Rail to Digital automated up to autonomous train operation

D8.3: Safety analysis for ATO functions

Due date of deliverable: 20/12/2024

Actual submission date: 12/12/2025

Leader/Responsible of this Deliverable: Gabriele Foreste, Hitachi rail STS

Reviewed: Y

Document status

Revision	Date	Description
01	20/12/2024	First issue
02	20/12/2024	Formal changes
03	20/12/2024	Formal changes
04	14/01/2025	Deleted comments in the document
05	04/03/2025	Formal change
06	04/03/2025	Formal change
07	19/12/2025	• Added ANNEX Cin order to provide traceability between Functions-Requirements-Hazards according to comments received by external review • Added improvement proposals in view of the evolutions of the solutions, in the next steps section 5.3 proposed by ERA.

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: 01/12/2022 Duration: 24 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
Gabriele Foreste	Hitachi	Task Leader Safety analysis and safety review for specific functions Chapters 3, 4.2, 4.3, 5.2
Angelo Viacava	SBB	Safety analysis and safety review for specific functions Chapters 2, 4.1, 5.1, 5.3, 5.4, 5.5, 5.6
Thidarat Panthong	DB	Safety analysis and safety review for specific functions Review of final document and Hazard Log contribution
David Fernandez	CAF	Safety analysis and safety review for specific functions Review of final document
Guy Larbat	Alstom	Safety analysis and safety review for specific functions Review of final document
Ammad Nadia	SNCF	Safety analysis and safety review for specific functions Review of final document
Markus Korb, Tomas Kertis	Siemens	Safety analysis and safety review for specific functions Review of final document

Sivertsen Terje	NRD	Safety analysis and safety review for specific functions Review of final document
Arana Sergio	CEIT	Safety Reviews of specific functions
Diego Garcia vaquero	ADIF	Safety Reviews of specific functions
Thomas Kayser	GTSD	Safety Reviews of specific functions
Thiyagarajan Saro	FT	Review final document

Disclaimer

EXECUTIVE SUMMARY

R2DATO has the challenging objective of improving the automation level for the railway system. Safety is a key element for any transportation system design. Unresolved safety concerns have been undefinedly postponing the widespread commercial application of fully automated cars. Safety gaps need to be prevented at an early stage, to avoid fatalities, avert development delays and ensure the credibility and applicability of R2DATO and ER-JU results. Safety thus needs to be built-in within the R2DATO design from the earliest stages.

Overview

This safety report identifies the needed safety requirements to ensure an adequate safety level for its scope. It also lists down known open points affecting safety. The safety results from this safety analysis need to be incorporated into the System Requiremen Specification (SRS). The integration of the identified safety requirements and the clarification of the open points need a time intensive discussion and cooperation between the safety experts from WP8.3 and the design experts tasked with updating the System Requiremen Specification (SRS). WP8.3 is not aware whether this integration task and the necessary resources have been already planned.

Scope, context, interfaces

This report is the main deliverable for the WP (Work Package) 8.3 within R2DATO. It specifically concerns the identification of safety requirements to control dangerous situations (i.e. hazards) caused by failures of three main modules of the Automated Train Operation (ATO). They are the Automated Driving Module (ADM), the Automated Processing Module (APM) and the Repository (REP). Other safety relevant R2DATO aspects are covered by the dedicated WP8.1 (Automating Functions), WP8.2 (the fourth module, i.e. perception) and WP8.4 (remote driving). This report is based on the System Requirements Specification (SRS) version 1.0.0. It extends and updates the hazard identification carried out by the X2R-4 project on the SRS version 0.3.0.

Safety analysis approach

Failures from the APM, ADM and REP functions can lead to dangerous situations (hazards), with the potential of causing catastrophic accidents, i.e. accidents with multiple fatalities. At the same time, the APM, ADM and REP functions are not a stand-alone technical solution. They are part of a complex railway environment, which includes built-in and consolidated safety solutions (safety barriers) to deal with specific hazards. For instance, automatic train protection (ATP) is an independent technical system which automatically and completely protects a train from overspeeding. As a result, the safety analysis takes into account not only the APM, ADM and REP modules, but also the overall railway system safety architecture. This allows to precisely quantify the safety responsibilities (SIL, Safety Integrity Level) for the APM, ADM and REP functions.

Main safety results

The first main result of this safety analysis is the identification and documentation of the applicable existing safety barriers within the railway system, which can partially or completely mitigate the effects of APM, ADM and REP failures. Such barriers were originally designed for fully manually operated trains; the safety analsis thus also evaluated and quantified their effectiveness in automated operation. The identified safety barriers are assumed to be fully independent on the APM, ADM and REP functions. The identified safety barriers are the preconditions to allow a safe automated operation. They have been listed in ANNEX D.

A second main result was the identification of the Safety Integrity Level (SIL) for the APM, ADM and REP functions. The SIL identifies how often a function can fail without compromising the overall railway safety level. The SIL also has a very significant impact on the development processes, time and costs. The SIL for the APM, ADM and REP functions is defined in ANNEX E.

Technical results: elements for a design update

A main design assumption in the System Requirement Specification (SRS) is that ADM functions are Basic Integrity, the lowest and less expensive Safety Integrity Level (SIL). This assumption is also needed to ensure backward compatibility with semiautomated driving modes (Grade of Automation 2). The safety analysis was not able to conclude that Basic Integrity is a suitable safety integrity level for ADM functions. ADM functions are a priority topic for the discussion between the safety and design experts and might require design modifications.

Known open points

A better clarification of some relevant operational processes is needed to improve the completeness and accuracy of the safety analysis. The safety analysis is based on the SRS; detailed information on operational processes (i.e. how the system is expected to be used) were out of scope for the SRS. Nevertheless, such operational information allows to evaluate the safety impact of some specific APM, ADM and REP failures. More detailed inputs (e.g. operational Use Cases) are needed for the following aspects:

- Coupling and decoupling processes
- Processes to handle emergencies and safety relevant communication to and from passengers, especially in case of fully automated operation

NOTE: The information concerning specific operational aspect (e.g. operational Use Cases) might have already been produced within R2DATO and a related safety analysis might be already planned (e.g. within WP8.1). If that is confirmed, it would greatly simplify the closure of this point.

Lessons learnt

X2R-4 carried out a safety analysis on the SRS 0.3.0, limited to the hazard identification and thus not covering the safety barriers and the SIL. Such analysis nevertheless already identified safety topics which are still relevant, for instance related to the ADM functions. The interaction between designers and safety experts in X2R-4 was minimal, limited mainly to the delivery of the hazard identification to the designers. As a result, only some of the identified safety topics were followed up and closed with the SRS update from 0.3.0 to 1.0.0. The lack of planned communication and interaction led to technical safety gaps which were already identified in the SRS 0.3.0 but are still currently unresoved in the SRS 1.0.0.

Next steps

WP8-3 performed each planned step of the safety analysis based on all the available input information. The safety analysis for the WP8.3 scope has therefore been completed. The next steps concern the following point:

- Closure of the known open points and the cooperation with design to explain, discuss and integrate the safety results into the design specification (SRS);
- Integrate in next phases in view of evolutions of solutions, the inputs coming from WP8.1, WP8.2, WP8.4, Harmonizing all the safety analysis that covers the entire Automation

Processes cluster, including technical enablers of Automating functions, Perception, ATO and remote driving;

- Improve the safety analysis in next phases in view of evolutions of solutions with safety relevant modification accoridng to existing TSI or add new safety relevant clauses to the TSI.

