <p>H8.1-05-1-d, Persons fall in the gap between the platform and the train</p>

Code of Practice	Specific function or general description	Managed hazards
		<p>H8.1-05-1-b, Persons trapped in the external door frame</p> <p>H8.1-05-2-d, unexpected train movement while people are boarding or leaving the train - scenario: unexpected jogging of the train</p> <p>H8.1-05-2-e, Door's release command while the train is moving</p> <p>H8.1-06-2, hot wheel</p> <p>H8.1-12-5, Hazards due to Insufficient ventilation/air conditioning in case of emergency</p>
TSI ENERGY Technical Specification for Interoperability relating to the 'Energy' subsystem of the rail system in the European Union.	This TSI covers various aspects of the railway system, including the energy subsystem, which is crucial for the consistent power supply required for trains to operate across different national networks.	H8.1-02, vehicle sets wrong traction system
TSI OPE Technical Specification for Interoperability relating to the "operation and traffic management" subsystem of the rail system in the European Union. - Appendix D - Route compatibility and Route Book – Gauging	<p>This TSI is a set of regulations that define the technical and operational standards for the operation and traffic management subsystem of the rail system within the European Union.</p> <p>The TSI OPE- Appendix D mentions that the compatibility between the vehicle and route needs to be ensured, with reference to the vehicle gauge and platform dimension. The specific parameters are defined at a national level.</p>	H8.1-05-1-d, Persons fall in the gap between the platform and the train

Code of Practice	Specific function or general description	Managed hazards
EN 50388-1:2022 – Railway Applications - Fixed installations and rolling stock - Technical criteria for the coordination between electric traction power supply systems and rolling stock to achieve interoperability	This standard establishes technical criteria for the coordination between electric traction power supply systems and rolling stock to achieve interoperability in railway applications.	H8.1-02, vehicle sets wrong traction system
- EN 50122 series – Railway applications – Fixed installations – Electrical safety, earthing and the return circuit	The standard deals with protection against electric shock and stray currents for railway applications.	H8.1-02, vehicle sets wrong traction system
- EN 50121 series – Railway applications – Electromagnetic compatibility (EMC)	EN 50121 series The standards defines a set of requirements for managing electromagnetic compatibility (EMC) in railway applications across Europe	H8.1-02, vehicle sets wrong traction system
EN 50119 – Railway applications – Fixed installations – Electric traction overhead contact lines	The standard specifies the requirements for overhead contact line systems used in railway applications	H8.1-02, vehicle sets wrong traction system
EN 16185-1 Railway Application – Braking Systems of Multiple Unit Transit-	The standard provides detailed requirements and definitions for the braking systems used in self-propelling thermal and electric trains operating on the European rail system network	H8.1-03-1, Braking force reduced or not given ⁴

Code of Practice	Specific function or general description	Managed hazards
EN 15663 Railway Application – Vehicle reference mass	The standard defines reference masses for vehicles. It specifies the forces and moments to consider regarding vehicle masses and braking conditions and provides a method for stress calculation of axles with outside axle journals.	H8.1-03-1, Braking force reduced or not given
EN 14752:2019+A1:2021- Railway Applications – Bodyside entrance systems for rolling stock.	The standard defines the design, construction, and maintenance of bodyside entrance systems for rolling stock	H8.1-05-2-e, Door's release command while the train is moving
EN14363 dynamic behaviour of trains Testing and Simulation for the acceptance of running characteristics of railway vehicles- Running behaviour and stationary test.	This standard is a guide for testing and simulation for the acceptance of running characteristics of railway vehicles	
EN 15437-1:2009 Railway applications - Axlebox condition monitoring - Interface and design requirements	This standard defines the requirements for axlebox condition monitoring in railway applications.	H8.1-06-2, hot wheel
EN 45545-2:2020 Railway applications - Fire protection on railway vehicles - Part 2:	This standard defines Requirements for fire behaviour of materials and components	H8.1-06-01, H8.1-12-5

Note: the applicability of the Code of Practice principle is limited by two factors:

- no specific Code of Practice exists for dealing with GoA3 and GoA4 operation in complex railway environments
- codes of practice are written based on the assumption that a railway vehicle is driven by a train driver and not by an automated system as in GoA3 and GoA4

Risk evaluation criteria

The following risk evaluation criteria have been applied when a Code of Practice is used to control a specific hazard:

- Is the Code of Practice applicable to the hazard?
- Does the Code of Practice fully control the hazard?

If the Code of Practice does not fully control the hazard, then the explicit risk estimation principle has been applied for the aspects of the hazards which are not controlled.

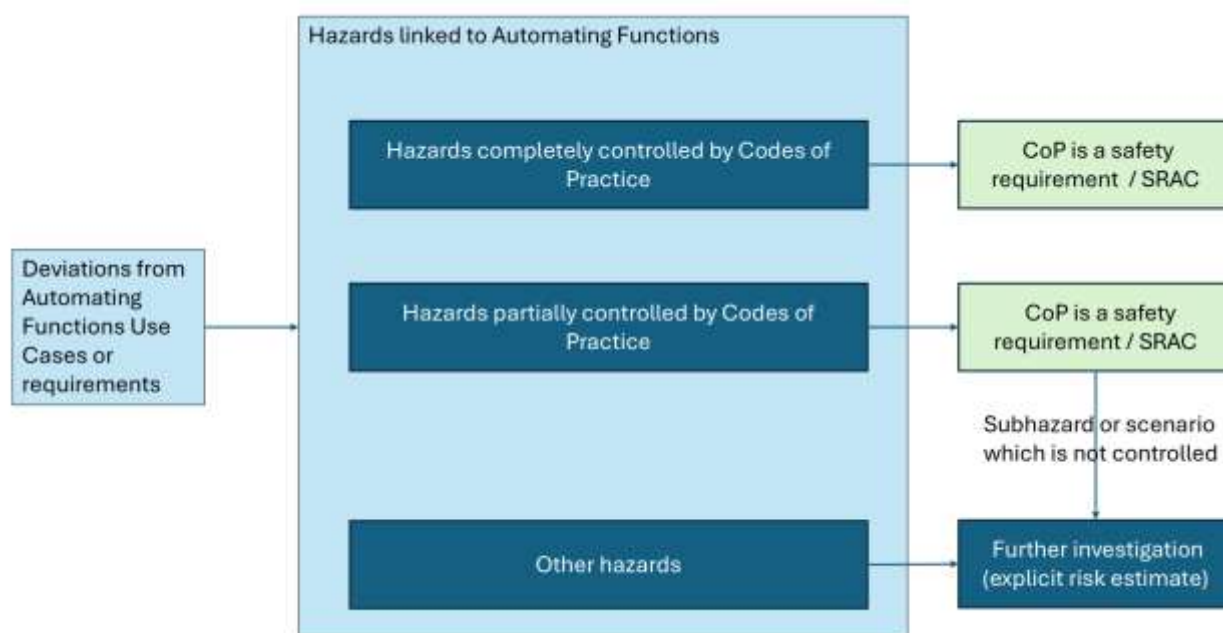


Figure 8 - Application of Code of Practice

Safety requirements

A Code of Practice can completely control a hazard if the application of the Code of Practice, or part thereof, ensures that the associated risk is mitigated to an acceptable level. For the scope of this safety analysis, the application of the Code of Practice needs to ensure an acceptable safety level for the controlled hazard.

For instance, the technical literature defining the ETCS / ATP technical system, defines a technical system which is capable of completely and independently controlling hazards related to overspeed and to the violation of the movement authority (MA)¹. As a result, the technical literature defining the ETCS / ATP technical system has been used as a Code of Practice capable of completely controlling the above-mentioned hazards.

Codes of practice were not written with GoA3 or GoA4 in mind; they on the contrary usually assume that a railway vehicle is driven by a train driver. As a result, it was unclear whether some Codes of Practice could completely control a hazard even under GoA3 and GoA4 operation. In such cases, a deeper investigation with the explicit risk estimation principle has been carried out.

4.5.3. Similar Reference Systems

The safety analysis checked whether similar reference systems could be selected to manage specific hazards. The requirements to be satisfied by a similar reference system have been originally listed down in the CSM-RA 402/2013, Annex II, Article 2.4.2 [4] and have been amended by the Regulation 2015/1136. It has been proven challenging to find an appropriate similar reference system to control any of the identified hazards, given the many specific, unique and complex interfaces, environmental and operational conditions of ATO in the railway context². As a result, no hazard has been managed through the similar reference system principle.

4.5.4. Explicit Risk Estimation

The explicit risk estimation principle has been applied when the codes of practice could not completely control a hazard. In that case, a quantitative analysis has been carried out. When necessary, a quantitative target (THR) for the hazards has been defined.

The explicit risk estimation principle has been applied to most of the identified hazards. More details on the techniques used for the explicit risk estimation can be found in ANNEX E.

¹ This statement is valid under the precondition that the input data for the ETCS / ATP have been entered correctly.

² GoA3 and GoA4 metros and people movers exist. Although they share several aspects with GoA3 and GoA4 railway systems, they present remarkable differences in the operational use and environment compared to a railway system. Even if not directly applicable as a similar reference system, GoA3 and GoA4 safety analyses and safety requirements for metros have been considered to inspire the R2DATO safety analysis.

Risk evaluation criteria

The design criteria from CSM-RA have been applied as risk acceptance criteria for the explicit risk estimation.

Functional failures of the Automating Functions can lead to catastrophic and critical accidents. The CSM-RA defines harmonised design criteria for technical failures with a credible direct potential for catastrophic and critical consequences. These criteria are expressed as Tolerable Functional Failure Rate (TFFR), i.e. the maximum tolerable number of technical failures per hour.

Table 5 - Harmonised design criteria from CSM-RA

Severity category	Consequences to persons	Initial TFFR [failures / h]
Catastrophic	Affecting a large number of people and resulting in multiple fatalities	1E-9
Critical	Affecting a very small number of people and resulting in at least one fatality	1E-7

The harmonised design criteria have been taken as initial TFFR for the technical failures leading to catastrophic and critical accidents. With a similar approach, TFFR values have also been defined for accidents with marginal and insignificant consequences:

Table 6 - Design criteria, extension to marginal and insignificant severity

Severity category	Consequences to persons	Initial TFFR [failures / h]
Marginal	No possibility of fatality, severe or minor injuries only	1E-6
Insignificant	Possible minor injury	1E-5

NOTE on TFFR vs THR

The harmonized design criteria by the CSM-RA are expressed as TFFR (Tolerable Functional Failure Rates): they define the tolerable failure frequency of a specific function.

The THR (Tolerable Hazard Rate) represent the tolerable occurrence frequency of a specific hazard. Hazards and Automatic Functions failures are linked, so also THR and TFFR can be linked: as shown in Figure 9 below, each standardised hazard is caused (or co-caused) by one or more Automating Function failures. As a result:

$$THR = \sum_{i=1}^n TFFR_i$$

Where:

THR = Tolerable Hazard Rate for a specific hazard

TFFR_i = Tolerable Functional Failure Rate of the Automating Function i, independently causing the specific hazard

The THR is the sum of the TFFR of the Automating Functions leading to the hazard. The equation above can always be written as:

$$THR \geq TFFR_j$$

Where:

TFFR_j is the lowest TFFR amongst all the functions causing the hazard

For the WP 8.1 analysis, the following conservative assumption has been made:

$$THR = TFFR$$

So the THR is always greater or equal to the lowest TFFR.

This means that the THR is set as equal to the most restrictive TFFR (i.e. the TFFR with the lowest value).

This is a conservative assumption (i.e. on the safe side). How this conservative assumption impacts the safety results is explained in ANNEX D.

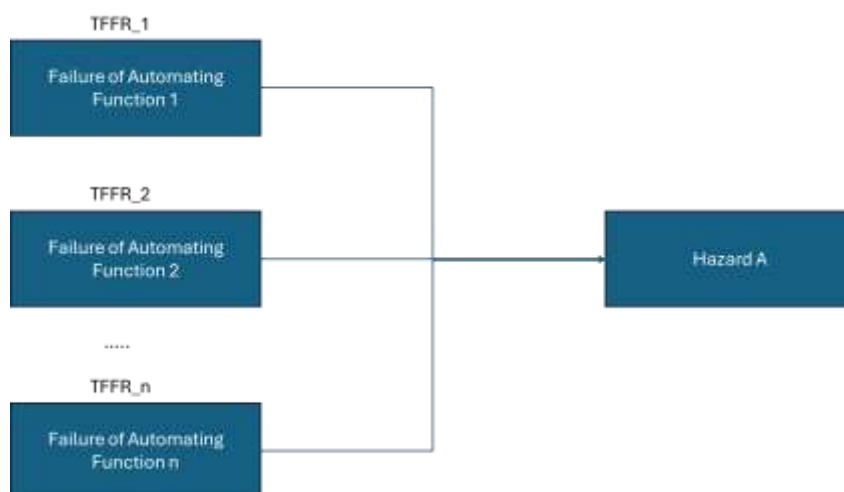


Figure 9 - Relation Automating Functions and Hazards

Safety requirements

The safety requirements defined through the explicit risk estimation are:

- The list of the safety barriers which can reduce the risk caused by the ATO failures
- The final THR for the hazards associated to the functions

External safety barriers and impact on THR

The starting point for the explicit risk estimation process is the initial THR, associated with hazards that have a credible direct potential for catastrophic and critical consequences (see Table 5 and Table 6).

Not every hazard possesses such potential. External barriers can reduce occurrence frequency or mitigate the severity of the potential consequences.

The following external barriers type have been identified:

- Technical barriers: safety functions by external systems (e.g. ATP or TCMS), which can independently mitigate the risk caused by an Automating Function failure.
- Human barriers: safety barriers linked to human intervention, e.g. railway staff in the context of GoA3/4; the human barriers include also operational and organizational barriers, if the operational or organisational barriers can fail due to human error (e.g. the train attendant or the railway undertaking staff check the train before it is taken out of service, to ensure that no passenger is still onboard).
- Physical barriers / preconditions: Some hazards do not directly lead to an accident; in some cases, physical preconditions need to be fulfilled. For instance, a train might be stopped at a station for passenger exchange, but the holding brake might not be applied. The train can start to roll down, potentially injuring the passengers, but only if the track is not flat. Physical barriers model such physical preconditions.

If external barriers, fully independent on ATO, are applicable to a hazard or to an accident, then the initial THR can be assigned a higher numerical value (e.g. 1.0E-06 per hour instead of 1.0E-08 per hour). A final THR is thus calculated, considering the risk reduction provided by the external barriers.

The list of the identified external safety barriers can be found in ANNEX C. The technical and human and organisational safety barriers are intended as safety requirements for the systems outside the ATO, i.e. as SRACs. ANNEX F contains more information on the calculation of the final THR based on the risk reduction provided by the external safety barriers.