ABBREVIATIONS AND ACRONYMS

Acronym or abbreviation	Meaning
ADM	Automatic Driving Module
APM	Automatic Processing Module
ATO	Automatic Train Operation
ATP	Automatic Train Protection
GoA	Grade of Autonomation
MA	Movement Authority
R2DATO	Rail To Digital Automated Up To Autonomous Train Operation
REP	Repository
PER	Perception
SRAC	Safety Related Application Conditions
TFFR	Tolerable Functional Failure Rate
X2R-4	Shift to Rail 4
SIL	Safety Integrity Level

Table 1: Acronyms and abbreviations

TABLE OF CONTENTS

1 INTRODUCTION

This document is the Task 8.3 deliverable; it contains the safety analysis and risk assessment in the context of advanced signaling and automation system – Completion of activities for enhanced automation systems, train integrity, traffic management evolution and smart object controllers.

The Safety Analysis was based on functions allocated to APM, ADM and REP modules, which were developed within WP6.5 (Design and specification activities) based on the System requirement Specifications (SRS) from X2R-4. The objective of the safety analysis is to provide an input to the WP6.5 future design and architecture activities. Chapter 6 summarises the safety analysis conclusions which are relevant to WP6.5. Other main results of the safety analysis which are an input to the design and architecture activities by WP6.5 are:

- the list of hazards (i.e. dangerous situations) which can be caused by failures of the APM, ADM and REP functions. They are documented in ANNEX A
- the list of external safety barriers; they are the technical, organisational or operational measures which are outside of the ATO system and fully independent on ATO. They can reduce the probability that a hazard (dangerous situation) evolves into an accident (harm to persons and / or loss of human lives) or reduce the accident consequences. The identified technical, organisational and operational safety barriers are intended as requirements whih are expected to be fulfilled by systems outside ATO, i.e. as SRAC (safety related application conditions). They are documented in ANNEX D
- whenever necessary, the applicable safety requirements to control the hazards caused by failures of the APM, ADM and REP functions:
    - the applicable safety requirements from the Codes of Practice (e.g. TSI, standards, regulations, …)
    - the safety relevant APM, ADM and PER functions and their related quantitative safety requirements (TFFR and SIL). They are documented in ANNEX E

The main steps of the safety analysis have also been documented and explained in chapter 4. Although not directly relevant for the WP6.5, the outlined processes help understand how the safety results have been achieved. They are listed down as follows:

- Systematically analyse the safety impact of **functional failures** for the ADM, APM and REP functions
- Identify the effect and consequence of functional failures and the possible **hazards** caused by functional failures of ADM, APM and REP functions;
- Identify the **hazard severity**, based on the hazard consequences (accidents);
- Identify whether the hazard could be completely controlled by codes of pratice 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 TFFR** to the analysed functional failures; the initial TFFR is based on the unmitigated hazard severity;
- Detect external **safety barriers** which can mitigate the risk related to the hazard and thus the TFFR ;
- Calculate a **final TFFR** for each functional failure of the ADM, APM and REP functions; the final TFFR takes into account the mitigation provided by the external safety barriers

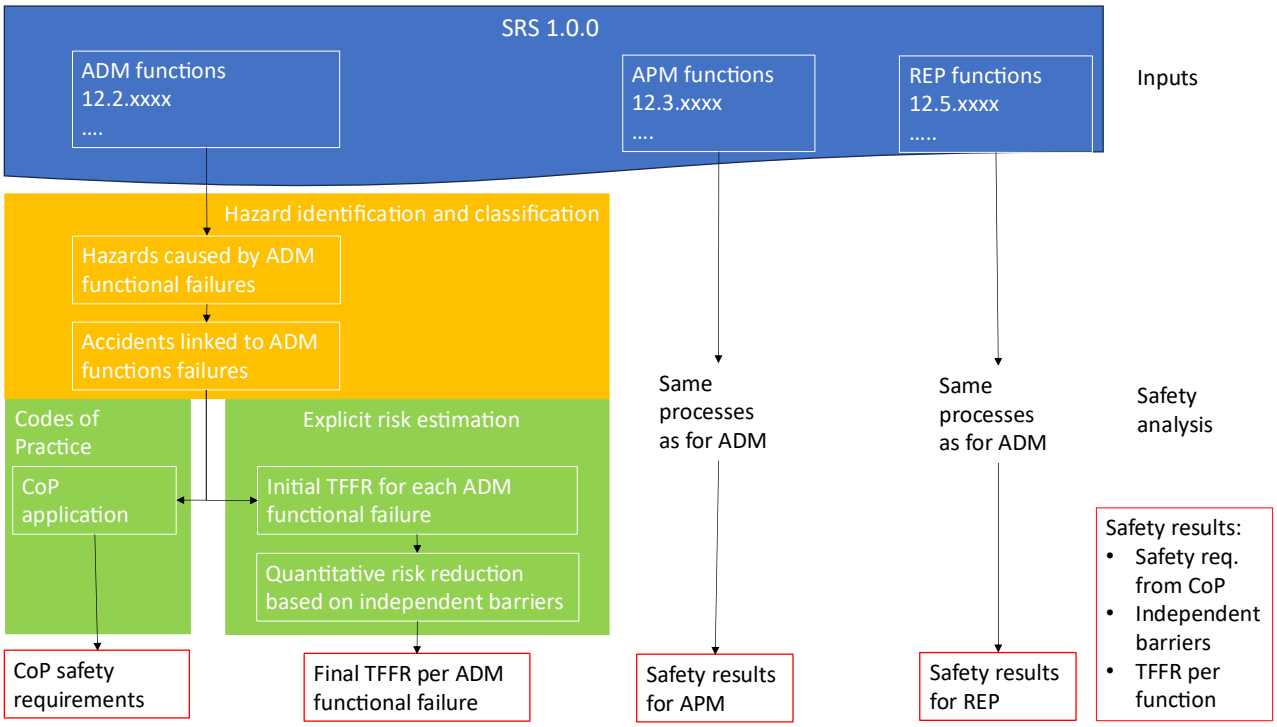

Figure 1: Safety analysis overview and results

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 below defines the operation principles for each GoA level.

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	Unattended train operation; all functions of train operation are automatic with no staff on-board to assume control in case of emergencies or degraded situations.

Table 2: Grades of Automation high level description

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

3 OBJECTIVE AND AIM

The aim of this document is to provide inputs to WP6.5 for the SRS update, based on a first evaluation of the safety risks caused by failures of the ADM, APM and REP functions in the context of ERTMS/ATO GoA3/4 (Driverless).

The safety evaluation is an input to the WP6.5 team to support modifications and updates to the architecture and design. The following safety results are the detailed safety inputs to WP6.5:

- the safety conclusions (see chapter 6)
- the list of external safety barriers, including the SRACs (see ANNEX D)
- the applicable safety requirements (see ANNEX D)
- the safety relevant APM, ADM and PER functions and their related quantitative safety requirements, i.e. TFFR and SIL (see ANNEX E).

The safety analysis inputs to WP6.5 and any review comments by WP6.5 are the basis for a discussion between the WP6.5 design team and the WP8 safety team. Modifications to the safety analysis and to the SRS are expected to arise, based on the discussion on the safety inputs to WP6.5.