Final THR and SIL

A SIL can be associated to the function according to its final THR:

Assumption: THR = TFFR (see NOTE above)

Table 7 - SIL and TFFR according to EN50129 [6]

Final TFFR [Failures / h]	SIL
$1\text{E-}9 \leq \text{TFFR} < 1\text{E-}8$	4
$1\text{E-}8 \leq \text{TFFR} < 1\text{E-}7$	3
$1\text{E-}7 \leq \text{TFFR} < 1\text{E-}6$	2
$1\text{E-}6 \leq \text{TFFR} < 1\text{E-}5$	1
$\text{TFFR} \geq 1\text{E-}5$	Basic Integrity

4.6. REVIEW OF THE SAFETY ANALYSIS

The safety analysis has been cross reviewed by a designated peer within WP 8.1. Additionally, the safety analysis results have been discussed within the WP 8.1 group during designated meetings and workshops.

Two review rounds have taken place, for both detailed peer review and of the overall discussion in the group. The first review round was focused on the hazard identification and classification, while the second round was focused on the identification of the external safety barriers and applicable codes of practice as well as, when applicable, on the explicit risk estimation.

5. TECHNICAL CONCLUSIONS

The Automating Functions are going to be implemented within the overall railway environment. On one side, Automating Function failures can lead to safety hazards. Hazards have been thus identified from the systematic analysis of Use Cases and Requirements for the Automating Functions.

On the other side, the railway environment already includes built-in risk control measures (i.e. safety barriers). These safety barriers, although not specifically developed to handle the Automating Function failures, can however in some cases completely control, or at least mitigate, the hazards caused by the Automating Function failures.

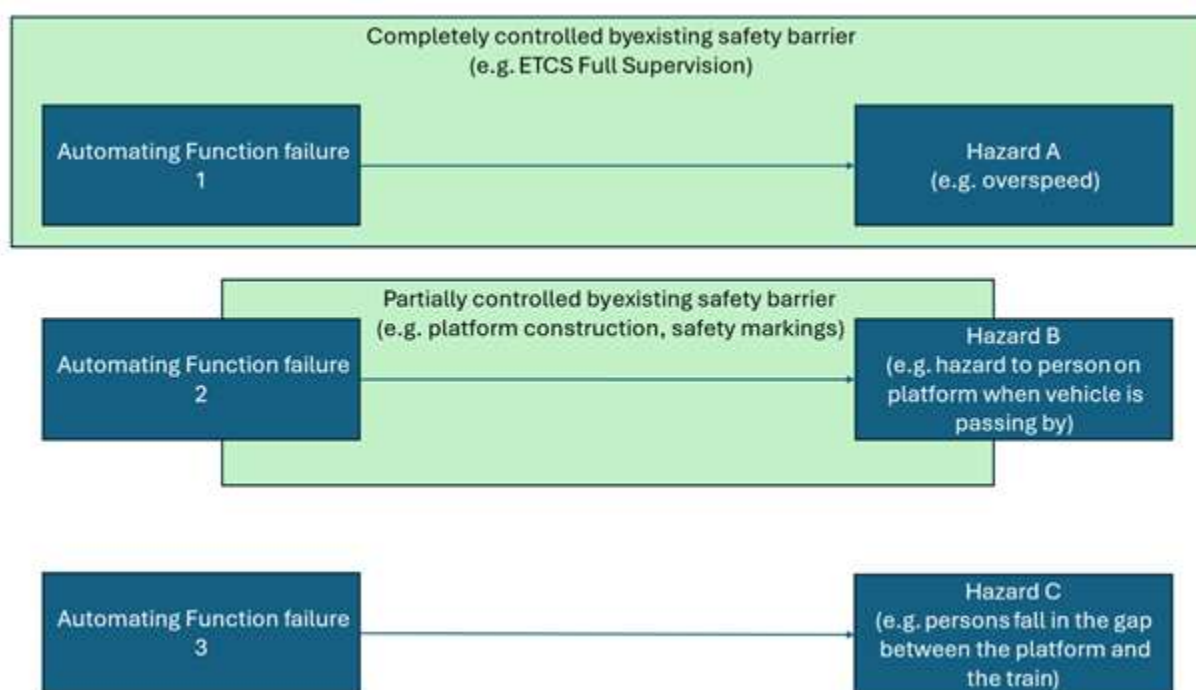


Figure 10 - Possibilities of mitigation of the hazards

The existing safety barriers, built-in in the railway environment, need to be considered to avoid overestimating the safety impact of the Automating Functions and thus overengineering them. At the same time, the railway environment is a complex, heterogeneous system, with regional and national differences across Europe. Additionally, different types of service (e.g. S-Bahn, regional lines, freight trains, long distance trains, high speed trains, ...) and operational modes (from ETCS L2 to unfitted for shunting movement), lead to very different applicable safety barriers.

Assumptions have therefore been formulated to clarify the limits, boundaries and specific scenarios for the WP 8.1 safety analysis. The main assumptions are:

- 1) The Automating Functions are applied in the context of the operational mode ETCS Full Supervision.
- 2) The operation with hazardous goods is excluded from the analysis.

Other specific assumptions are listed in chapter 4.2. If the assumptions are not met, the hazards identified by WP 8.1 are still applicable, but their quantitative targets (THR) need to be re-evaluated.

5.1. AUTOMATING FUNCTIONS

WP 8.1 is not tasked with designing the specific Automating Functions to control the open hazards, as:

- 1) open hazards might also be partially or completely controlled by other means, different from Automating Functions (e.g. new operational rules).
- 2) designing optimal solutions for Automating Functions requires a cooperation from designers and architects (to ensure the efficiency and applicability of the solutions) and safety experts (to ensure their overall safety)

The results of this safety analysis are therefore an input to the overall design and architecture for joint Automating Functions. Nevertheless, wherever applicable, suggestions of technical solutions have been included, as a starting point for the joint discussion between designers, architects and safety experts.

5.2. OUT OF SCOPE HAZARDS

The following hazard has been considered as out of scope for the safety analysis. It shall be considered in the security analysis.

Table 8 - Out of scope hazards

Hazard	Explanation
H8.1-07 Explosion Hazard	Bombs and terrorism (see UC5.1-047) are intentional sabotage, they are outside of the safety analysis, as the safety analysis deals only with unintentional dangerous failures. Bombs and terrorists are nevertheless relevant topics, which should be included in the security analysis.

Additional out-of-scope hazards can be found in Table 2 in Chapter 4.2.

5.3. HAZARDS PARTIALLY ANALYSED

The following hazards have been partially analysed due to missing inputs. They shall be refined once additional inputs are available.

Table 9 - Hazards partially analysed

Hazard	Explanation
H8.1-16-1 Hazard due to self-check of the vehicle not performed or results not communicated or not processed	The consequences depend on the kind of self-check and on the kind of self-check results, which were not specified in detail in the input documents. It is assumed that a dedicated concept shall be defined, as a basis to integrate the safety analysis.
H8.1-16-2 hazard due to failed safe reaction (e.g. in case of no self-check)	A generic requirement has been formulated: "Indications of the lamp indicating maintenance needs "Störleuchtmelder/ Leuchtmelder Instandhaltungsbedarf" shall be safely communicated to the operator/ TCC." The required safety integrity level depends on the kind of self-check and on the kind of self-check results.

5.4. HAZARDS COMPLETELY CONTROLLED BY CODE OF PRACTICE

The following hazards have been found to be completely controlled by Codes of Practice (CoP). The applicability of the defined Codes of Practice shall be discussed with the designers and architect.

If the Codes of Practice are deemed applicable and unless otherwise specified in the Table 10 below, the Automating Functions leading to these hazards can be implemented as Basic Integrity functions.

Table 10 - Hazards completely controlled by Code of Practice

Hazard	CoP + explanation / <i>clarifications</i>
H8.1-01-1 a Vehicle untimely sets itself in motion by applying traction from standstill Scenario a: collision train-train, derailment	ETCS FS- Subset 026 §3.13 Speed and distance monitoring <i>The CoP does not prevent a vehicle from unintentionally moving, but triggers an emergency brake in case of overspeed, preventing derailment and SPAD (signal passed at danger).</i>
H8.1-01-2 Vehicle travels in the wrong direction	ETCS- Subset 026 <i>The CoP does not prevent a vehicle from unintentionally moving in the wrong direction but triggers an emergency brake after a few meters (values depending on national parameters).</i>

Hazard	CoP + explanation / <i>clarifications</i>
H8.1-01-3 Excessive speed	ETCS FS- Subset 026 §3.13 Speed and distance monitoring <i>The CoP triggers an emergency brake in case of overspeed, preventing derailment and SPAD (signal passed at danger).</i>
H8.1-02 Vehicle sets wrong traction system	TSI Energy §4.2.16 If a system separation section is traversed with pantographs lowered, it shall be designed to avoid the electrical connection of the two power supply systems by an unintentionally raised pantograph. § 4.3.4 part 2: The relevant information to perform the switching of the circuit breaker, change of maximum train current, change of the power supply system and pantograph management shall be transmitted via ERTMS when the line is equipped with ERTMS. Applicable sections of the related standards: EN 50388-1:2022, EN50122, EN50119, EN50121 <i>The CoP shall be implemented with the necessary safety integrity level, based on the infrastructure, on the rolling stocks (e.g. dual modes vehicles) and on the train compositions (e.g. trains with multiple pantographs).</i>
H8.1-05-1-b Persons trapped in the external door frame	TSI LOC&PAS §4.2.5.5.3 Door obstacle detection §4.2.5.5.7 Door - traction interlock <i>The door obstacle detection prevents a door from closing if an obstacle is detected within the frame; the door traction interlock inhibits traction if a door is open. Together they prevent physical harm to persons caught in the door frame, e.g. from being crushed between the external door and the door frame or from being dragged by a moving train.</i> <i>The CoP shall be implemented with the necessary safety integrity level, taking into consideration that the hazard could lead to 'single fatality and/or severe injury'.</i> <i>NOTE: if an Automating Function replaces or integrates or affects the manual override of the traction interlock (see TSI LOC&PAS §4.2.5.5.7 (2)), then such Automating Function shall be designed with the necessary safety integrity.</i>
H8.1-05-2-a Unexpected train movement while people are boarding or leaving the train – train rolling backward	ETCS Subset026 §3.14.3 3.14.3 Reverse Movement Protection 3.14.3.1 The Reverse Movement Protection (RMP) shall prevent the train from moving in the opposite direction to the permitted one. The permitted movement direction of a train shall be the one of the

Hazard	CoP + explanation / <i>clarifications</i>
	<p>currently valid MA, if available on-board. See chapter 4 concerning permitted direction for special cases.</p> <p>3.14.3.2 When a reverse movement is detected, the brake command shall be triggered after a distance specified by the national value</p> <p><i>The ETCS automatically stops a train rolling backward by triggering the brakes.</i></p>
H8.1-05-2-e Doors release command while the train is moving	TSI LOC & PAS §4.2.5.5.6 and §4.2.5.5.8 <i>The TSI LOC & PAS §4.2.5.5.8 specifically deals with hazard of doors unlocked or released or opened when the train is running.</i>
H8.1-09 Hazard due to two trains approaching each other with excessive speed	ETCS FS - Subset 026 - §3.13 Speed and distance monitoring <i>The CoP triggers an emergency brake in case of overspeed, preventing derailment and SPAD (signal passed at danger).</i>
H8.1-10-3-a Hazard to passengers due to unexpected, excessive train movements during travel Scenario: jerk	TSI LOC&PAS § 4.2.4.2.1. Functional requirements (15) For speeds higher than 5 km/h, the maximum jerk due to the use of brakes shall be lower than 4 m/s ³ . EN14363 dynamic behaviour of trains <i>If the technical characteristic of the rolling stock allows a jerk due to traction higher than 4 m/s³, then also the jerk due to traction shall be lower than 4 m/s³.</i> <i>The CoP shall be implemented with the necessary safety integrity level, taking into consideration that the hazard could lead to 'No possibility of fatality, severe or minor injuries only.</i>
H8.1-13-1-a Hazard due to wrong JP	ETCS FS - Subset 026 §3.13 Speed and distance monitoring ETCS / ATP protection ATP protects against overspeed (ATP (in FS) will trigger EB in case of overspeed) § 3.14.2 ATP: Roll Away Protection (RAP) §3.14.3 Unauthorised Direction Movement Protection
H8.1-13-1-b Hazard due to wrong MP	ETCS FS - Subset 026 §3.13 Speed and distance monitoring ETCS / ATP protection ATP protects against overspeed (ATP (in FS) will trigger EB in case of overspeed) § 3.14.2 ATP: Roll Away Protection (RAP)

Hazard	CoP + explanation / <i>clarifications</i>
	§3.14.3 Unauthorised Direction Movement Protection
H8.1-13-3 Hazard due to wrong train ETCS mode	ETCS subset 026 - Part 4 - Clause 4.5.2 Strict validation of mode transitions Subset 125: ATO over ERTMS: System Requirement Specification: The ATO System shall be ready for ATO operation (ATO Operational) when the following conditions are satisfied: The current ETCS Mode is FS Mode and “ENTRY IN FULL SUPERVISION” procedure has finished (See [Ref 5] §4.4.9.1.4). When the ETCS-OB is not in FS Mode, the ATO-OB traction command shall be safely cut-out. <i>The CoP (the above quoted requirements from Subset 125) shall be implemented with the necessary safety integrity level, taking into consideration that the hazard could lead to ‘multiple fatalities and/or severe injuries.</i>
H8.1-13-4 Hazard due to lost train location	trackside supervision function: axle counters, balises; Subset-026 part 2 - §2.6.5.1.4 / 2.6.6.1.4 Train detection and train integrity supervision are performed by the trackside equipment of the underlying signalling system (interlocking, track circuits etc.) and are outside the scope of ERTMS/ETCS. Safety barrier outside of ATO. ETCS Subset 026/03 - Cold Movement Detection: 3.15.8.1 After being switched off (i.e. once in No Power mode), the ERTMS/ETCS on-board equipment shall be capable, if fitted with, to detect and record whether the engine has been moved or not, during a period of at least 72 hours. 3.15.8.1.1 To allow small movements e.g. for coupling in No Power mode, the ERTMS/ETCS on-board equipment shall consider that no cold movement has occurred as long as the train does not move for more than 2m away from the train position stored when No Power mode was entered <i>NOTE: if an Automating Function replaces or integrates or affects the cold movement detection (e.g. through an automatic reaction after a cold movement is detected), then such Automating Function shall be designed with the required safety integrity level (i.e., unless further consideration applies, the same safety integrity level as the cold movement detection function).</i>
H8.1-14 loss of train integrity	TSI CCS:

Hazard	CoP + explanation / <i>clarifications</i>
	<p>7.6. Train detection systems specific implementation rules.</p> <p><i>Note: in case no train detection system is installed (e.g. no track circuits or no axle counters; that could be the case for Moving Blocks), a Train Integrity Monitoring System shall be applied; the loss of integrity shall be monitored and reported with the required safety integrity level.</i></p>

5.5. HAZARDS PARTIALLY CONTROLLED BY CODE OF PRACTICE

The following hazards listed in Table 11 are only partially controlled by Code of Practice (CoP). The CoP might not be sufficient to completely control the hazard from a quantitative point of view (THR) and / or specific GoA3/4 scenarios might exist, for which the CoP cannot control the hazard and needs e.g. to be updated or integrated with other risk control measures.