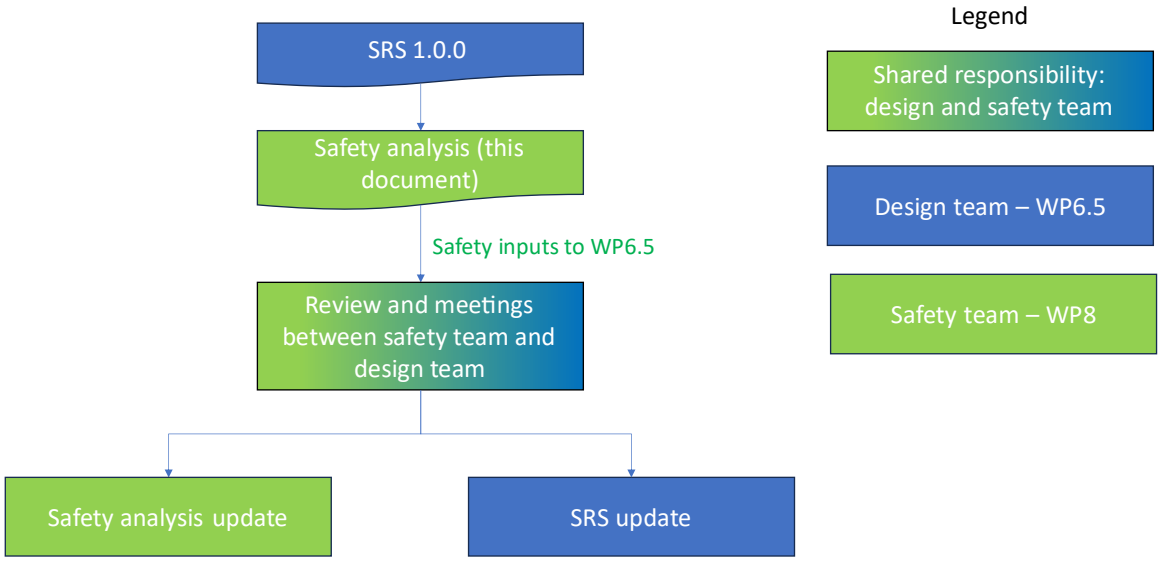

Figure 2: Objective of the safety analysis: inputs for the SRS update

The scope of the analysis is described In the following chapters, together with the deliverable description and the task description from the Grant Agreement.

3.1 SCOPE OF THE SAFETY ANALYSIS

The Safety analysis covers all the functions of APM, ADM and REP modules and is based on the technical description within the SRS by WP6.5, version 1.0.0 [17] The safety analysis only identifies hazards that arise from the failure of the function under consideration. This safety analysis presents the hazard identification, mitigations, risk evaluation, and the final Tolerable Functional Failure Rates (TFFR) per function after the mitigations have been applied.

3.2 DELIVERABLE DESCRIPTION

	Deliverable description from Grant Agreement	Output of deliverable
Deliverable 8.3	• Hazard identification and Risk assessment file: reports the entire safety analysis with a Safety classification of each function with consequent risk reduction and final safety classification • Functions classification: it is an extract of Hazard identification and Risk assessment file, for every functions has been reported the Hazards, Safety barriers applied and final safety classification.	• The Hazard identification and Risk assessment has been described in ANNEX B • The Functions classification has been described in ANNEX E

Table 3: List of Task8.3 deliverables

3.3 TASK DESCRIPTION

	Task definition from Grant Agreement (Task 8.3)	Output of deliverable
Task 8.3	Complete the safety analysis in conformity with RAC (Risk Acceptance Criteria) guideline by ERA and CENELEC 50126 standard	The prerequisites of Hazard identification and risk assessment analysis, consist of the functions provided by specification delivered by WP6.5 reported in the document [1] , in details, is reported an architecture where are diagrammed all modules (involved in the analysis of Task8.3) and for any modules are listed all functions that explain the behavior of any modules, furthermore the complete safety analysis has been

	Task definition from Grant Agreement (Task 8.3)	Output of deliverable
		completed based on hazard identification provided by X2Rail4 project. Following the satisfaction of the above mentioned prerequisites, the output of Task8.3 consists in releasing a safety analysis based on the functions (described in the technical specification) where Hazards, Barriers and final safety classification are identified for each function

Table 4: Task description

4 SAFETY ANALYSIS

The Safety analysis is aimed at identifying the final TFFR of APM, ADM and REP functions. The safety analysis has been carried out in two stages:

1. The hazard identification and classification by X2R-4 has been reviewed and expanded to include the modifications from the SRS 0.3.0 to the SRS 1.0.0
2. The risk analysis, not covered by X2R-4, has been carried out. Codes of practice and external safety barriers have been identified and evaluated. They are measures to mitigate the consequences or probability of accidents caused by ADM, APM and REP failures. Quantitative safety requirements (final TFFR) for APM, ADM and REP functions have been identified, in case the codes of practice and the external safety barriers could not reduce the risk to a tolerable level.

The workflow details are reported in Figure 3: Safety Workflow:

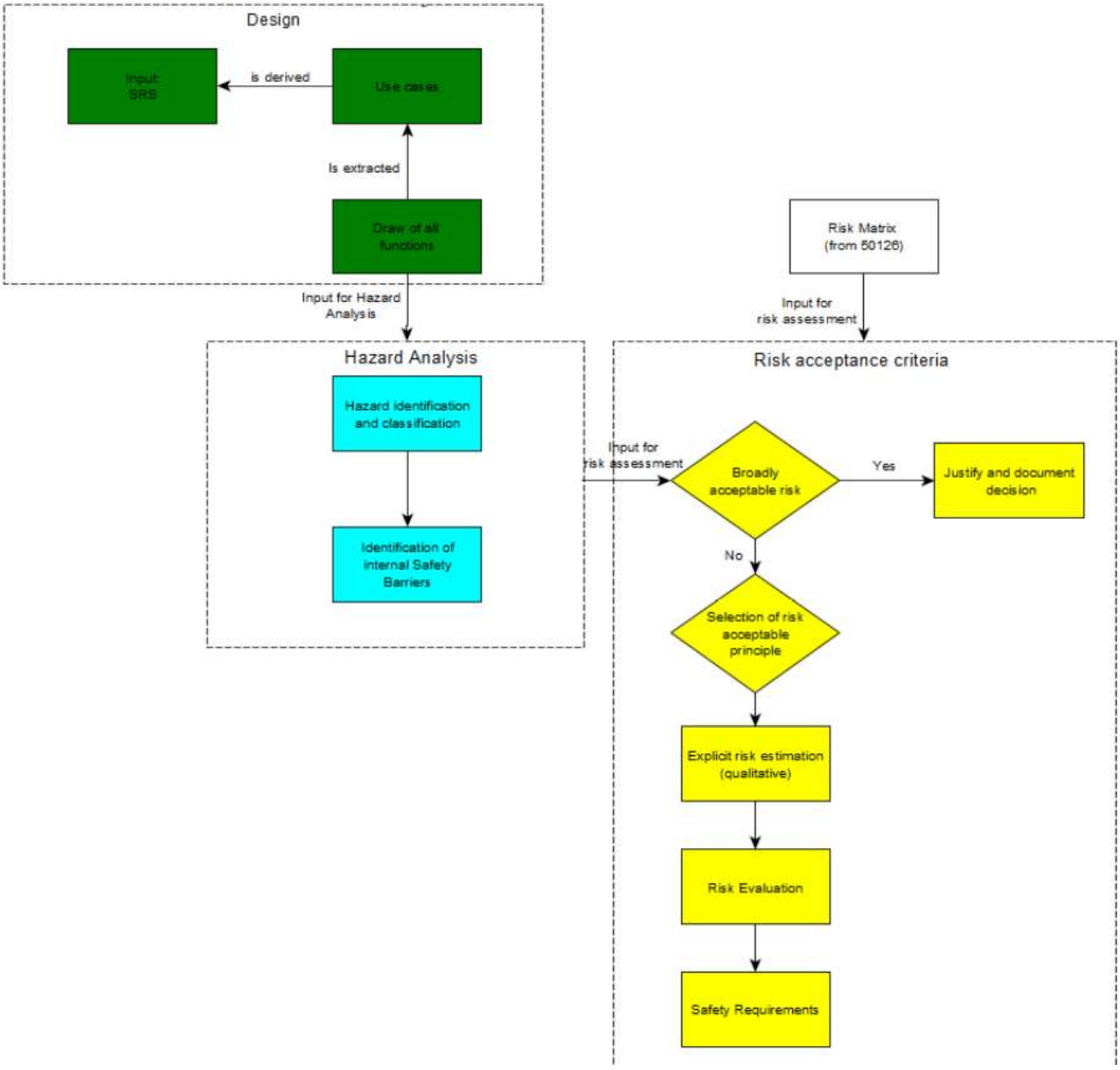

Figure 3: Safety Workflow

This figure shows all the steps performed in the safety analysis (for Phase 3 and Phase 4)

4.1 LIMITS AND ASSUMPTIONS

4.1.1 Limits and interfaces of the safety analysis

This safety analysis covers only the functional failures of the ADM, APM and REP, as defined in the SRS logical component (SRS chapter 12) functions and in the context of the SRS technical Use Cases (SRS chapter 13). The identified hazards and mitigation measures contained within this analysis are thus derived bottom-up, through a systematic evaluation of the effects of ADM, APM and REP failures. This approach ensures the evaluation and mitigation of the risks caused by any failures of the outputs from APM, ADM and REP.