The best solution to handle these hazards needs to be discussed and agreed between designers, architects and safety experts. The open hazards scenarios might be addressed by means outside of the Automating Functions (e.g. operational risk control measures), by safety related Automating Functions or by a mix of them. The overall safety solutions need to be implemented with the necessary safety integrity level, based on the identified THR.

Wherever applicable, suggestions of technical solutions have been included, as a starting point for the joint discussion between designers, architects and safety experts.

Table 11 - Hazards partially controlled by Code of Practice

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
H8.1-03-1 Parking brake force reduced or not given	<p>EN 16185-1, 5.11.4 Parking brake</p> <p>The purpose of a braking brake is to keep the train stationary in shut down configuration for an indefinite period of time without energy supply.</p> <p>The parking brake shall be capable of securing an EMU/DMU in the load condition design mass in working order in accordance with EN 15663 in a stabling point (depot) on a gradient of 0,5 % if not otherwise specified.</p> <p>TSI LOC&PAS §4.2.4.1 (2) Functional requirements</p> <p>Units shall be equipped with a parking brake function used when the train is parked, allowing the application of a brake force without any available energy on board for an unlimited period.</p>	1.00E-09

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p>TSI LOC&PAS §4.2.4.4.5 Parking braking command</p> <p>For units assessed in fixed or predefined formations, and for locomotives assessed for general operation, the parking brake command shall be activated automatically when the unit is switched off. For other units, the parking brake command shall be either activated manually, or activated automatically when the unit is switched off.</p> <p><i>EN16185-1 defines the characteristic of the parking brakes; the TSI LOC&PAS defines the automatic application of the parking brake for selected trains. Together they are sufficient to completely control the hazard.</i></p> <p><i>However, the TSI LOC&PAS has a specific limited applicability, as the automatic application of the parking brakes is ensured only for units assessed in fixed or predefined formations, and for locomotives assessed for general operation. Additionally, the LOC&PAS requirements do not include the check of the application of the parking brakes (some brakes might be out of service due to mechanical failures), which is a driver responsibility in GoA1. Lastly, the parking brake effort is not sufficient for units parked on steep gradients and additional measures (e.g. brake shoes / scotches) are needed. To handle these limitations, the following additional requirement has been formulated:</i></p> <p><u>It shall be ensured that the train is adequately immobilized for an extended period or higher gradient (e.g. brake shoes). The correct application of the parking brake and train immobilization is to be checked before shutting off the train.</u></p> <p>Note: the scenario to avoid is a shut-down train rolling down due to no application of the parking brakes or insufficient parking brake effort. Such train might e.g. enter an already occupied track, potentially causing a train-train collision. A possible safe outcome is that an insufficient application of the parking brakes is detected and that the train is prevented from automatically shutting down. The failure is communicated to the entity in charge of identifying and</p>	

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	implementing a safe reaction (e.g. application of brake shoes)	
H8.1-03-3 Passenger alarm – emergency brake request fails	<p>LOC&PAS § 4.2.5.3.2 Passenger alarm- requirements for information interface</p> <p>(3) At the triggering of the passenger alarm, both visual and acoustic signs shall indicate to the driver that one or more passenger alarms have been activated.</p> <p>(4) A device in the cab shall allow the driver to acknowledge his awareness of the alarm. The driver's acknowledgement shall be perceivable at the place where the passenger alarm was triggered and shall stop the acoustic signal in the cab.</p> <p>LOC&PAS § 4.2.5.3.2 Passenger alarm- Requirements for activation of the brake by the passenger alarm</p> <p>(1) When the train is stopped at a platform or departing from a platform, activation of a passenger alarm shall lead to a direct application of the service brake or the emergency brake, resulting in a complete stop. In this case, only after the train has come to a complete stop, a system shall allow the driver to cancel any automatic braking action initiated by the passenger alarm.</p> <p>(2) In other situations, 10 +/-1 seconds after activation of the (first) passenger alarm, at least an automatic service brake shall be initiated unless the passenger alarm is acknowledged by the driver within this time. The system shall allow the driver to override at any time an automatic braking action initiated by the passenger alarm.</p> <p>LOC&PAS §4.2.5.3.5: Passenger alarm: Safety requirements</p> <p>For the scenario 'failure in the passenger alarm system leading to the impossibility for a passenger to initiate the activation of brake in order to stop the train when train departs from a platform', it shall be demonstrated that the risk is controlled to an acceptable level considering that the functional failure has typical credible potential to lead directly to "single fatality and/or severe injury".</p>	1.00E-09

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p><i>The TSI LOC&PAS identifies an interface between passengers and driver and, in case of passenger alarm outside the platform, requires a driver reaction within 10 +/- 1 seconds. The TSI LOC&PAS requirements need to be integrated for operation in GoA3/4, as no driver is available in GoA3/4. WP 8.1 points out that an unwanted automatic application of the emergency braking in some specific emergency situations (e.g. fire onboard) is dangerous, as it might prevent the train from reaching a safe area for passengers' evacuation. It is outside of WP 8.1 scope to define the specific safety concept for the passenger alarm in GoA3/4. A concept might consider the following aspects:</i></p> <p><i>1) the passenger alarm and the train position are safely transmitted to an entity in charge to manage it (e.g. Emergency Manager)</i></p> <p><i>2) a bidirectional communication is safely established between the passengers on the train and the entity in charge of managing the passenger alarm</i></p> <p><i>3) In other situations, xx +/-1 seconds after activation of the (first) passenger alarm, at least an automatic service brake shall be initiated unless the passenger alarm is acknowledged by the designed entity within this time. The system shall allow the designed entity to override at any time an automatic braking action initiated by the passenger alarm.</i></p> <p><i>4) It shall be possible to inhibit the automatic service brake if the passenger alarm is activated on specific track sections (e.g. long tunnels).</i></p>	
H8.1-05-1-a Doors are released on the wrong side or outside of a safe area for the passenger exchange	TSI LOC&PAS 4.2.5.5.6 and 4.2.5.5.8 door opening <i>The TSI LOC&PAS defines the scenarios in which one or multiple external doors are unlocked or released or opened in inappropriate areas (e.g. wrong side of train). The existing technical solutions developed according to the TSI LOC&PAS for GoA1 rely on a door unlock (or release or open) command by the train driver, who is trained to provide a safe command. For GoA3/4 doors are released by an Automating Function, e.g. by the ADM; the scenario concerning door unlock or release or open in inappropriate areas needs to consider also the door unlock (or release or open) request by an Automating Function. Either sufficient additional external safety barriers, independent on the Automating Functions, are built, or the Automating Function</i>	1.00E-08

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p><i>concerning the door unlock (or release or open) request needs to be implemented with the necessary safety integrity.</i></p> <p>Subset 125, clause 6.4.2.5 - The JP shall identify, for each Stopping Point, if the ATO-OB must manage train doors opening (including the sides for opening the doors) and train doors closing</p> <p>ERTMS/ETCS; Subset 34, version 3.2.0; Train Interface FIS; section 2.4.6 "Station platform"</p> <p>ERTMS/ETCS; Subset 026-5, version 3.6.0; System Requirements Specification - Chapter 5 Procedures; section 5.20.8 "Station platform"</p> <p><i>The SS 34 and SS 026-5 only require that the platform info is delivered to the OBU. The fact that the platform information is available for the OBU does not prevent a door from opening outside a platform or on the wrong side, e.g. because of a failure of the Automating Function door unlock (or release or open) request. The platform info needs to be safely, autonomously and independently from the Automating Functions processed by the vehicle (e.g. DCUs, door control units) to prevent a door from opening on the wrong side or outside of the platform.</i></p> <p><i>Same remark for SS 125.</i></p> <p><u>Under the assumption that the door unlock (or release or open) request by an Automating Function (e.g. from ADM) is only available as a Basic Integrity function, a potential safety architecture could be the following:</u></p> <ol style="list-style-type: none"> <u>1) safety relevant function: the vehicle (e.g. door control unit + OBU) receives the platform information, completely independently on ADM</u> <u>2) safety relevant function: the vehicle (e.g. OBU) knows the train position (e.g. odometry)</u> <u>3) the ATO sends a door unlock (or release or open) request with Basic Integrity</u> 	

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p>4) <u>safety relevant function: the vehicle (e.g. door control unit) checks the request and only opens the doors if the preconditions are met</u></p> <p>a <u>the doors are unlocked (or released or opened) on the side with the platform, based on the platform information</u></p> <p>b <u>the position of the door is within the platform (i.e. the train has stooped completely within the platform), based on the train position and the platform information.</u></p> <p><u>The safety relevant functions need to be implemented with the necessary safety integrity level, considering that the THR might be further reduced if:</u></p> <ul style="list-style-type: none"> • <u>passengers usually do not stand in the door area (e.g. long-distance trains)</u> • <u>external doors are only centrally released but not opened; the passengers still need to request opening e.g. through a push button</u> 	
H8.1-05-1-d Persons fall in the gap between the platform and the train	<p>TSI OPE - Appendix D - Route compatibility and Route Book – Gauging</p> <p><i>The TSI OPE defines the gauging and the distance between trains and platforms. However, the gap between platforms and trains can still be enough for a person to fall in it.</i></p> <p><u>Each infrastructure manager shall evaluate the risk for this hazard and, if necessary, define safety measures. Elements to be considered in the risk estimate include:</u></p> <ul style="list-style-type: none"> • <u>the existence and width of the gap between the platform and the trains operated on that platform</u> • <u>the platform characteristic</u> • <u>the expected number of persons getting on and off</u> • <u>the potential for overcrowding</u> • <u>the train characteristics.</u> <p><u>If the risk is not acceptable, new safety barriers or safety functions need to be introduced, e.g. the supervision of the passenger exchange.</u></p>	3.3E-07

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
<p>H8.1-05-2-c</p> <p>Unexpected train movement while people are boarding or leaving the train - traction applied by the train</p>	<p>Door - traction interlock according to TSI LOC & PAS, section 4.2.5.5.7</p> <p>(1) Traction power shall be applied only when all doors are closed and locked. This shall be ensured through an automatic door-traction interlock system. The door-traction interlock system shall prevent traction power being applied when not all of the doors are closed and locked.</p> <p>(2) The traction interlock system shall be provided with a manual override, intended to be activated by the driver in exceptional situations, to apply traction even when not all of the doors are closed and locked.</p> <p>EN14752:2019+A1:2021 Railway applications - Bodyside entrance systems for rolling stock</p> <p><i>The CoP are not sufficient in GoA3/4. The CoP assumes an implicit safety barrier, i.e. that the train driver does not spuriously require traction when doors are still open, or at least the train driver does that mistake very rarely (human error of a trained professional).</i></p> <p><i>An Automating Function, on the contrary, might fail ""often"" and ""systematically"", unless specific quantitative safety requirements (TFFR) on the traction request are set.</i></p> <p><i>Additionally, the train driver acts as a constant monitoring: if the hazard arises, the driver is expected to detect it and react appropriately, e.g. by applying the service brakes. The driver then continues the journey only if is safe to do so.</i></p> <p><i>As a last point, if the manual override is commanded by an Automating Function, then it shall be ensured that the manual override is not spuriously activated by the Automating Function.</i></p> <p><u>A safety function shall be implemented, that covers the following task with a suitable TFFR:</u></p> <p><u>- ATO (e.g. ADM) can request traction only when the doors are closed</u></p> <p><u>Additionally, the manual override of the door-traction interlock needs to either:</u></p> <p><u>be completely separated from ATO (i.e. ATO cannot override the door traction interlock)</u></p>	<p>1.00E-07</p>

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<u>OR</u> <u>be implemented with a suitable TFFR</u>	
H8.1-05-2-d Unexpected train movement while people are boarding or leaving the train - unexpected jogging	<p>LOC&PAS TSI 4.2.5.5.7 Door-traction interlock</p> <p><i>The CoP is not sufficient to handle the hazard. The scenario to be avoided is as follows: the train stops partly within the platform, but it overshoots or undershoots its target stopping point. People on the platform get close to the external doors, expecting them to be opened. Unaware to the persons close to the external doors, the train starts to jog. People might fall and be run over by the train.</i></p> <p><u>A safety function shall ensure that passengers are informed (e.g. through an acoustic and visual warning) before the trains starts to jog.</u></p>	3.30E-05
H8.1-06-1 Ignition and Fire (e.g. fire onboard)	<p>TSI LOC&PAS</p> <p>§4.1.4 "Categorisation of rolling stock for fire safety"</p> <p>§4.2.10 "Fire safety and evacuation" 4.2.10.1 "General and Categorisation"</p> <p>§4.2.10.2 "Measures to prevent fire"</p> <p>TSI LOC&PAS §4.2.10.2.1 Material requirements</p> <p>§4.2.10.3 "Measures to detect/control fire"</p> <p>§4.2.10.4 "Requirements related to emergencies" (including §4.2.10.4.2 Smoke Control)</p> <p>§4.2.10.5 "Requirements related to evacuation"</p> <p>Appendix J-1, index [30]:</p> <p>EN 45545-2:2020 Railway applications - Fire protection on railway vehicles - Part 2: Requirements for fire behaviour of materials and components</p> <p>NOTES: '- For hot axle boxes / hot wheel see references in H8.1-06-2</p> <p>- For hazard to passengers while in closed vehicle due to door management see references in H8.1-05-3 and TSI LOC&PAS 4.2.5.5.9 "Door emergency opening"</p> <p><i>The CoPs define the preconditions to prevent and contain fires. to slow down their propagation and to limit toxic gases and smoke. However, such measures alone are not sufficient</i></p>	1.00E-07

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p><i>to handle the hazard, as in some cases additional reactions by the train driver and train staff are needed (e.g. in case an evacuation at a safe area is needed).</i></p> <p><i>Additionally, according to TSI LOC&PAS §4.2.10.4.2 Smoke Control, point (4), it is permissible to manually switch off or close all means of external ventilation and to switch off the ventilation and recirculation at vehicle level.</i></p> <p><u>A safety concept to handle emergencies, including topics such as the reaction to fire or smoke detection and the train evacuation, shall be defined.</u></p> <p><u>After fire or smoke detection a safety reaction shall be implemented.</u></p>	
H8.1-06-2 Hot wheel	<p>ON-BOARD: TSI LOC&PAS 4.2.3.3.2 (Axle bearing condition monitoring)</p> <p>TRACKSIDE: EN 15437-1:2009 (Axle box condition monitoring)</p> <p><i>Not sufficient, the Code of Practice is thought to be applied together with human supervision to act.</i></p> <p><i>- On-board detection: Train driver to stop in the next suitable location. Then, operational procedure to check status and decide next actions.</i></p> <p><i>- Trackside detection: Traffic control personnel to call the driver and manage traffic to stop the train. Then, operational procedure to check status and decide next actions.</i></p> <p><u>Operational rule for reaction after hot wheel detection shall be implemented</u></p>	1.00E-09
H8.1-12-3 Insufficient availability of vehicle functions required in an emergency	<p>TSI SRT 4.2.3.3.4 & TSI LOC&PAS 4.2.10.4.4.</p> <p>(2) The unit shall be designed so that, in the event of fire on-board, the running capability of the train will enable it to run to a suitable firefighting point.</p> <p>(3) Compliance shall be demonstrated by application of the specification referenced in Appendix J-1, index 63, in which the system functions impacted by a 'type 2' fire shall be:</p> <p>— braking for rolling stock of fire safety category A: this function shall be assessed for a duration of 4 minutes.</p>	1.00E-07

Hazard	Code of Practice + <i>explanation</i> + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p>— braking and traction for rolling stock of fire safety category B: these functions shall be assessed for a duration of 15 minutes at a minimum speed of 80 km/h.</p> <p><i>The TSI requirements in this cell are necessary but not sufficient. The traction and braking command are expected to be handled by an automated system (e.g. ADM) in GoA3/4. In case of emergency, such automated system shall handle traction and braking and needs to do so based on the kind of emergency, rolling stock and track characteristic, following reaction rules and remote instructions from the emergency management centre; for instance, in case of fire on a long tunnel, the train might be required to run to the next safe evacuation area, prioritizing traction over energy optimization and passenger alarm. As a result, additional Automating Functions are necessary, see below.</i></p> <p><u>A) The TSI text at point (2) shall be amended and clarified for GoA3 and GoA4 operation. In case of GoA3 or 4 operations, instead of "the unit shall be designed" a possible and suggested amendment is "The unit, including ATO, and the communication between the unit and the emergency management centre shall be designed ..."</u></p> <p><u>B) The TSI text at point (3) shall be amended. A possible and suggested amendment is: add at the end of point (3) "While assessing compliance of the braking and traction, the communication between the unit and the emergency management centre and the ATO command of the braking and traction shall be considered"</u></p> <p><u>NOTE: the communication is only partially in scope of TSI LOC & PAS, as it does not only involve the rolling stock, but also the infrastructure. An analogous clause in the TSI Infra should be added.</u></p>	
H8.1-12-4 Passenger get nervous/ panic (in an emergency)	TSI LOC&PAS 4.2.5.8 Internal air quality 4.2.7.1.4 lamp control 4.2.10.4.1 Emergency lighting 4.2.10.5.1. Passenger emergency exits	1.00E-07

Hazard	Code of Practice + explanation + <u>additional requirement / SRAC</u>	Final THR [1 / h]
	<p><i>The TSI LOC&PAS assumes that the handling of the emergency is facilitated by the presence of train staff (train driver or train attendant). No train driver or train attendant is present in GoA4. Passengers without instructions in case of emergency may panic, leading to injuries and potentially dangerous occurrence (such as trying to break windows to escape, being unable to open the emergency doors when needed, or trying to open the emergency doors when not needed, e.g. before the train reaches the intended area for evacuation).</i></p> <p><u>Additional functions shall be implemented for communication from train to operational / traffic manager and from operational /traffic managers to the passengers</u></p> <p><u>A dedicated safety concept for emergency handling shall be developed. This concept shall also address the possibility to bypass some safety functions in an emergency (e.g. avoid an unwanted train stop and ensure traction).</u></p>	
H8.1-13-5 Hazard due to wrong train data or adhesion factor	<u>A dedicated safety concept for entering and handling train data, including the adhesion factor, shall be developed.</u>	1.00E-09

5.6. HAZARDS NOT CONTROLLED BY CODE OF PRACTICE

For the following hazards listed in Table 12 no specific Codes of Practice (CoP) have been identified, but the described external safety barriers have been considered. The applicability of the external safety barriers needs to be verified between the designers, architects and safety experts.

The best solution to handle these hazards needs to be discussed and agreed between designers, architects and safety experts. The open hazards scenarios might be addressed by means outside of the Automating Functions (e.g. operational risk control measures), by safety related Automating Functions or by a mix of them. The overall safety solutions need to be implemented with the necessary safety integrity level, based on the identified THR.

Wherever applicable, suggestions of technical solutions have been included, as a starting point for the joint discussion between designers, architects and safety experts.

Table 12 - Hazards not controlled by Code of Practice

Hazard	Safety barrier + <u>Safety requirements / SRAC</u>	Final THR [1 / h]
H8.1-11-1 Hazard to persons outside the train due to failure to recognize the vehicle	Person can recognise vehicle because of the Marker light / Head light / front light activation. Maintenance workers are trained to follow the rules for going in a track in operation.	1.00E-07
H8.1-11-3 Hazard to person outside the vehicle due to unfavourable aerodynamic behaviour when vehicle is passing by	Announcement system at station/platform to warn passengers at platform about passing train according to national rules is established. Person can recognise vehicle because of the Marker light / Head light /front light activation. National rules about the allowance of train passing platforms with a certain speed and safety markings on the platform apply.	3.30E-06
H8.1-12-1 Evacuation of passengers in an emergency not possible H8.1-12-2 Evacuation of passengers in an emergency is complicated H8.1-12-5 Hazards due to Insufficient ventilation/air conditioning in case of emergency	Note: for fire emergencies, see also H8.1-06-1. The detection of an emergency and the communication with the emergency management centre can independently occur outside ATO, e.g. through passengers calling the emergency number with their mobile phones, or through RU staff monitoring the stations through CCTV. RU have operational rules about evacuation <u>Additional functions shall be implemented for communication from train to operational / traffic manager and from operational /traffic managers to the passengers</u> <u>A dedicated safety concept for emergency handling shall be developed. This concept shall also address the possibility to bypass some safety functions in an emergency (e.g. avoid an unwanted train stop and ensure traction).</u>	1.00E-07

For the following hazards listed in Table 13 neither specific CoP nor other external safety barriers have been identified. The best solution to handle these hazards needs to be discussed and agreed between designers, architects and safety experts. The open hazards scenarios might be addressed by means outside of the Automating Functions (e.g. operational risk control measures), by safety

related Automating Functions or by a mix of them. The overall safety solutions need to be implemented with the necessary safety integrity level, based on the identified THR.

Wherever applicable, suggestions of technical solutions have been included, as a starting point for the joint discussion between designers, architects and safety experts.

Table 13 - Hazards with no Code of Practice and no external safety barriers

Hazard	Explanation + <u>Safety Requirement / SRAC</u>	Final THR [1 / h]
H8.1-04 Insufficient track guidance, track guidance fails, derailment due to flat wheel	<p><i>Possible causes for a flat wheel include:</i></p> <p>1) parking brake applied while traction is applied</p> <p>2) excessive slip, if not mitigated from slip and slide protection</p> <p><i>A flat wheel can be detected by the train driver in GoA1; in GoA4, if not detected and negated by an Automating Function or another risk control measure, the mechanical damages to the wheel over time might evolve to a point where derailment cannot be excluded.</i></p>	1.00E-09
H8.1-05-2-b Unexpected train movement while people are boarding or leaving the train - rolling forward	<p><i>Rolling forward, e.g. due to gravity on tracks with a gradient, is possible even with open doors and no traction applied.</i></p> <p><u>The train shall be safely immobilized (e.g. by the holding brake application) during the passenger exchange</u></p>	1.00E-07
H8.1-05-3 Hazards to persons locked inside a train not in passenger service	<p><i>A person is on a train out of service and the train goes e.g. to the depot. The person might try to leave the train in an unsafe area (e.g. depot) or be left without heating or cooling for an undefined amount of time.</i></p> <p><i>Possible causes include persons unaware that the train reached its final destination (language barriers, asleep, intoxicated) or persons entering by mistake an out of service train at its last station.</i></p> <p><u>A safety function or process shall be implemented to ensure that all passengers left the train before taking the train out of service and locking the external doors.</u></p>	3.00E-07
H8.1-10-1 hazard due to no cooling/ no heating in normal operation	<p><u>An announcement for the passengers about malfunction of HVAC and additional information, like the affected train unit shall be made.</u></p> <p><u>Malfunction of the HVAC shall be communicated to operator/ IM.</u></p>	1.00E-07

Hazard	<i>Explanation + <u>Safety Requirement / SRAC</u></i>	Final THR [1 / h]
H8.1-10-3-b Hazard to passengers due to unexpected, excessive train movements during travel - scenario: lateral movement	<u>IM shall be responsible for the quality of the track (supervision and maintenance to avoid twisted tracks).</u>	1.00E-06
H8.1-13-1-c Hazard due to wrong GoA level	<u>A safety concept to safely switch between GoA levels shall be developed</u>	1.00E-09

5.7. HAZARDS LINKED TO OTHER HAZARDS

The following hazards listed in Table 14 have been linked to other hazards:

Table 14 - Hazards linked to other hazards

Hazard	Linked to
H8.1-06-2 "hot wheel"	H8.1-12 "Emergency Situation" H8.1-03-2 "ATO requests traction while brakes are applied"
H8.1-07 "Explosion Hazard"	H8.1-04 „Insufficient track guidance, track guidance fails due to flat wheel“ H8.1-06-1 "Ignition and Fire"
H8.1-09 "Hazard due to two trains approaching each other with excessive speed"	H8.1-13-4 "hazard due to lost train location"
H8.1-10-1 "hazard due to no cooling/ no heating in normal operation"	H8.1-12-2 "Evacuation of passengers in an emergency is complicated" H8.1-05-2 "Hazard to persons while boarding or door opening while vehicle is in motion"

Hazard	Linked to
H8.1-10-3-a "Hazard to passengers due to unexpected, excessive train movements during travel - scenario: jerk"	H8.1-01-1 "Vehicle untimely sets itself in motion by applying traction from standstill"
H8.1-11-2 "Hazard to persons outside the train due to unexpected train movement "	H8.1-01-1-a "Vehicle untimely sets itself in motion by applying traction from standstill"
H8.1-12-2 "Evacuation of passengers in an emergency is complicated"	H8.1-12-1 "Evacuation of passengers in an emergency not possible"
H8.1-12-5 "Hazards due to Insufficient ventilation/air conditioning in case of emergency"	H8.1-06-1 "Ignition and Fire"

6. CONCLUSIONS

The safety analysis within the scope of WP 8.1 has been successfully concluded. The WP 8.1 safety results have been achieved: hazards have been identified, applicable codes of practice (standards) have been listed, and safety risks have been evaluated and classified.

The achieved WP 8.1 safety results form the foundation for the safe design and specifications of the automating functions. They also serve as the basis for the crucial safe integration between the new automating functions and the existing railway systems.

The safety analyses performed and documented in this deliverable provide foundational input for the development and enhancement of Automating Functions. The list of hazards, their risk classification, and the standards and external safety barriers serve as checklists to verify whether the current design (e.g., SRS) is sufficiently safe. They are a tool to determine whether safety-relevant design modifications are needed, and which improved or new safety functions are required. The integration of safety results into the design is both necessary and urgent. It is necessary because an unsafe design would not be approved for commercial use (as demonstrated by autonomous cars). It is urgent because as the design becomes more advanced and detailed, the more impactful and potentially disruptive safety improvements become, leading to development delays and additional financial costs.

The initiatives described below also offer an opportunity to move beyond current non-harmonized national operational procedures handled by human operators.

The following proposed subsequent activities present opportunities to leverage the WP 8.1 safety results. A joint working group comprising designers and safety experts can be created to collaboratively integrate the WP 8.1 safety results into the automating functions design and specifications. Additional working groups could proactively address and integrate known open points.

For effectively managing emergency situations, the development of harmonized operational procedures is paramount. These procedures will be key to controlling risks, especially as the automated functions are designed not only to detect unwanted scenarios but also to react to them. Therefore, an additional working group made of railway operators and experts in emergency management and safety management can be created to develop harmonized procedures for handling emergencies. Moreover, this presents an opportunity for significant advancements in ATO architecture and design, as well as for interfacing systems, all of which play a critical role in orchestrating the overall system's response to emergencies.

Finally, continuous and proactive examination of safety aspects by all relevant stakeholders throughout the ongoing development lifecycle is essential.

These proposed activities require significant time investment and technical discussion. It is strongly recommended to plan the related activities and resources starting from 2026 in the context of the second wave.

6.1. PROPOSAL OF FUTURE WORK PACKAGES

Following the analyses conducted within WP 8.1, the following key areas have been identified for future exploration and enhancement:

Table 15 - Proposal for future Work Packages

Proposed Work Package	Aim	Participants	Deliverable
Integration of WP 8.1, WP 8.2, WP 8.3 and WP 8.4 safety results	<p>Integration of the safety results from WP 8.1, WP 8.2, WP 8.3 and WP 8.4</p> <p>Allocation of the Tolerable Hazard Rates (THRs) derived from WP 8.1 analyses into specific Tolerable Functional Failure Rates (TFFRs) of specific functions for the system development.</p> <p>Safety analysis of currently missing use cases regarding coupling and self-checks (see note below table)</p> <p>Exploration of country-specific use cases to broaden applicability</p>	Safety experts	Consolidated hazard log
Safe design and specification for the Automating Functions	<p>Update of the design and specifications based on the safety results (e.g. external safety barriers and SRACS)</p> <p>Impact analysis of new SRS releases to identify and integrate any safety-relevant changes, such as new or modified functions</p>	<p>Designers</p> <p>Architects</p> <p>Safety experts</p>	Updated System Requirements Specifications (SRS)
Safe emergency management for automatic operation	Definition and harmonization of operational and technical procedures and protocols to safely handle emergencies in automatic operation without	Railway undertakings (focus: operational expertise)	<p>Emergency procedures and protocols</p> <p>Specification of the IMS logical</p>

Proposed Work Package	Aim	Participants	Deliverable
	<p>train driver and train staff on board</p> <p>Definition of logical components like IMS (Incident Management System)</p> <p>Advancement of the Technology Readiness Level (TRL) of involved subsystems</p> <p>Integration between GoA3/4 and the IMS</p>	<p>Infrastructure managers (focus: emergency management)</p> <p>Rolling stock experts (focus: technical expertise and emergency management)</p> <p>Safety experts</p> <p>Designers and architects (focus: technical expertise and IMS specification)</p>	<p>components within the overall GoA3/4 architecture</p>

Note: The inputs analysed by WP 8.1, particularly the Use Cases, lacked sufficient detail to perform a comprehensive safety analysis for automated coupling/uncoupling and automated self-checks. It is recommended that a meeting be held between designers, architects, and safety experts to clarify the level of detail required for the Use Cases.