A top-down approach was not in scope of WP8.3, as the overall system level ATO functions and the operational Use Cases[1] were not an input to WP8.3. A top-down approach based on system level ATO functions and operational Use Case ensures that the hazards arising from the operation are systematically analysed and mitigated.

The bottom-up and the top-down approach are complementary to ensure a complete safety analysis at a R2DATO level. The top-down approach is able to identify hazards which are linked to operational aspects not covered by the SRS or which are not linked to any of the logical functions (and thus cannot be identify by analysing only the logical functions failure). As a result, the results from WP8.3 need to be integrated and harmonized with the safety results from the other R2DATO safety analyses in the WP8.1, WP8.2 and WP8.4.

The following sections contain examples of what is explicitly excluded from this WP8.3 safety analysis.

4.1.1.1 No systematic top-down hazards identification

This safety analysis is based only on the logical functions from the SRS. This safety analysis needs to be integrated with a top down safety analysis based on the ATO system level functions and operational use cases. WP8.3 assumes that the top-down safety analysis concerning Automating Functions is going to be performed by WP8.1.

4.1.1.2 No PER (perception) hazards

This safety analysis does not cover the perception system (PER). The PER safety analysis is planned to be performed by WP8.2. The results of the WP8.3 safety analysis are expected to be strictly related to the results of the PER safety analysis:

[1] the SRS does contain technical Use Cases. They explain how the logical system works, as a sequence of different logical functions, including inputs and outputs between such functions. They specify a logical design and architecture, as a precondition to develop a technical solution, with a point of view closer to the manufacturer. Operational Use Cases, on the contrary, explain the operational context, as well the expected operational steps and outcomes. They specify the operational objective that the technical solution needs to achieve, with a point of view closer to the railway operator. The difference is clearer if the technical Use Case from the SRS are compared with the Operational Use Cases, provided e.g. as an input to WP8.2 for the PER system.

- PER is aimed at gathering relevant data from the environment to allow a driverless operation.
- outputs from PER are then processed by APM, which defines the adequate reactions to the environmental situations and hazards.

An ATO safety function might thus include the detection by PER and the reaction by APM: from a safety perspective, PER and APM cannot be easily functionally split. As a conclusion, the results of this safety analysis need to be cross checked and harmonized with the results from the PER safety analysis.

4.1.1.3 No remote driving hazards

This safety analysis does not cover functions and hazards related to remote driving. The safety analysis covering the remote driving is planned to be performed by WP8.4.

4.1.1.4 No final safety results for the overall R2DATO scope

The overall safety results for the whole R2DATO scope require a harmonization and consolidation of the results produced by the WP8.1, WP8.2, WP8.3 and WP8.4 safety analysis. This consolidation and harmonization task is outside the scope of WP8.3. It is unknown to WP8.3 whether this task has been already planned.

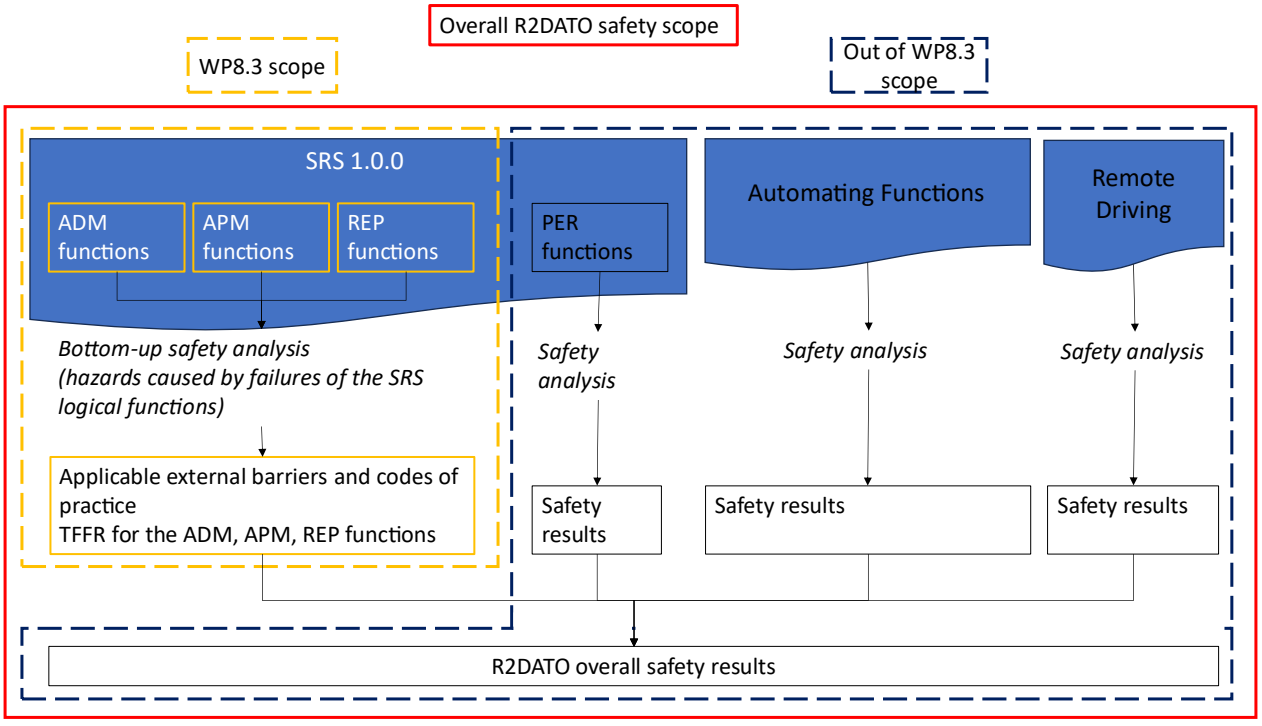

Figure 4: Safety analysis limits and interfaces within R2DATO

4.1.2 Assumptions

The following table collects assumptions applied during the safety analysis.

ID	Title and text	Comment
General_ETCS_FS_OS	**Operation only under ETCS FS or OS** GoA3 and GoA4 operation is allowed only under ETCS Full Supervision (FS) or On Sight (OS).	
Siemens_Assumption_01	***Daily test on the horns and signals is needed.*** It is typically required to perform daily test on horns, to monitor their random failures. Such test may be don by sensors for each usage of horns of manually by operator's staff..	
Siemens_Assumption_02	***TCMS function „Horn status/Horn Defect" shall have the safety relevance with TFFR < 1e-06*** The horn status is used by APM to have an acknowledge on the horn actiavation. The activation is safety relevant so monitoring and appropriate reaction is needed. This may be used also as automatic monitoring to reject daily tests (Siemens_Assumption_01)	
Siemens_Assumption_03	***Input signal by perception (mic.) on usage of horns, then the TFFR of horn status from TCMS may be lower.*** This barrier may replace the daily test on the horns "Siemens_SafBar_01" If appropriate safety reaction is introduced (another functions like braking, head lights, track side communication devices, etc.) the safety relevance on the "horn status" may be rejected. This may be used also as automatic monitoring to reject daily tests (Siemens_Assumption_01).	
Siemens_Assumption_04	***TCMS*** TCMS shall use another signals to open door independently, i.e. speed sensor, signal from ATO, passenger press button (depends on mode)" i.e. also Code of Practice, TSI req.	
Acquire_train_data_01	**ADM function "Acquire train data"** The outputs of the ADM function "Acquire train and ADM data" are only used by other ADM functions. They are not used, directly or indirectly, by any other safety relevant function.	

4.2 SYSTEM DEFINITION

This chapter is an extract from the SRS, section 6.1. It describes the input information used for the hazard identification, risk assessment and requirement derivation. The inputs include the operational Use Cases descriptions in §4.2.2 and Functions definition in §4.2.3.

4.2.1 Logical architecture

The target system is an interoperable ATO over ETCS system covering the different grades of automation, The current document is for GoA3/4, an evolution for the future autonomous trains based on the GoA2 functions specified for TSI 2022 and the new functions required for GoA3/4,
The figure TBD shows a larger scope with the logical architecture of a complete railway system where the GoA3/4 logical components required for operation are highlighted in yellow. The railway system actors are represented in light blue, they are external to the logical system and will be described in chapter 9 with their associated functions or responsibilities.
The railway system logical architecture is made of logical components with logical interfaces (FIS level). Each logical component involved in Safety analysis will be described in sections §4.2.1.1, §4.2.1.2 and §4.2.1.3 with its allocated functions.
The upper part of the diagram is dedicated to the trackside logical components which are highlighted in cyan (Train Control, Route Control, Incident Solving Manager, Traffic Management, Train Management, Digital Map, Operational Execution, Mission Data, Train Data).
The lower part of the diagram is dedicated to onboard logical components which are highlighted in yellow for the GoA3/4 components (Repository, Automatic Processing Module, Perception, Automatic Driving Module) and dark blue for the other components (Train Protection, Signal Converter, Localization, Onboard Recording Device).
The communication channels between onboard and trackside components are SS-026 for ETCS, C48 for RU (Train Control and Monitoring System/Train Management), C34 for infrastructure data (Repository/Digital Map), C14 for Journey Profile (Repository/Operational Execution), C1 for Mission Profile (Repository/Mission Data), C24 for train information (Repository/Train Data) and C19 for reporting incidents (Repository/Incident Solving Manager).
The logical components identified in the logical architecture permit interchangeability or interoperability. They must be allocated to physical components in a physical architecture with interfaces defined at FFFIS level (see chapter 15).
This specification will focus on GoA3/4 components and their interfaces:
- Automatic Driving Module is the evolution of GoA2 onboard component
- Repository manages the communication with trackside and stores relevant information
- Automatic Processing Module substitutes driver and train attendant responsibilities for reacting in case of incident.

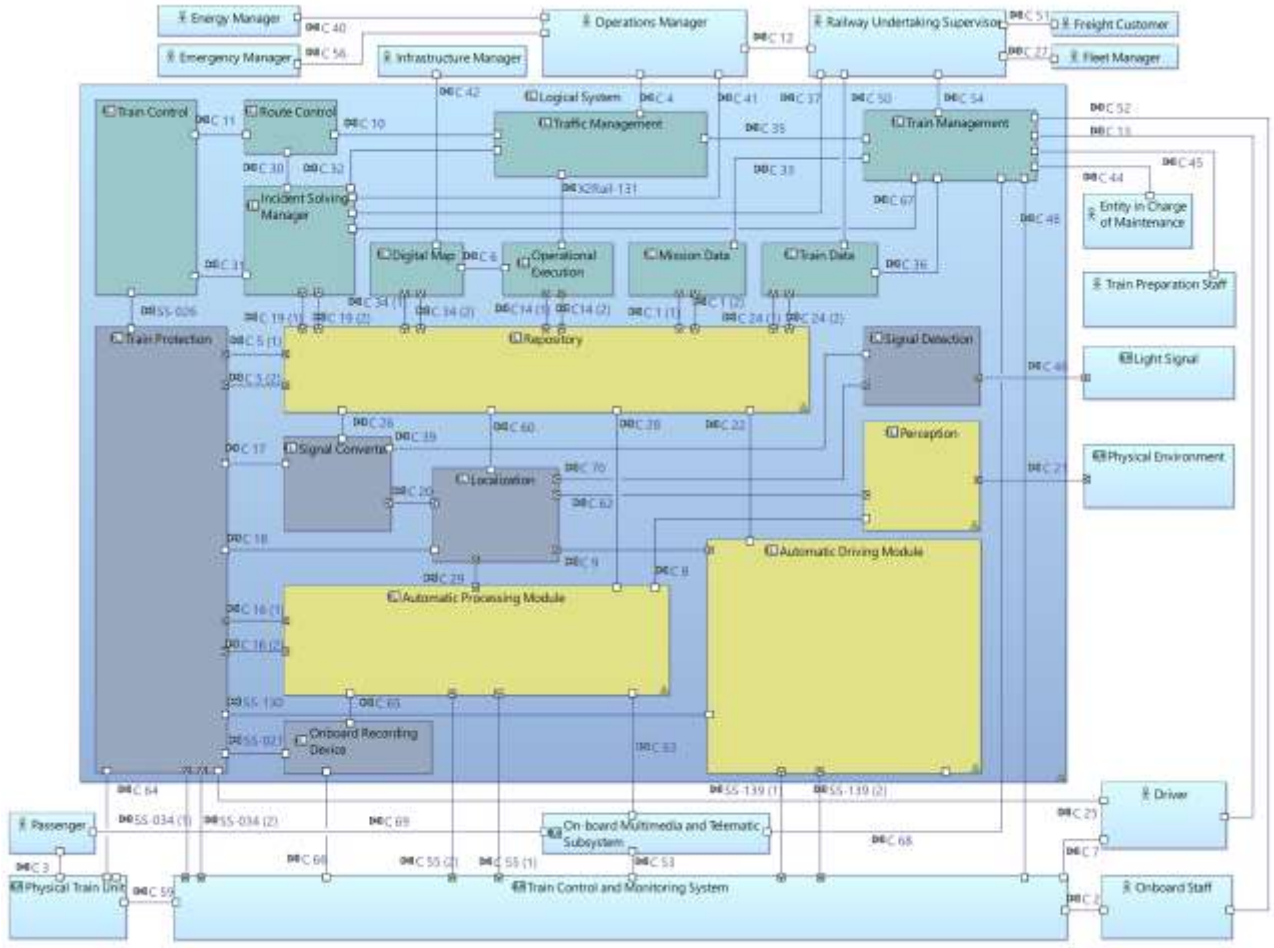

Figure 5: Logical Architecture

For the scope of WP8.3, only the ADM, APM and REP modules will be analysed from a safety point of view, in the sections below are reported a description of logical components involved:

4.2.1.1 Automatic Driving Module (ADM)

This paragraph is an extract from §10.2 of the SRS 1.0.0.

The Automatic Driving Module (ADM) component is in the train and drives a train automatically. Application: GoA2, GoA3, GoA4. Rationale: re-use of SS-125 ATO-OB core functions. Interoperable/interchangeable module active in all GoA levels.

Allocated functions:

- Acquire train and ADM data
- Control initial traction effort
- Stop exactly at the intended location
- Supervise service brake efficiency during operation
- Respect JP Timing Points and Optimize the consumption
- Determine maximum authorised speed
- Check departure conditions
- Regulate traction and braking effort

- Request holding brake
- Determine ADM state
- Compute Operational Speed and Acceleration
- Manage low adhesion
- Start door opening or closing sequence
- Detect that final stopping point has been reached

4.2.1.2 Automatic Processing Module (APM)

This paragraph is an extract from §10.3 of the SRS 1.0.0

The Automatic Processing Module (APM) component is in the train and should substitute driver and train attendant responsibilities for reacting in case of incident. It manages mission execution, safe reflexive reactions, evaluated reactions and safety procedures in cooperation with ISM. Application: GoA2, GoA3, GoA4. Rationale: new module emulating the driver in GoA3/4. Interoperable/interchangeable module active in all GoA levels (GoA2 will be selected by default if there is no Mission Profile).