6.2. OPPORTUNITIES FOR FURTHER DEVELOPMENT

WP 8.1 identified the following topic as an opportunity for further development:

Table 16 - Opportunnities for further development

Topic	Objective
<p>SIL certification for AI-based functions</p> <p>Safety topics for AI</p>	<p>Take it into consideration once safety topics for Ai or ML evolve</p>

6.3. GAINED INSIGHTS

WP 8.1 has yielded insights that can help to optimize subsequent project phases:

- **Synergistic Collaboration:** The necessity of proactive and continuous exchange between designers, architects and safety experts is highlighted as crucial for optimizing safety evaluations and ensuring the seamless integration of subsystems involved. A collaborative approach could explore diverse design and architectural solutions to achieve required safety levels for automated functions, identifying the most technically feasible, economically viable, and safety-assured architecture.
- **Early Engagement for Integration:** Timely and ongoing collaboration with WP 8.1 before and during follow-up works is essential for understanding and integrating results effectively.

- Proactive Review Processes: Engaging with the review group prior to deliverable due dates is vital for ensuring quality and alignment.
- Optimized Communication Pathways: Establishing clear communication channels and guidance from the outset, particularly from the system pillar, is key to streamlining the integration of safety analyses and enhancing overall project efficiency.
- Functional Safety Analysis Approach: A shift towards a functional rather than subsystem-based approach for safety analyses is identified as a more efficient and effective strategy, enabling a holistic view of system functionalities. This ensures that analyses are holistically integrated within broader system functionalities like emergency handling.

7. REFERENCES

The subsequent chapter presents the reference documentation.

7.1. INPUT DOCUMENTS

The input document are the documents containing the system definition.

Table 17 - Input documents

Ref.	Document ID	Document title
[1]	FP2-T5_1-D-NSR-124-06	Deliverable D5.1 with Annexes 1-4 “WP5.1 – Documentation of use cases for automating functions”
[2]	FP2-T6_1-D-SMO-035-03	Deliverable D6.1 “D6.1 – Report on sets of non-functional and functional requirements (SRS) for automating functions”
[3]	FP2-T1_3-A-SNCF-005-01	GRANT AGREEMENT Project 101102001 — FP2 - R2DATO

7.2. SAFETY REGULATIONS AND SAFETY STANDARDS

The legal safety framework is the set of applicable laws and regulations used as a mandatory cornerstone for the safety analysis processes. They have been followed and implemented during the safety analysis.

Table 18 - Legal safety framework

Ref.	Document ID	Document title	Version
[4]	CSM-RA 402/2013	COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009	402/2013
[5]	CSM-RA 2015/1136	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment	2015/1136

The following standards have been used when necessary to integrate and better precise the legal safety framework, on specific, limited topics. It is not claimed that they are fully applicable nor that they have been systematically implemented.

Table 19 - Safety standards – processes

Ref.	Document ID	Document title	Version
[6]	EN 50126-1	Railway applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process	2017
[7]	EN 50126-2	Railway applications-The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety	2017
[8]	EN 50129	Railway applications-Communication, signalling and processing systems – Safety related electronic systems for signalling	2018
[9]	EN 45545	Railway applications – Fire protection on railway vehicles	2024
[10]	EN 50553	Railway applications - Requirements for running capability in case of fire on board of rolling stock	2012

7.3. TECHNICAL REGULATIONS AND STANDARDS

Technical standards, including the technical specifications for interoperability (TSI), have been consulted as a support for the hazard identification and the identification of safety requirements. Overall conformity³ with the technical standards, including the TSIs, is not a mandatory precondition for operating vehicles equipped with APM, ADM and REP functions.

On the contrary, only specific requirements from the technical standards are relevant for this safety analysis. These specific requirements have been identified and documented as external safety barriers (see ANNEX C). The identified requirements from ANNEX C shall be fulfilled.

³ “overall conformity” is meant as “it has been demonstrated that the whole standard / TSI has been sufficiently fulfilled” e.g. through a certificate by an assessor / a notified body- This overall conformity is NOT required.

Technical specification for interoperability

Table 20 - List of referenced TSI

Document ID	Document title	Version
TSI LOC&PAS Locomotives and Passengers TSI	Commission Regulation (EU) No 1302/2014 of 18 November 2014	2014
Control Command and Signalling TSI	Commission Implementing Regulation (EU) 2023/1695 of 10 August 2023	2023
Safety in Railway Tunnels TSI	Commission Regulation (EU) No 1303/2014 of 18 November 2014	2014
Operation and Traffic Management TSI	Commission Implementing Regulation (EU) 2023/1693	2023
Infrastructure TSI	Commission Regulation (EU) No 1299/2014 of 18 November 2014	2014

Other technical standards

Table 21 - List of other referenced standard

Document ID	Document title	Version
EN 14752:2019+A1:2021	Railway applications- Bodyside entrance systems for rolling stock	2021
ETCS Subset-026-3	ERTMS/ETCS - System Requirements Specification Chapter 3 Principles	V4.0
ETCS Subset- 125	ERTMS/ATO - System Requirement Specification	V1.00
IEC 62290 parts 1-3	Railway applications - Urban guided transport management and command/control systems - Part 1: System principles and fundamental concepts Part 2: Functional requirements specification Part 3: System requirements specification	2025
IEC 62267	Railway applications - Automated urban guided transport (AUGT) - Safety Requirement	2009

ANNEX A. HAZARD LOG

The Hazard Log is the working tool which has been used to guide and document the safety analysis. It has been created with the contribution of the participants involved in WP 8.1. Each participant oversaw the safety analysis and the review for one or more use cases or requirements.

The hazard log is located in the first worksheet of the Excel file “Risk Analysis” in ANNEX G.

ANNEX B. HAZARD LIST

The following Table 22 summarizes the identified standardized hazards in a hazard list. Each standardized hazard is linked to the use cases in which it may occur, based on the hazard identification (see chapter 4.4.1). The same hazard can also occur at different use cases. A better overview is provided by summarizing the hazards into groups. Some hazards are grouped together and marked with a bold heading. The related hazards are listed under this grouping.

Table 22 - Hazard list

Hazard ID	Standardized operational hazard	Use cases
H8.1-01	Vehicle movement	See subdivided hazards
H8.1-01-1-a and H8.1-01-1-b	Vehicle untimely sets itself in motion by applying traction from standstill	UC5.1-012, UC5.1-018, UC5.1-025, UC5.1-028, UC5.1-028, UC5.1-032, UC5.1-033, UC5.1-027, UC5.1-007, UC5.1-012, UC5.1-015, UC5.1-017, UC5.1-057, UC5.1-066, UC5.1-070, ATOREQ.38, ATOREQ.39
H8.1-01-2	Vehicle travels in the wrong direction	UC5.1-005, UC5.1-027
H8.1-01-3	excessive speed	UC5.1-007, UC5.1-007, UC5.1-009, UC5.1-018, UC5.1-025, UC5.1-026, UC5.1-027, UC5.1-037, UC5.1-069, UC5.1-070, ATOREQ.10, ATOREQ.17, ATOREQ.17, ATOREQ.25, ATOREQ.81
H8.1-02	Vehicle sets wrong traction system	UC5.1-001, UC5.1-004, UC5.1-021, ATOREQ.9, ATOREQ.51, ATOREQ.52, ATOREQ.53, ATOREQ.81
H8.1-03	Vehicle braking	See subdivided hazards
H8.1-03-1	Parking brake force reduced or not given	UC5.1-001, UC5.1-009, UC5.1-009, UC5.1-009, UC5.1-012, UC5.1-013, UC5.1-013, UC5.1-018, UC5.1-018, UC5.1-049, UC5.1-065, UC5.1-073, ATOREQ.15, ATOREQ.39, ATOREQ.41, ATOREQ.42, ATOREQ.56, ATOREQ.56, ATOREQ.81, UC5.1-026, UC5.1-026
H8.1-03-2	ATO requests traction while brakes are applied	UC5.1-009, UC5.1-038
H8.1-03-3	Passenger alarm - emergency brake request fails	UC5.1-035

Hazard ID	Standardized operational hazard	Use cases
H8.1-03-4	No reaction to detected obstacle	UC5.1-002, UC5.1-021, UC5.1-021, UC5.1-022, UC5.1-027, UC5.1-033, UC5.1-034, UC5.1-036, UC5.1-036, UC5.1-038, UC5.1-071, UC5.1-074, UC5.1-020
H8.1-04	Insufficient track guidance, track guidance fails, derailment	UC5.1-037
H8.1-05	Hazards during passenger boarding	See subdivided hazards
H8.1-05-1	Hazard to persons while boarding or door opening while vehicle is stationary	UC5.1-014, UC5.1-015, UC5.1-017, UC5.1-017, UC5.1-018, UC5.1-018, UC5.1-018, UC5.1-018, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-020, UC5.1-020
H8.1-05-1-a	Doors are released on the wrong side or outside of a safe area for the passenger exchange	See H8.1-05-1
H8.1-05-1-b	Persons trapped in the external door frame	See H8.1-05-1
H8.1-05-1-c	Passenger trapped in the platform screen door	See H8.1-05-1
H8.1-05-1-d	Person falls in the gap between platform and train	See H8.1-05-1
H8.1-05-2	Hazard to persons while boarding or door opening while vehicle is in motion	UC5.1-018, UC5.1-018, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-019, UC5.1-063
H8.1-05-2-a	Unexpected train movement while people are boarding or leaving the train - Scenario: train rolling backward	See H8.1-05-2
H8.1-05-2-b	Unexpected train movement while people are boarding or leaving the train - Scenario: train rolling forward	See H8.1-05-2
H8.1-05-2-c	Unexpected train movement while people are boarding or leaving the train - scenario: traction applied by the train	See H8.1-05-2
H8.1-05-2-d	Unexpected train movement while people are boarding or leaving the	See H8.1-05-2

Hazard ID	Standardized operational hazard	Use cases
	train - scenario: unexpected jogging of the train	
H8.1-05-2-e	Doors release command while the train is moving	See H8.1-05-2
H8.1-05-3	Hazards to persons locked inside a train not in passenger service	UC5.1-011, UC5.1-011, UC5.1-011, UC5.1-019, UC5.1-023
H8.1-06-1	Ignition and Fire	UC5.1-021, UC5.1-037, UC5.1-038, UC5.1-040, UC5.1-040, UC5.1-041, UC5.1-041, UC5.1-041, UC5.1-043, UC5.1-044, UC5.1-047, UC5.1-056, ATOREQ.39
H8.1-06-2	hot wheel	UC5.1-037
H8.1-07	Explosion Hazard	UC5.1-041, UC5.1-041, UC5.1-042, UC5.1-043
H8.1-08	Violation of the Vehicle clearance profile	UC5.1-062
H8.1-09	Hazard due to two trains approaching each other with excessive speed	UC5.1-013
H8.1-10	Conditions in the vehicle	See subdivided hazards
H8.1-10-1	Hazard due to no cooling/ no heating in normal operation	This hazard was not derived from the Use Case analysis but was instead proposed by experts from Work Package 8.1.
H8.1-10-2	Hazards due to interior objects	UC5.1-023
H8.1-10-3-a	Hazard to passengers due to unexpected, excessive train movements during travel - scenario: jerk	UC5.1-007, UC5.1-017, UC5.1-023, UC5.1-045, ATOREQ.81
H8.1-10-3-b	Hazard to passengers due to unexpected, excessive train movements during travel - scenario: lateral movement	See H8.1-10-3-b
H8.1-11	Hazards to persons outside the vehicle	See subdivided hazards
H8.1-11-1	Hazard to persons outside the train due to failure to recognize the vehicle	UC5.1-001, UC5.1-001, UC5.1-002, UC5.1-002, UC5.1-007, UC5.1-009, UC5.1-009

Hazard ID	Standardized operational hazard	Use cases
H8.1-11-2	Hazard to persons outside the train due to unexpected train movement	UC5.1-012, UC5.1-017, UC5.1-023, UC5.1-025, UC5.1-027
H8.1-11-3	Hazard to person outside the vehicle due to unfavourable aerodynamic behaviour when vehicle is passing by	UC5.1-014, UC5.1-015, UC5.1-015, UC5.1-016, UC5.1-016, UC5.1-051, UC5.1-056, UC5.1-056, UC5.1-066, UC5.1-071
H8.1-12	Emergency Situation	See subdivided hazards
H8.1-12-1	Evacuation of passengers in an emergency not possible	UC5.1-015, UC5.1-015, UC5.1-035, UC5.1-036, UC5.1-036, UC5.1-036, UC5.1-036, UC5.1-038, UC5.1-054, UC5.1-054, UC5.1-054, UC5.1-055, UC5.1-056, UC5.1-057, UC5.1-057, UC5.1-057, UC5.1-059
H8.1-12-2	Evacuation of passengers in an emergency is complicated	UC5.1-015, UC5.1-036, UC5.1-038, UC5.1-040, UC5.1-040, UC5.1-042, UC5.1-047, UC5.1-047, UC5.1-048, UC5.1-048, UC5.1-048, UC5.1-048, UC5.1-049, UC5.1-050, UC5.1-050, UC5.1-052, UC5.1-053, UC5.1-053, UC5.1-056, UC5.1-057, UC5.1-057, UC5.1-059, UC5.1-059, UC5.1-060
H8.1-12-3	Insufficient availability of vehicle functions required in an emergency	UC5.1-004, UC5.1-007, UC5.1-010, UC5.1-018, UC5.1-021, UC5.1-022, UC5.1-028, UC5.1-035, UC5.1-037, UC5.1-038, UC5.1-038, UC5.1-042, UC5.1-044, UC5.1-049, UC5.1-057
H8.1-12-4	Passengers get nervous/ panic	UC5.1-011, UC5.1-017, UC5.1-021, UC5.1-021, UC5.1-022, UC5.1-035, UC5.1-036, UC5.1-038, UC5.1-047, UC5.1-047, UC5.1-048, UC5.1-051, UC5.1-051, UC5.1-056, UC5.1-057, UC5.1-059
H8.1-12-5	Hazards due to Insufficient ventilation/ air conditioning in case of emergency	UC5.1-041, UC5.1-041, UC5.1-042, UC5.1-064
H8.1-13	hazard due to incorrect train data	See subdivided hazards
H8.1-13-1	Hazard due to wrong data received	UC5.1-006, UC5.1-003, UC5.1-006, UC5.1-014, UC5.1-014, ATOREQ.61, ATOREQ.46, ATOREQ.47, UC5.1-014, UC5.1-014, UC5.1-014