Allocated functions:

- Determine running direction
- Command and supervise horn
- Deactivate Driver Activity Control
- Emulate action from driver
- Manage supervision orders
- Start coupling
- Start splitting
- Define if consist is master or slave
- Determine APM state
- Manage mission execution
- Monitor system status
- Check departure conditions except signalling
- Define evaluated reaction depending on incident
- Define reflexive reaction depending on incident
- Monitor OMTS status
- Monitor incidents affecting passengers
- Monitor Passenger Alarm
- Monitor doors and platform gap incidents
- Monitor fire alarm
- Monitor shunting circuit compensator defect
- Monitor other train unit failures
- Inhibit sanding

4.2.1.3 Repository (REP)

This paragraph is an extract from §10.5 of the SRS 1.0.0

The Repository (REP) component is in the train and communicates with trackside to acquire JP and infrastructure data from IM or MP and train information from RU. In addition, it collects and reports incidents to trackside. The C19 channel is used for receiving European Instructions or information to OMTS. The REP communication principles are specified in chapter 15. Application: GoA2, GoA3, GoA4. Rationale: new module dedicated to communication and sharing of information with all on-board modules including safety related data received from DM. Interoperable/interchangeable module active in all GoA levels and interfacing with OE in GoA2 and with DM, OE, MD, TD and ISM in GoA3/4. For keeping compatibility with GoA2, REP has 2 modes for communication with trackside: one working with SS-126 structure for GoA2 trackside and one working with SP static data (C34 with DM) and JP/SP dynamic data (C14 with OE) for GoA3/4 trackside.

Allocated Functions:

- Manage reporting
- Acquire train parameters
- Acquire JP
- Acquire Segment Profile information
- Map REP with route
- Determine REP state
- Acquire MP
- Acquire instructions
- Acquire OMTS information

4.2.2 Use Cases descriptions

This paragraph is an extract from §13 of the SRS 1.0.0.

The Use cases are based on the operational context of Goa3/4, They focus on the user needs related to unattended train operation and to the transitions with the other operational contexts, The Use Cases are expressed in the form of sequence diagrams showing the various interactions between the actors and the main logical components, each one being represented by a timeline. Each timeline describes the functions and exchanges involved in these interactions. The timeline includes also the mode associated to the logical component or the state associated to the actor when the scenario leads to a change of mode or state (door opened or closed for example), The sequence diagrams use specific symbols and constructions for modelling. Actors are represented with light blue boxes, logical components with dark blue boxes, functions with green boxes, modes with grey bubbles and data flows with arrows. Constructions permit to introduce conditions (ALT), iterations (LOOP), parallelism (PAR), options (OPT) and references to other UCs (REF) see Figure 6.

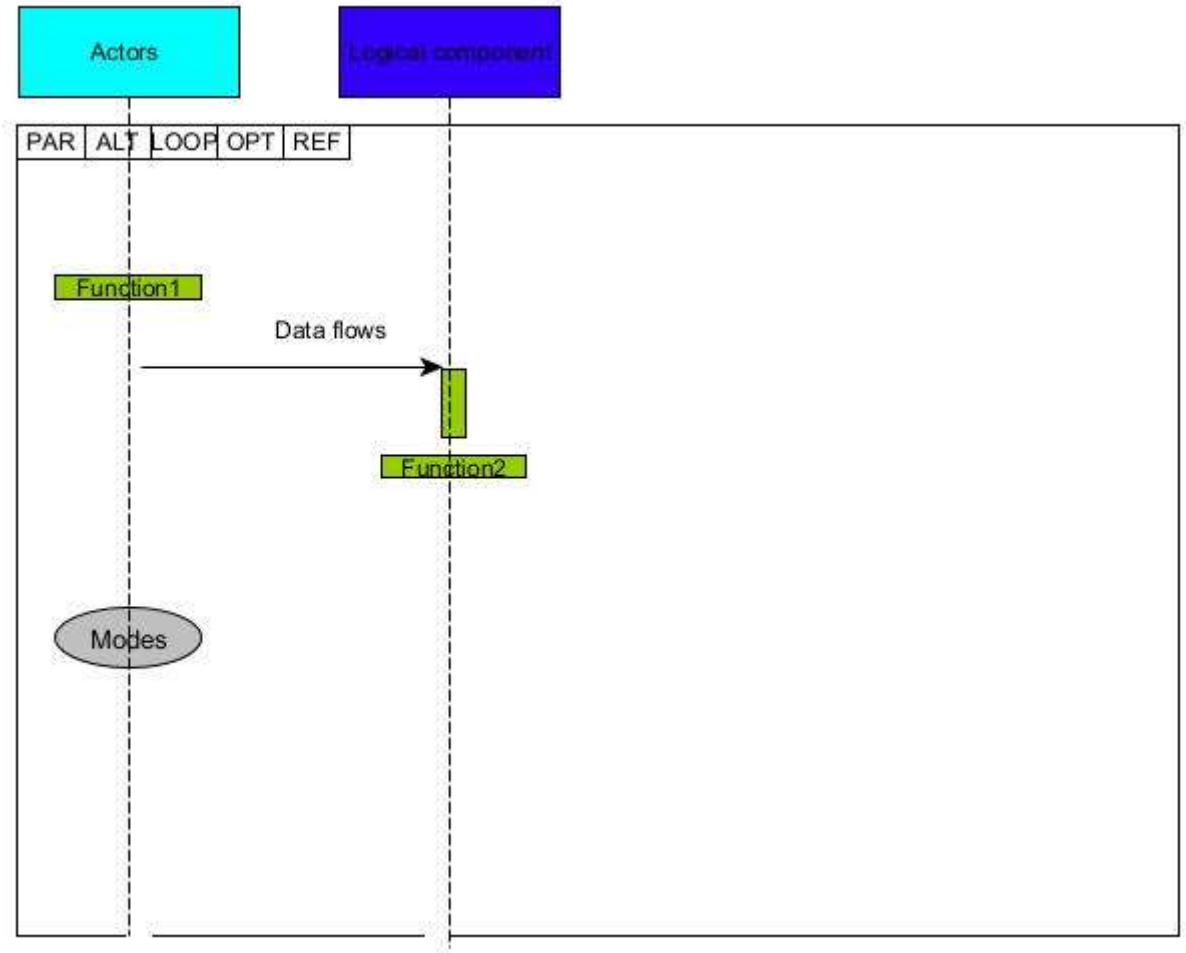

Figure 6: Use Case diagram

Note: For more details check some use cases examples see the §13.2 of [1] document.

The sequence diagrams are informative only, in fact they permit to make the link with the functions, but they do not reflect all possible combinations existing in a test scenario where specific values of variables are set. For the scope of Safety analysis as in §3.1, the use cases provide an operational description about functions allocated to the logical components (see 4.2.1.1, 4.2.1.2. 4.2.1.3) interface with other functions belonging to other logical components. This information is very useful in order check the overview of how the functions are implemented in the operational context providing a complete view of the function's usage across the entire system, in this way is It is easier to understand the propagation of an error from one function to another one.

4.2.3 Functions descriptions

This paragraph is an extract from §12 of the SRS 1.0.0.

The logical component functions are associated to a logical component of the logical architecture see Figure 5: Logical Architecture, The logical functions are elementary and provide a technical description of the behaviour of the logical component with respect to a specific task, furthermore each function is described with its associated inputs and outputs.

4.3 HAZARD IDENTIFICATION

This chapter:

- illustrates the safety methodology for the hazard identification.
- illustrates how the hazard identification is documented in the hazard log.

4.3.1 Hazard identification inputs

The hazard identification is based on the systematic analysis of each logical function belonging to ADM, APM and REP, as described in the SRS version 1.0.0 (see sections 4.2.1.1, 4.2.1.2 and 4.2.1.3).

The technical Use Cases in the SRS version 1.0.0 have been taken into account during the hazard identification. The technical Use Cases define the logical and functional interfaces between the ADM. APM and REP functions and the other relevant railway systems and actors. As a result, the Use Cases have been used to provide the relevant technical context for the safety analysis, including supporting the impact evaluation at a vehicle level and at the railway system level of the functional failures by ADM, APM and REP.

4.3.1.1 Technical literature

The following standards and regulations have been taken into account to support the hazard identification and the identification of the external safety barriers:

- TSI LOC & PAS;
- TSI SRT;
- TSI OPE;
- EN14752;
- EN45545.

4.3.2 Hazard identification process

The hazard identification within R2DATO is built upon the analogous hazard identification performed by X2R-4. As the X2R-4 hazard identification had been performed on the SRS version 0.3.0, while the R2DATO input document is the updated SRS version 1.0.0, the R2DATO hazard identification checked, updated and extended the X2R-4 hazard identification.

The hazard identification is based on the logical functions defined within the SRS. As a result, the hazard identification carried out is a functional, bottom-up hazard identification. More details on the boundaries of the safety analysis can be found in section 4.1.

Each function output of each APM, ADM and REP logical function has been analysed. For each function output, different failures modes were considered, namely commission, omission, early, late, incorrect. For the scope of this analysis, the above listed failure modes also cover the failure mode too much and too little. Intentional sabotage, including cybersecurity threats and attacks, is not in the scope of this hazard identification and has not been explicitly covered. The failure mode list, with a short explanation on the meaning of each failure mode, can be found in ANNEX F.

The impact of each considered failure mode was defined, at three levels:

- initial effect, i.e. the failure impact on the function itself
- intermediate effect, i.e. the failure impact on the ADM, APM or REP component
- final effect, i.e. the failure impact at a vehicle and railway system level

Hazards have been formulated as the conditions and situations which could lead to an accident, in line with the hazard definition from CSM-RA 402/2013.

The results of the hazard identification process have been documented within the hazard log, as shown by the following figure.

Figure 7: Hazard log cells dealing with the hazard identification

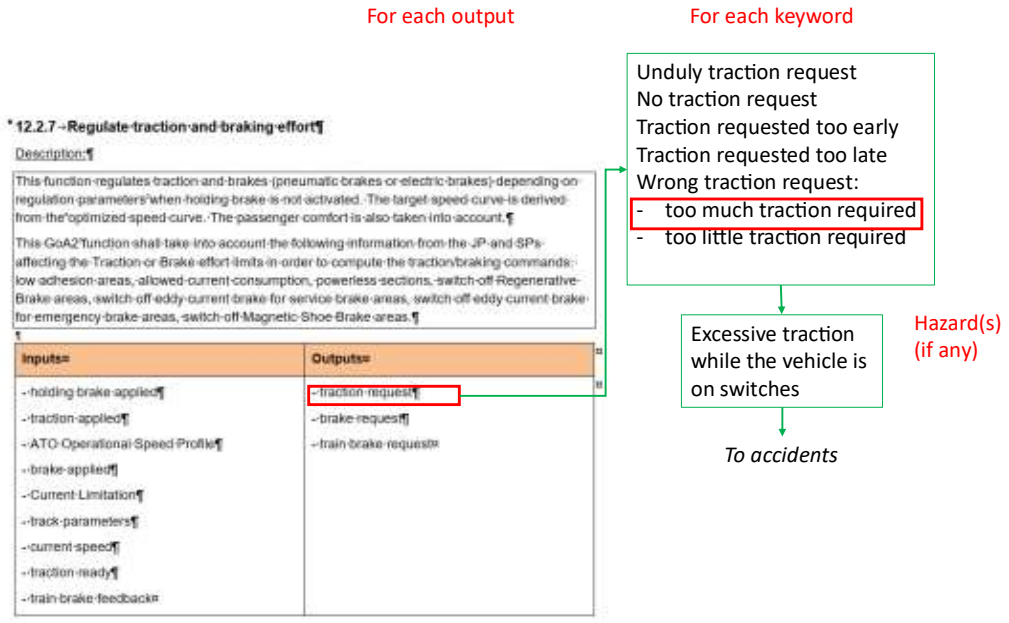

Figure 8: Hazard identification: application example for the function “regulate traction and braking effort”, output “traction request”, keyword “wrong (too much)”

4.3.3 Hazard classification process

Each hazard can cause one or more kind of accidents (e.g. collision).A list of high-level accident categories has been created and hazards have been linked to the corresponding accident category. Each accident category is linked with its potential consequences in terms of fatalities and

weighted injuries. For instance, accidents of the category “collisions” or “derailment” and which involve passenger trains are classified as “catastrophic” accidents. As a result, the hazard classification is based on the severity of the accident category which the hazard could cause (see also Table 5).

The results of the hazard identification process have been documented within the hazard log, as shown by the following figure. When needed, additional explanations on the failure chain (i.e., how a functional failure could lead to an accident) are also included in the hazard log.

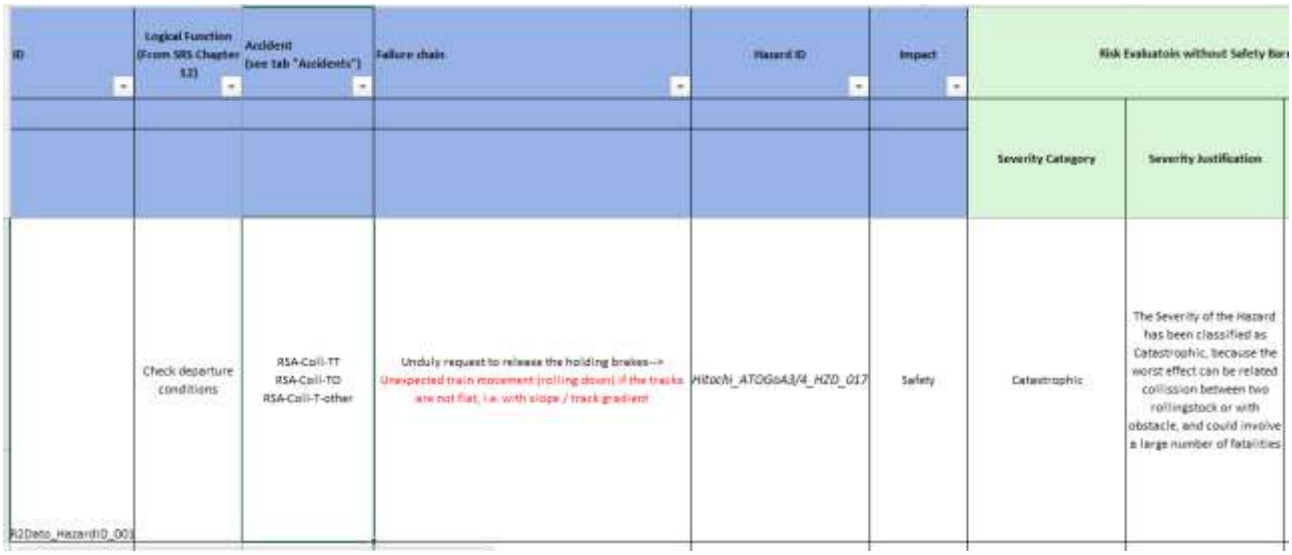

Figure 9: Hazard log cells dealing with the hazard classification

4.3.3.1 Hazard severity

Hazards are described and classified according to the severity classification of the potentially associated accidents.