Hazard ID	Standardized operational hazard	Use cases
H8.1-13-1-a	Hazard due to wrong JP	See H8.1-13-1
H8.1-13-1-b	Hazard due to wrong MP	See H8.1-13-1
H8.1-13-1-c	Hazard due to wrong GoA level	UC5.1-001, UC5.1-003
H8.1-13-2	Hazard due to software update failure	UC5.1-001
H8.1-13-3	hazard due to wrong train ETCS mode	UC5.1-007, UC5.1-007, UC5.1-009, UC5.1-001, UC5.1-007, UC5.1-010, UC5.1-027, UC5.1-012, UC5.1-012, UC5.1-013, UC5.1-013, UC5.1-013
H8.1-13-3b	hazard due to wrong train mode (ATO operation states, TCMS modes)	See H8.1-13-3
H8.1-13-4	Hazard due to lost train location	UC5.1-010, UC5.1-013, UC5.1-001
H8.1-13-5	hazard due to wrong train data or adhesion factor	UC5.1-006, UC5.1-007, UC5.1-073
H8.1-14	loss of train integrity	UC5.1-007, UC5.1-007, UC5.1-018, UC5.1-027, ATOREQ.34, ATOREQ.38, ATOREQ.43, ATOREQ.44, ATOREQ.81, ATOREQ.26
H8.1-15	hazard while remote driving	See subdivided hazards
H8.1-15-1	Remote driving the wrong train	UC5.1-007
H8.1-15-2	Remote driving the train on a wrong route	UC5.1-007
H8.1-15-3	Remote controlled train moving without a valid video stream	UC5.1-007, UC5.1-007
H8.1-16	Hazard due to failed checks of the vehicle	See subdivided hazards
H8.1-16-1	hazard due to self-check of the vehicle not performed or results not communicated or processed	UC5.1-008, UC5.1-009, UC5.1-007
H8.1-16-2	Hazard due to failed safe reaction	UC5.1-037, UC5.1-043, ATOREQ.14

ANNEX C. EXTERNAL SAFETY BARRIERS AND SAFETY RELATED APPLICATION CONDITIONS

The following section presents the external safety barriers considered within the risk analysis. The external safety barriers are safety related preconditions fulfilled by systems outside ATO. They have been considered as risk reduction measures existing outside ATO and independent on ATO. As a result, they need to be fulfilled by the systems outside ATO as Safety related Application Conditions (SRACs). If one or more of the SRACs are not fulfilled, the related affected hazards need to be re-evaluated.

Three categories of safety barriers are listed in the Table 23 below:

- 1) Safety barriers derived from Codes of Practice,
- 2) Existing safety barriers typically implemented in railway operations, and
- 3) Newly proposed safety barriers.

Every user of the analysis results presented in this document should check if the considered Safety barriers and SRACS (see also chapter 4.2) apply to the system under consideration.

Safety barriers derived from Codes of Practice

Table 23 - List of applied Codes of Practice

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_01	<p>ETCS Subset 026</p> <p>§3.13.10.2.6</p> <p>In level 2: Train trip shall be initiated if:</p> <p>a) the on-board equipment detects that the minimum safe front end has passed the</p> <p>EOA/LOA location, OR</p> <p>b) while being in release speed monitoring, the on-board equipment receives a balise group whose first possible location (see 3.4.4.4.3.1) is known by linking information to be:</p> <ul style="list-style-type: none"> • in rear of the EOA by a distance shorter than the distance between the active Eurobalise antenna and the front end of the train, OR • at the EOA, OR • in advance of the EOA. 	<p>H8.1-01-1-a,</p> <p>H8.1-01-1-b,</p> <p>H8.1-01-2,</p> <p>H8.1-02,</p> <p>H8.1-03-01</p>

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
	<p>§3.13.10.2.7</p> <p>In Level 1: Train Trip shall be initiated if the on-board equipment detects that the minimum safe antenna position has passed the EOA/LOA location.</p> <p>§3.14.2 Roll Away Protection</p> <p>§3.14.3 Unauthorised Direction Movement Protection</p> <p>§4.6.3 train trips (EB) if condition [12], [16]:</p> <p>[12] The train/engine overpasses the EOA/LOA with its min safe antenna position) AND (ERTMS/ETCS level is 1) ; [16]:</p> <p>(The train/engine overpasses the EOA/LOA with its min safe front end) AND</p> <p>(ERTMS/ETCS level is 2).</p>	
SB_02	<p>Subset 026</p> <p>§3.13 Speed and distance monitoring</p> <p>ETCS / ATP protection</p> <p>ATP protects against overspeed (ATP (in FS) will trigger EB in case of overspeed)</p> <p>§ 3.14.2 ATP: Roll Away Protection (RAP)</p> <p>§3.14.3 Unauthorised Direction Movement Protection</p>	H8.1-01-3
SB_03	<p>EN 50388-1:2022 – Railway Applications - Fixed installations and rolling stock - Technical criteria for the coordination between electric traction power supply systems and rolling stock to achieve interoperability</p> <ul style="list-style-type: none"> - EN 50122 series – Railway applications – Fixed installations – Electrical safety, earthing and the return circuit - EN 50122-1: Covers general protective provisions for electrical safety and earthing. - EN 50122-3: Focuses on the mutual interaction of AC and DC traction systems - EN 50119 – Railway applications – Fixed installations – Electric traction overhead contact lines - EN 50121 series – Railway applications – Electromagnetic compatibility (EMC) 	H8.1-02

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
	<p>Ensures that electrical installations do not interfere with other systems and comply with EMC requirements</p> <p>TSI Energy</p> <p>§4.2.16 If a system separation section is traversed with pantographs lowered, it shall be designed so as to avoid the electrical connection of the two power supply systems by an unintentionally raised pantograph.</p> <p>- 4.3.4 part 2 : The relevant information to perform the switching of the circuit breaker, change of maximum train current, change of the power supply system and pantograph management shall be transmitted via ERTMS when the line is equipped with ERTMS.</p>	
SB_04	<p>Parking braking requirements:</p> <p>'EN 16185-1, 5.11.4 (parking brake):</p> <p>- The purpose of a braking brake is to keep the train stationary in shut down configuration for an indefinite period of time without energy supply.</p> <p>- The parking brake shall be capable of securing an EMU/DMU in the load condition design mass in working order in accordance with EN 15663 in a stabling point (depot) on a gradient of 0,5 % if not otherwise specified.</p> <p>Applying of parking brakes: LOC&PAS</p> <p>Subset026:</p> <p>ATP: Roll Away Protection (RAP)</p>	H8.1-03-01
SB_05	<p>LOC&PAS TSI Commission Regulation (EU) No.1302/2014 (clause 4.2.5.3.2, 4.2.5.3.3, 4.2.5.3.5) and Guidance for the application LOC&PAS TSI</p> <p>- Clause 4.2.5.3.5: Passenger alarm: Safety requirements</p> <p>(1) For the scenario 'failure in the passenger alarm system leading to the impossibility for a passenger to initiate the activation of brake in order to stop the train when train departs from a platform', it shall be demonstrated that the risk is controlled to an acceptable level considering that the functional failure has typical credible potential to lead directly to "single fatality and/or severe injury.</p>	H8.1-03-03

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_06	<p>ON-BOARD</p> <p>TSI LOC&PAS 4.2.3.3.2 (Axle bearing condition monitoring)</p> <p>(2) For units of maximum design speed higher than or equal to 250 km/h, on board detection equipment shall be provided.</p> <p>(3) For units of maximum design speed lower than 250 km/h and designed to be operated on others track gauge systems than the 1520 mm system, axle bearing condition monitoring shall be provided and be achieved either by on board equipment (according to specification in 4.2.3.3.2.1) or by using track side equipment (according to specification in 4.2.3.3.2.2).</p> <p>TRACKSIDE</p> <p>EN 15437-1:2009 (Axle box condition monitoring)</p>	H8.1-06-2
SB_07	<p>Subset 34 and 36-5: platform information is available for the OBU</p> <p>Subset 125, clause 6.4.2.5 - The JP shall identify, for each Stopping Point, if the ATO-OB has to manage train doors opening (including the sides for opening the doors) and train doors closing</p> <p>ERTMS/ETCS; Subset 34, version 3.2.0; Train Interface FIS; section 2.4.6 "Station platform"</p> <p>ERTMS/ETCS; Subset 026-5, version 3.6.0; System Requirements Specification - Chapter 5 Procedures; section 5.20.8 "Station platform"</p> <p>TSI LOC&PAS 4.2.5.5.6 door opening</p>	H8.1-05-01-a
SB_06	<p>Door obstacle detection according to TSI LOC&PAS, section 4.2.5.5.3</p> <p>Door - traction interlock according to TSI LOC & PAS, section 4.2.5.5.7</p>	H8.1-05-1-b
SB_09	<p>TSI OPE - Appendix D - Route compatibility and Route Book – Gauging</p>	H8.1-05-1-d

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_10	<p>Subset026</p> <p>§3.14.2</p> <p>3.14.2.2 The Roll Away Protection (RAP) shall prevent the train from moving in a direction, which conflicts with the current position of the direction controller in the active desk.</p>	H8.1-05-2-a
SB_11	<p>Door - traction interlock according to TSI LOC & PAS, section 4.2.5.5.7</p> <p>(1) Traction power shall be applied only when all doors are closed and locked. This shall be ensured through an automatic door-traction interlock system. The door-traction interlock system shall prevent traction power being applied when not all of the doors are closed and locked.</p> <p>(2) The traction interlock system shall be provided with a manual override, intended to be activated by the driver in exceptional situations, to apply traction even when not all of the doors are closed and locked."</p> <p>EN14752:2019+A1:2021 Railway applications - Bodyside entrance systems for rolling stock</p>	H8.1-05-2-c, H8.1-05-2-d
SB_12	<p>TSI LOC & PAS 4.2.5.5.7 and 4.2.5.5.8</p> <p>For the scenario several doors are unlocked (with train crew not correctly informed of this door status) or released or opened in inappropriate areas (e.g. wrong side of the train) or situations (e.g. train running), it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible direct potential to lead to:</p> <ul style="list-style-type: none"> — ‘fatality and/or severe injury’ for units in which passengers are not supposed to stay in standing position in the door area (long distance), or to — ‘fatalities and/or severe injuries’ for units in which some passengers stay in standing position in the door area in normal operation. <p>For information: Door opening inhibited by the door control system if speed > 3 - 5 km/h EN 14752:2019+A1:2021- Railway applications. Bodyside entrance systems for rolling stock sections 4.8 and 5.1.2.</p>	H8.1-05-2-e

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_13	<p>TSI LOC&PAS</p> <p>4.1.4 "Categorisation of rolling stock for fire safety"</p> <p>4.2.10 "Fire safety and evacuation" 4.2.10.1 "General and Categorisation"</p> <p>4.2.10.2 "Measures to prevent fire"</p> <p>TSI LOC&PAS 4.2.10.2.1 Material requirements (1) The selection of materials and components shall take into account their fire behaviour properties, such as flammability, smoke opacity and toxicity. (2) Materials used to construct the rolling stock unit shall comply with the requirements of the specification referenced in Appendix J-1, index [30] for the 'Operation Category' as defined below: ...</p> <p>4.2.10.3 "Measures to detect/control fire"</p> <p>4.2.10.4 "Requirements related to emergencies"</p> <p>4.2.10.5 "Requirements related to evacuation"</p> <p>Appendix J-1, index [30]:</p> <p>EN 45545-2:2020 Railway applications - Fire protection on railway vehicles - Part 2: Requirements for fire behaviour of materials and components</p>	H8.1-06-01, H8.1-12-5
SB_14	<p>Installation of ETCS Level2 incl. handling of all defined modes of ETCS (for GoA 4)</p> <p>Subset 026</p> <p>§3.13 Speed and distance monitoring</p> <p>ETCS / ATP protection</p> <p>ATP protects against overspeed (ATP (in FS) will trigger EB in case of overspeed)</p>	H8.1-09
SB_15	<p>Traction/ Braking Control System</p> <p>TSI LOC&PAS 4.2.4.2.1. (15) For speeds higher than 5 km/h, the maximum jerk due to the use of brakes shall be lower than 4 m/s³.</p> <p>EN14363 dynamic behaviour of trains</p>	H8.1-10-3-a

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_16	<p>For authorised persons there is existing a rule regarding maintenance on track</p> <p>persons are responsible to secure all maintenance staff in Germany:</p> <p>Prohibition of accessing the track area, as per § 62 EBO</p> <p>Regulation for staff: "DGUV Verhalten bei Arbeiten im Gleisbett"/RIL 132.0118</p> <p>RiL 408: Züge fahren</p> <p>Ril 513.2020: Maßnahmen zur Abwendung von Überfüllungen auf Bahnsteigen sicherstellen</p> <p>Ril 513.2011: Sicherungsmaßnahmen auf Bahnseigen sicherstellen</p> <p>Ril 513.2030: Warn- und Sicherheitsschilder</p>	H8.1-11-1
SB_17	<p>construction and design related standards/rules existing, e.g. to install white, yellow or tactic marked line at station related to allowed speed for passing trains; national rules to be considered (similar regulation assumed in other countries);</p> <p>Example for Germany (equal regulation assumed in other counties):</p> <p>Regulation for staff:</p> <ul style="list-style-type: none"> - "DGUV Behaviour when working on the track" - In a group, the responsible task of some of the persons is to warn the others (RiL 132.0118) <p>At platform:</p> <ul style="list-style-type: none"> - white marker line, warning signs, acoustic warning if required according to existing regulations for station operation <p>Regulation for station management especially for overcrowded platform:</p> <ul style="list-style-type: none"> - Ril 513.2020: Maßnahmen zur Abwendung von Überfüllungen auf Bahnsteigen sicherstellen - Ril 513.2011: Sicherungsmaßnahmen auf Bahnsteigen sicherstellen - Ril 513.2030: Warn- und Sicherheitsschilder 	H8.1-11-3

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
SB_18	<p>TSI 1302/2014</p> <p>4.2.10.4.4.</p> <p>(2) The unit shall be designed so that, in the event of fire on-board, the running capability of the train will enable it to run to a suitable firefighting point.</p> <p>(3) Compliance shall be demonstrated by application of the specification referenced in Appendix J-1, index 63, in which the system functions impacted by a 'type 2' fire shall be:</p> <p>— braking for rolling stock of fire safety category A: this function shall be assessed for a duration of 4 minutes.</p> <p>— braking and traction for rolling stock of fire safety category B: these functions shall be assessed for a duration of 15 minutes at a minimum speed of 80 km/h.</p> <p>the TSI requirements in this cell are necessary but not sufficient. Please consider the SRACS in column F on the TSI points (2) and (3).</p>	H8.1-12-3
SB_19	<p>TSI 1302/2014</p> <p>4.2.5.8</p> <p>4.2.7.1.4</p> <p>4.2.10.4.1</p> <p>4.2.5.8 Internal air quality</p> <p>— In case of interruption of the ventilation, due to an interruption of the main power supply or to a breakdown of the system, an emergency provision shall ensure the supply of outside air into all passenger and staff areas.</p> <p>If this emergency provision is ensured through battery supplied forced ventilation, the duration in which the CO2 level will remain below 10 000 ppm shall be defined, assuming a passenger load derived from the load condition 'design mass under normal payload'.</p> <p>4.2.7.1.4 lamp control</p> <p>"Note: where it is intended to use lights to inform of an emergency situation (operating rule, see TSI OPE), this should be done only by means of head lamps in flashing/blinking mode. "</p>	H8.1-12-4

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
	<p>4.2.10.4.1 Emergency lighting</p> <p>1) To provide protection and safety on board in the event of emergency the trains shall be equipped with an emergency lighting system. This system shall provide a suitable lighting level in the passenger and in the service areas, as follows:</p> <p>(2) for units of maximum design speed higher than or equal to 250 km/h, during a minimum operating time of three hours after the main energy supply has failed,</p> <p>(3) for units of maximum design speed lower than 250 km/h, during a minimum operating time of 90 minutes after the main energy supply has failed.</p> <p>(4) Lighting level of at least 5 lux at floor level.</p> <p>(5) Values of lighting level for specific areas and conformity assessment methods shall be as specified in the specification referenced in Appendix J-1, index 62.</p> <p>(6) In the event of fire, the emergency lighting system shall continue to sustain at least 50 % of the emergency lighting in the vehicles not affected by fire for a minimum of 20 minutes. This requirement shall be deemed to be fulfilled by a satisfactory failure mode analysis.</p>	
SB_20	<p>Partially: ATO to be used together with ATP that supervises the speed and distance. Defined in Subset 125 and Subset 026 (for GoA2)</p> <p>ERTMS/ATO (covered for GoA2 under driver supervision). Assumed SIL4 ATP in 8.3 for supervised modes.</p>	H8.1-13-1-a, H8.1-13-1-b
SB_21	<p>ETCS subset 026 - Part 4 - Clause 4.5.2</p> <p>Strict validation of mode transitions, if the train changes the mode from SR or SH to FS, these onboard functions need to be active (Figure 1 Active function table)</p> <p>Check linking consistency</p> <p>Check message consistency for balise groups announced by linking and for other balise groups marked as linked while the linking consistency is checked</p>	H8.1-13-3

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
	<p>Check balise detection degradation</p> <p>Check balise crosstalk while expecting repositioning information</p> <p>Check safe radio connection (only level 2)</p>	
SB_22	<p>Subset 125: ERTMS/ATO: System Requirement Specification: The ATO System shall be ready for ATO operation (ATO Operational) when the</p> <p>following conditions are satisfied:</p> <p>The current ETCS Mode is FS Mode and “ENTRY IN FULL SUPERVISION” procedure has finished (See [Ref 5] §4.4.9.1.4).</p> <p>When the ETCS-OB is not in FS Mode, the ATO-OB traction command shall be safely cut-out.</p>	H8.1-13-3
SB_23	<p>Trackside supervision function:</p> <p>axle counters, balises; Subset-026 part 2 - §2.6.5.1.4 / 2.6.6.1.4</p> <p>Train detection and train integrity supervision are performed by the trackside equipment of the underlying signalling system (interlocking, track circuits etc.) and are outside the scope of ERTMS/ETCS. Safety barrier outside of ATO.</p> <p>onboard:</p> <p>ETCS Subset 026/03 - Cold Movement Detection:</p> <p>3.15.8.1 After being switched off (i.e. once in No Power mode), the ERTMS/ETCS on-board equipment shall be capable, if fitted with, to detect and record whether the engine has been moved or not, during a period of at least 72 hours.</p> <p>3.15.8.1.1 To allow small movements e.g. for coupling in No Power mode, the ERTMS/ETCS on-board equipment shall consider that no cold movement has occurred as long as the train does not move for more than 2m away from the train position stored when No Power mode was entered.</p> <p>train location lost while train is running:</p> <p>3.16.3.4 Supervision of safe radio connection</p> <p>3.16.3.4.1 When the difference between the time stamp of the latest received message and the current on-board time is greater than the T_NVCONTACT parameter (national value), the on-board shall apply the reaction required by trackside (see 3.16.3.4.2).</p>	H8.1-13-4

Barrier ID	Safety barrier description (Code of Practice)	Hazard ID
	<p>3.16.3.4.2 It shall be possible to select one of the following reactions (National value):</p> <ul style="list-style-type: none"> a) Train trip b) Apply service brake c) No reaction <p>3.14.1.7 If the brake command was triggered due to supervision of the safe radio connection (T_NVCONTACT) the brake command shall be released at standstill or if a new message has been received from the RBC.</p> <p>3.13.10.4.10 The on-board equipment shall compare the estimated speed and train position with the ceiling and braking to target supervision limits and shall trigger/revoke commands to the train interface (traction cut-off if implemented, service brake if available for use or emergency brake) and supervision statuses, by evaluating and taking into account the conditions as specified in clause 3.13.10.4.10.1.</p> <p>3.14.1.2 In case only the application of (the non-vital) service brake has been commanded, and the service brake fails to be applied, the emergency brake command shall be given.</p>	
SB_24	<p>TSI CCS and TIMS for passenger trains (Baseline 4: Subset 91/120: Train integrity should be at least SIL 2, still under discussion)</p> <p>For all ETCS Tracks:</p> <p>TSI CCS:</p> <p>7.6. Train detection systems specific implementation rules.</p> <p>For tracks where moving block is applied:</p> <p>TSI CCS 7.2.9.1: "An ETCS Level 2 Trackside application with no or reduced train detection (formerly ETCS level 3) relies on on-board information to determine track occupation and requires that the on-board is able to fulfil the requirements for confirmed train length information as specified in Appendix A, Table A 2, index 27"</p> <p>Baseline 4: Subset 91/ 120: Train integrity should be at least SIL 2, still under discussion</p>	H8.1-14

Existing Safety barriers

The Table 24 presents additional safety barriers that were identified by experts within the Work Package, rather than being derived from established Codes of Practice.

Table 24 - List of applied existing safety barriers

Barrier ID	Existing Safety barrier description	Hazard ID
SB_25	Before any maintenance/inspection activity around or inside the train, required measures shall be taken to keep the train standstill at all times.	H8.1-01-1-b
SB_26	A person fallen in the gap can self-rescue or be rescued by other nearby persons	H8.1-05-1-d
SB_27	A person inside a train not in passenger service can self-rescue (e.g. use their phone to call for rescue).	H8.1-05-3
SB_28	Train attendants coordinate evacuation of the passengers (GoA3).	H8.1-06-1
SB_29	The training of cleaners to remove trash, working equipment and cleaning equipment.	H8.1-10-2
SB_30	Person can recognise vehicle because of the Marker light / Head light /front light activation. Maintenance workers are trained to follow the rules for going in a track in operation.	H8.1-11-1, H8.1-11-2
SB_31	Announcement system at station/platform to warn passengers at platform about passing train according to national rules is established. Person can recognise vehicle because of the Marker light / Head light /front light activation. National rules about the allowance of train passing platforms with a certain speed and safety markings on the platform apply.	H8.1-11-3
SB_32	The detection of an emergency and the communication with the emergency management centre can independently occur outside ATO, e.g. through passengers calling the emergency number with their mobile phones, or through RU staff monitoring the stations through CCTV. RU have operational rules about evacuation.	H8.1-12-1

Proposals for new (not already implemented) safety barriers

The Table 25 presents proposals for new (not already implemented) safety barriers that were identified by experts within the Work Package.

Table 25 - List of proposed new safety barriers

Barrier ID	New Safety barrier proposal description	Hazard ID
SB_35	<p>IEC62290-2 - 5.5.10 Manage traction power supply on train. (for metro)</p> <p>This function is intended to manage traction power supply during train operation (e.g. selection of current collector, AC/DC selection, voltage selection, automatic raising and lowering of pantographs and collector shoes, automatic opening/closing of circuit breakers).</p> <p>This function is for instance applicable if several power systems are fitted for a given line.</p>	H8.1-02

The Table 26 lists all identified Safety-Related Application Conditions (SRACs).

Table 26 - List of derived Safety related application conditions (SRAC)

SRACs No.	SRAC Description	Related hazards
SRAC_01	Temporary Speed restrictions shall be transferred to ETCS in real time.	H8.1-01-3
SRAC_02	<p>It shall be ensured that the train is adequately immobilized for an extended period or higher gradient (e.g. brake shoes).</p> <p>The correct applying of the parking brake is to be checked before shutting off the train.</p>	H8.1-03-1
SRAC_03	Between the stations the acknowledgment and the reaction of the passenger emergency alarm shall be done in a safe way.	H8.1-03-3
SRAC_04	GoA 4: operational rule for reaction after flat wheel detection be implemented	H8.1-04

SRACs No.	SRAC Description	Related hazards
SRAC_05	<p>Each infrastructure manager shall evaluate the risk for this hazard and, if necessary, define safety measures.</p> <p>Elements to be considered in the risk estimate include:</p> <ul style="list-style-type: none"> - the existence of a gap between the platform and the trains operated on that platform - the platform characteristic - the expected number of persons getting on and off - the potential for overcrowding - the train characteristics. <p>If the risk is not acceptable, new safety barriers or safety functions need to be introduced, e.g. the supervision of the passenger exchange.</p>	H8.1-05-1-d
SRAC_06	the train shall be safely immobilized (e.g. by the holding brake application) during the passenger exchange	H8.1-05-2-b
SRAC_07	<p>a function shall be implemented, that covers the following driver's task with a suitable TFFR:</p> <ul style="list-style-type: none"> - ATO can request traction only when the doors are closed <p>Additionally, the manual override of the door-traction interlock needs to either:</p> <ol style="list-style-type: none"> 1) be completely separated from ATO (i.e. ATO cannot override the door traction interlock) <p>OR</p> <ol style="list-style-type: none"> 2) be implemented with a suitable TFFR 	H8.1-05-2-c
SRAC_08	a safety function or process shall be implied to check if all passengers left the train	H8.1-05-3
SRAC_09	after fire detection a safety reaction shall be implemented	H8.1-06-1
SRAC_10	GoA 4: operational rule for reaction after hot wheel detection and stopping of train shall be implemented	H8.1-06-2

SRACs No.	SRAC Description	Related hazards
SRAC_11	An announcement for the passengers about malfunction of HVAC and additional information, like the affected train unit shall be made. Malfunction of the HVAC shall be communicated to operator/ IM.	H8.1-10-1
SRAC_12	IM shall be responsible for the quality of the track (supervision and maintenance to avoid twisted tracks).	H8.1-10-3-b
SRAC_13	Existing, country specific standards and rules regarding trains passing crowded stations shall be followed. Risk analysis for related platform/station shall be updated and requested by the infrastructure manager if needed. For GoA4 operation: Requirements for the activation of horn and emergency brake shall be defined. Correct function of head lights/marker lights on vehicle shall be ensured.	H8.1-11-1, H8.1-11-3
SRAC_14	Additional functions shall be implemented for communication from train to operational / traffic manager and from operational /traffic managers to the passengers A dedicated safety concept for emergency handling shall be developed. This concept shall also address the possibility to bypass some safety functions in an emergency (e.g. avoid an unwanted train stop and ensure traction).	H8.1-12-1, H8.1-12-2, H8.1-12-3, H8.1-12-4, H8.1-12-5
SRAC_15	A) The TSI text at point (2) shall be amended and clarified for GoA3 and GoA4 operation. In case of GoA3 or 4 operations, instead of "the unit shall be designed" a possible and suggested amendment is "The unit, including ATO, and the communication between the unit and the emergency management centre shall be designed ..." B) The TSI text at point (3) shall be amended. A possible and suggested amendment is: proposal to add at the end of point (3) "While assessing compliance of the braking and traction, the communication between the unit and the emergency management	H8.1-12-3

SRACs No.	SRAC Description	Related hazards
	<p>centre and the ATO command of the braking and traction shall be considered"</p> <p>NOTE: the communication is only partially in scope of TSI LOC & PAS, as it does not only involve the rolling stock, but also the infrastructure. An analogous clause in the TSI Infra should be added.</p>	
SRAC_16	<p>in future update of the TSI Operations there shall be a GoA level train- track compatibility check.</p> <p>The solution in the Use cases and in the SRS looks not completely standardized so it may be necessary to export safety requirements to the subsystems like TCMS related to driver's presence in the cabin.</p> <p>It shall be defined how the system reacts if it loses GoA4.</p>	H8.1-13-1-c
SRAC_17	<p>For ATP on board ERTMS a SIL4 Odometry system is required according to Subset 091 and a safety function related to location of a train.</p>	H8.1-13-4
SRAC_18	<p>A technical solution on the train shall be implemented to detect and communicate the loss of train integrity.</p> <p>For moving block, a train Integrity Monitoring System (TIMS) is required.</p>	H8.1-14
SRAC_19	<p>self-checks shall be carried out according to the planned periods and results shall be communicated to the IM (or the entity in charge) to process.</p>	H8.1-16-1
SRAC_20	<p>"Störleuchtmelder/ Leuchtmelder Instandhaltungsbedarf" (lamp indicating maintenance needs)</p> <p>Indications of the lamp shall be safely communicated to the operator/ TCC.</p>	H8.1-16-2

ANNEX D. FINAL THR FOR THE HAZARDS

The Table 27 below contains the final THR for each of the identified hazards.

Basic Integrity

Some hazards are associated to BI (Basic Integrity). They are the hazards that have the potential to be completely controlled by a Code of Practice (CoP), given that the CoP is correctly applied and with the necessary and sufficient safety integrity. The users of this document (e.g. designers supported by safety engineers) need therefore to verify whether, with regards to the users scope (e.g. design of the Automating Function for a generic or specific application) the CoP are correctly applied with the sufficient and necessary safety integrity; if that is true, then the Automatic Functions associated to the hazard can be implemented with Basic Integrity, as the hazard is already completely controlled by CoP.

For instance, for the hazard H8.1-01-2 – vehicle travels in the wrong direction – is marked as BI. This means one or more CoP have been identified for the hazard; they are listed in ANNEX C. The specific Code of Practice is SB_01 in ANNEX C, i.e. the operation under ETCS FS, including the Rollback Protection function. If the generic or specific application is compliant with operation under ETCS FS, with specific reference to the Rollback Protection, then the hazard is completely controlled, and the related Automating Functions can be implemented as BI.

If the CoP is not fully applied, or if it is applied without a sufficient safety integrity, then the THR from the Table 27 below is not applicable and needs to be updated.

For instance, for the hazard mentioned above H8.1-01-2 – vehicle travels in the wrong direction, if the generic or specific application includes operation outside ETCS, or anyhow without any safety function equivalent to the SIL4 ETCS Rollback Protection, then the risk analysis for the hazard needs to be H8.1-01-2 customised and the THR for the Automating Functions dealing with the hazard needs to be recalculated.

Quantitative targets (e.g. 1.00 E-7 occurrence per hour)

Some hazards are associated to quantitative targets, defined based on the CSM-RA harmonised design targets. The quantitative targets consider the severity of the consequences (accidents) caused by the hazards and the risk reduction by the external safety barriers, i.e. by risks control measures outside the Automating Functions and completely independent on them.

For instance, a hazard which could lead to catastrophic consequences (e.g. collision) and not mitigated by any external safety barrier would have a final THR of 1.00E-09 occurrences / hour. On their other hand, if external safety barriers were identified for that hazard, the final THR has been adjusted accordingly (e.g. to 1E-8 occurrence per hours).

Table 27 - Final THR per hazard

Hazard ID	Hazard	Final THR
H8.1-01-1-a	Vehicle untimely sets itself in motion by applying traction from standstill – collision train-train	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-01-1-b	Vehicle untimely sets itself in motion by applying traction from standstill – collision train-staff	1.00E-04
H8.1-01-2	Vehicle travels in the wrong direction	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-01-3	Excessive speed	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-02	vehicle sets wrong traction system	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-03-1	Parking brake force reduced or not given	1.00E-09
H8.1-03-3	Passenger alarm - emergency brake request fails	1.00E-09
H8.1-04	Insufficient track guidance, track guidance fails, derailment due to flat wheel	1.00E-09
H8.1-05-1-a	Doors are released on the wrong side or outside of a safe area for the passenger exchange	1.00E-08

Hazard ID	Hazard	Final THR
H8.1-05-1-b	Persons trapped in the external door frame	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-05-1-d	Persons fall in the gap between the platform and the train	3.3E-07
H8.1-05-2-a	Unexpected train movement while people are boarding or leaving the train - rolling backward	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-05-2-b	Unexpected train movement while people are boarding or leaving the train - rolling forward	1.00E-07
H8.1-05-2-c	Unexpected train movement while people are boarding or leaving the train - traction applied by the train	1.00E-07
H8.1-05-2-d	Unexpected train movement while people are boarding or leaving the train - unexpected jogging	3.30E-05
H8.1-05-2-e	Doors release command while the train is moving	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-05-3	Hazards to persons locked inside a train not in passenger service	3.00E-07
H8.1-06-1	Ignition and Fire	1.00E-07
H8.1-06-2	Hot wheel	1.00E-09
H8.1-07	Explosion Hazard	no final THR as the CoP can fully mitigate the hazard, therefore, the related

Hazard ID	Hazard	Final THR
		Automating Functions can be implemented as Basic Integrity
H8.1-09	Hazard due to two trains approaching each other with excessive speed	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-10-1	hazard due to no cooling/ no heating in normal operation	1.00E-07
H8.1-10-3-a	Hazard to passengers due to unexpected, excessive train movements during travel	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-10-3-b	Hazard to passengers due to unexpected, excessive train movements during travel - scenario: lateral movement	1.00E-06
H8.1-11-1	Hazard to persons outside the train due to failure to recognize the vehicle	1.00E-07
H8.1-11-2	Hazard to persons outside the train due to unexpected train movement	1.00E-04
H8.1-11-3	Hazard to person outside the vehicle due to unfavourable aerodynamic behaviour when vehicle is passing by	3.30E-06
H8.1-12-1	Evacuation of passengers in an emergency not possible	1.00E-07

Hazard ID	Hazard	Final THR
H8.1-12-2	Evacuation of passengers in an emergency is complicated	1.00E-07
H8.1-12-3	Insufficient availability of vehicle functions required in an emergency	1.00E-07
H8.1-12-4	Passengers get nervous/ panic	1.00E-07
H8.1-12-5	Hazards due to Insufficient ventilation/air conditioning in case of emergency	1.00E-07
H8.1-13-1-a	hazard due to wrong JP	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-13-1-b	hazard due to wrong MP	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-13-1-c	hazard due to wrong GoA level	1.00E-09
H8.1-13-3	hazard due to wrong train ETCS mode	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-13-4	hazard due to lost train location	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-13-5	hazard due to wrong train data or adhesion factor	1.00E-09

Hazard ID	Hazard	Final THR
H8.1-14	loss of train integrity	no final THR as the CoP can fully mitigate the hazard, therefore, the related Automating Functions can be implemented as Basic Integrity
H8.1-16-1	hazard due to self-check of the vehicle not performed or results not communicated or processed	No final THR (this hazard needs to be analysed further)
H8.1-16-2	hazard due to failed safe reaction	No final THR (this hazard needs to be analysed further)

ANNEX E. EXPLICIT RISK EVALUATION – RISK REDUCTION

An explicit risk estimation has been carried out in case hazards could not be completely controlled through codes of practice or similar reference systems. The explicit risk estimation has been performed on a hazard per hazard basis. It was aimed at identifying the final (i.e. residual) THR (Tolerable Hazard Rate) for the analysed hazard, once the external safety barriers have been considered.

Initial THR

The starting point of the explicit risk estimation is the definition of an initial THR. The initial THR is selected based on the severity of the accident linked to the hazard. According to the CSM-RA [2] and [3], Art.3 points (36) and (37) and Annex I, clause 2.5.5 (a) and (b):

“(a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.

(36) “highly improbable” means an occurrence of failure at a frequency less than or equal to 10^{-9} per operating hour;

(b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable

(37) “improbable” means an occurrence of failure at a frequency less than or equal to 10^{-7} per operating hour.”

Table 28 - Initial THR based on the harmonised design criteria from CSM-RA [2] and [3]

Severity category	Consequences to persons	Initial THR [failures / h]
Catastrophic	Affecting a large number of people and resulting in multiple fatalities	1E-9
Critical	Affecting a very small number of people and resulting in at least one fatality	1E-7

Safety barriers

Safety barriers are defined according to the CSM-RA [2] and [3], Article 3, point (34). The explicit risk estimation evaluated only external safety barriers, as defined below:

External safety barrier = a technical, operational or organisational risk control measure outside the system under consideration (i.e. outside the Automating Functions), which is:

- capable of reducing the risk associated to the hazard
- completely independent on the Automating Functions from a physical and functional point of view

NOTE: for the exhaustive definition of independence, see EN50129 [6], Annex A, section A 4.2.2.1 “Physical independence” and A 4.2.2.2 “Functional independence” as well as Annex B, section B.3.2 “Independence of items”

Risk reduction – technical safety measures

The risk reduction is calculated differently for the different risk control measures.

The risk reduction for each technical risk control measures is calculated according to the “composite fail safe principle” from EN50129 [6], based on the assumption that:

- 1) The external technical safety barrier is completely independent on the Automating Function
- 2) The external safety barrier alone prevents the dangerous consequences caused by an Automating Function failure

In other words, for an accident to happen, both the Automating Functions and the external technical safety barrier need to be in a dangerous failure state at the same time (see EN50129 [6], Annex B, figure B.2). From an FTA (Fault Tree Analysis) point of view, this is modelled by an AND gate between two items i.e. Automating Function and External Technical Safety Barrier, with each item modelled with a Dormant Failure Event.

Numerical values for the risk reduction have been calculated considering the formula A.1 in Annex A of EN50129 [6] and the model in EN50129 [6], Annex B, figure B.2. Numerical values for the risk reduction have been validated through FTAs. Assumed realistic estimate have been formulated for the failure rate and for the inspection interval of the External Technical Safety Barrier.

NOTE 1: complete physical and functional independence between the external technical safety barriers and the Automating Function needs to be ensured at a system level to avoid common cause failures for random failures; if that is not possible, the results from the risk analysis (with specific reference to the THR) need to be adapted accordingly.

NOTE 2: adequate independence (e.g. development independence for SW) for the external technical safety barriers and the Automating Function needs to be ensured at a system level to avoid systematic faults affecting both the external technical safety barrier and the Automating Function.

Risk reduction – measures implemented by human actors (including operational and organisational measures directly carried out by persons)

The risk reduction for risk control measures which are directly implemented by human actors (e.g. a check by the Railway Undertaking staff) is calculated based on the available literature concerning human errors, based on the following parameters:

- Task complexity (3 categories: intuitive task with clear rules and good training, clear rules and good training, no rules and no routine)
- Work conditions (2 categories: Good conditions for sight, noise, temperature, influence of physical forces or otherwise)
- Stress level (2 categories: optimal or otherwise)

Risk reduction – operational and organizational safety measures not implemented by human

In some cases, it was not possible to determine whether a specific operational or organisational risk control measure was implemented through a technical solution or through human intervention. In that case, a conservative risk reduction factor based on expert judgement was performed. Example: “Passenger on platform should be informed about passing train; national rules about the allowance of train passing platforms”

Other risk reduction factors – physical and probabilistic

Where applicable, other risk reduction factors have been considered, such as the presence of physical limitations preventing a hazard from evolving into an accident.

Additionally, probabilistic considerations have been considered for some hazards, e.g. if the hazard does not directly lead to accidents. For instance, an Automating Function failure causing a lack of traction usually only affects availability, with no safety impact. The lack of traction can have safety relevant consequences only in an emergency scenario (e.g. fire onboard, with the train needing traction to reach a safe area for evacuation). As emergency scenarios are rare. In those cases, a regular inspection of the Automating Function is needed

Final THR

The final THR reflects the residual THR once the risk reduction due to the external, independent safety barriers has been calculated.

ANNEX F. HAZOP

The HAZOP table is located in the attached Excel-File. For the evaluation of the hazard H8.1-12 some adjustments have been made, which can be found in the further worksheets of this file.



FP2-T8_1-D-SMO-09
3-03_%20Annex_F_H/

ANNEX G. RISK ANALYSIS

The excel table attached below presents the complete Risk Analysis for all identified hazards. Table 29 lists the columns of the table with an explanation.

Table 29 - Risk Analysis columns explanation

Column	Description	Explanation
Column A	Hazard ID	The numbering of the line
Column B	Hazard description	Description of the Hazard
Column C	Comment	Additional information of the hazard, e.g. covering at another use case of work package
Column D	Responsible participant	Lead participant of the analysis of the use case.
Column E	Related UC	Use case of WP 5.1 in which the hazard is related.
Column F	Accident	The list of accidents happened in case of failure condition happen on functions
Column G-I	Risk Evaluation without Safety Barriers	Risk evaluation of the hazard without Safety barriers, including the severity category, severity justification and initial THR.
Column J-L	Code of Practice	Reference to an external Subsets, TSI etc, which can be compared to the concept of failure described above
Column M-O	Similar reference system analysis	Consideration of similar reference system that address this hazard, justification of the applicability and the evaluation, if the hazard is completely controlled by this similar reference system.
Column P	All Safety barriers description	Description of all barriers to the hazard.
Column Q-U	Technical Safety Barriers	These columns describe the external technical barriers which can intervene in the event of the condition for the analysed hazard occurs, according to the inspection interval applied on barriers (column R) and function failure rate of barriers (column S) it is possible to calculate a factor for the risk reduction (columns T, U) which contributes to the initial risk reduction applied to the initial THR (see column I).

Column	Description	Explanation
Column V-AC	Human Safety Barrier	<p>These columns describe the Human barriers which can intervene in the event of the condition for the analysed hazard occurs, in accordance with the following risk reduction options:</p> <p>Risk reduction based on task (column W, X)</p> <p>Risk reduction based on work condition (column Y, Z)</p> <p>Risk reduction based on stress level (column AA, AB)</p> <p>It is possible to calculate the total risk reduction factors based on human safety barriers (column AC) which contributes to the initial risk reduction applied to the initial THR (see column I).</p>
Column AD-AG	Operational barriers	<p>These columns describe the operational obstacles that may apply if the conditions for the analysed hazard occur. The description and the applicable traffic density (Column AE) are specified.</p> <p>It is possible to calculate the total risk reduction factors based on operational safety barriers (column AG) which contributes to the initial risk reduction applied to the initial THR (see column I).</p>
Column AH-AK	Physical barrier	<p>These columns describe the Physical barriers with physical condition which can reduce the risk reduction according to the percentage of intervention of a physical barrier (column AI), it is possible to calculate a factor for the risk reduction (column AK) which contributes to the initial risk reduction applied to the initial THR (see column I)</p>
Column AL-AM	Functions Traceability	Description of linked functions and functions independencies.
Column AN	Final Risk reduction factor	In this column is reported the sum of all the contributions calculated for each external barrier is reported and represents the final risk reduction factor to be applied to the initial THR of the hazard.
Column AO-AR	Final THR for hazard	<p>In these columns have been reported the final values of final THRs of hazards according to the Final risk reduction factors reported in column AN and according to which initial THR was chosen on functions according to the following initial THRs choices:</p> <p>THR=1E-09 (column AO)</p> <p>THR=1E-07 (Column AP)</p> <p>THR=1E-06 (Column AQ)</p> <p>THR=1E-05 (Column AR)</p>

Column	Description	Explanation
Column AS	Final Impact	In this column is reported the final impact after the external safety barriers application.
Column AT	Comments	In this column are reported all comments related risk evaluation analysis.
Column AU	Assumptions	In this column are reported all assumptions related risk evaluation analysis.
Column AV	SRAC description	In this column are reported all Safety related application condition (SRAC) applicable on the function's safety analysis
Column AW	Exported to	It is reported to which external module, body, natural person, manual etc. the SRAC is exported.

The Risk Analysis is located in the third worksheet of the attached Excel file, while an overview of the results can be found in the fourth worksheet.



FP2-T8_1-D-SMO-09
3-03_Annex_G_Risk_A