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

Table 5 Severity classification

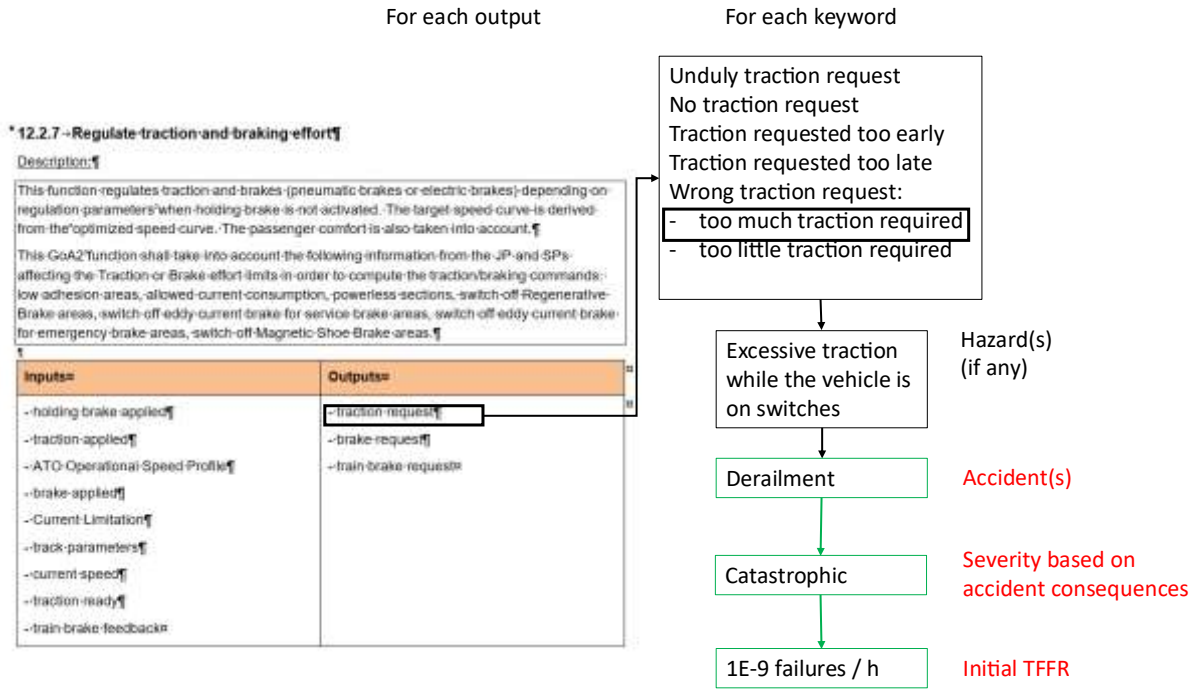

Figure 10: Hazard classification: application example for the accident category "derailment"

4.3.4 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.

4.4 Risk Acceptance Principles

The risk acceptance principles have been selected in accordance with the CSM-RA:

- 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 Codes of Practice

Whenever possible, codes of practice have been applied to manage the related applicable hazards.

The following codes of practice were deemed applicable to manage specific hazards in the GoA3 and GoA4 context:

Code of practice	Specific function	Managed hazard
Set of specifications 3 (ETCS B3 R2 GSM-R B1)	• *MA supervision* • *Speed monitoring*	• Violation of the MA • Overspeed
"Sanding device" (SAM S 901)	SRS function: Inhibit sanding	Excessive sanding
SNCF_SafBar_03 Code of practice "Passenger access system" (SAM C 305).	SRS function: Emulate action from driver	Hazards related to the function *Emulate action from driver*- see Hazard List ANNEX B.

Table 6 Applied codes of practice

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

4.5.1 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.

4.5.2 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 in case of functional failures of the APM, ADM and REP functions.

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)[2]. 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

[2] This statement is valid under the precondition that the input data for the ETCS / ATP have been entered correctly

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.

4.6 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 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 context[3]. As a result, no hazard has been managed through the similar reference system principle.

4.7 EXPLICIT RISK ESTIMATION

The explicit risk estimation principle has been applied when the codes of practice could not completely control a hazard caused by a functional failure of an APM, ADM or REP function. In that case, a quantitative analysis has been carried out. When necessary, a quantitative target (TFFR) for the logical APM, ADM or REP function 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 G.

4.7.1 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 APM, ADM and REP 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 TFFR (Tolerable Functional Failure Rate), i.e. the maximum tolerable number of technical failures per hour.

Severity category	Consequences to persons	Initial TFFR from CSM-RA [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

Table 7 Harmonised design criteria from CSM-RA

[3]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 taken into account to inspire the R2DATO safety analysis.

The harmonised design criteria have been taken as initial TFFR for the APM, ADM and REP 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:

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

Table 8 Design criteria, extension to marginal and insignificant severity

4.7.2 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 APM, ADM and REP functional failures
- The final TFFR for the APM, ADM, REP functions

4.7.2.1 External safety barriers and impact on TFFR

The starting point for the explicit risk estimation process is the initial TFFR. The initial TFFR is associated to an APM, ADM or REP function, whose failure has a credible direct potential for catastrophic and critical consequences.

Not every APM, ADM or REP failure has a credible direct potential for catastrophic and critical consequences. External barriers can reduce the frequency of occurrence of a hazard or mitigate the severity of the potential consequence of that hazard.

The following external barriers type have been identified:

- Technical barriers: safety functions by external systems (e.g. ETCS system, ATP or TCMS), which can independently mitigate the risk caused by an APM, ADM or REP 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 APM, ADM and REP, are applicable to a hazard or to an accident, then the initial TFFR can be improved[4]. A final TFFR is thus calculated, taking into account the risk reduction provided by the external barriers.

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

4.7.2.2 Final TFFR and SIL

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

Final TFFR [Failures / h]	SIL
1E-9 ≤ TFFR < 1E-8	4
1E-8 ≤ TFFR < 1E-7	3
1E-7 ≤ TFFR < 1E-6	2
1E-6 ≤ TFFR < 1E-5	1
TFFR ≥ 1E-5	Basic Integrity

Table 9: SIL and TFFR

4.8 Review of the Safety Analysis

The safety analysis has been cross-reviewed at first by a designated peer within WP8.3; when necessary, safety topics have been discussed within the WP8.3 group during designated meetings and workshops.

5 KNOWN OPEN POINTS AND NEXT STEPS

The safety analysis has been performed and documented as an input to the ATO architecture and design; modifications to the ATO architecture and design are expected.

5.1 Needed Design Modifications

Some specific topics require a cooperation between architect and design experts and safety experts. In case of modifications to the SRS, several solutions at a design and architecture level can achieve the necessary safety level for the APM, ADM and REP functions. The target of the cooperation between the architects, design and safety experts is to identify the best option to ensure a technically feasible, economically viable architecture and design for the ADM, APM and REP modules, without compromising on the necessary safety level.

[4] Improved = increased. A higher TFFR means that it is tolerable that the related function fails more often.

The most relevant safety challenge concerns ADM, as:

- On one side, ADM needs to include Basic Integrity functions only, even in GoA3/4, to ensure backward compatibility with GoA2
- On the other side, the safety analysis based on the SRS 1.0.0 identified the need for some ADM function to be SILx

As a result, modifications to the SRS are needed. To keep ADM functions within Basic Integrity it is necessary to implement one or more of the following actions:

- Clarify existing safety barriers which have not been documented yet, if any
- Add additional independent safety barriers (e.g. at a vehicle level)
- Add a supervision of some hazardous ADM outputs by the safety relevant APM

Related proposals have been drafted by the safety team. Such proposals are simply a starting point for the design and architecture modifications and are aimed at starting a cooperation with the architects and design experts. Architects and design experts are expected to check the hazard identification and its assumptions together with the safety experts; it is expected that better design alternatives could be elaborated by the architects and design experts. It is strongly suggested to allocate time and resources to this prioritized topic and to create a dedicated task force composed of architects, design experts and safety experts.

5.2 Clarification on specific Operational Processes

The SRS contains a vast and well structured amount of information, which enabled the functional safety analysis for the vast majority of the functions. Some specific logical functions nevertheless require a deeper level of detail concerning the operational context in which they are used. For instance, the hazards related to the coupling and decoupling functions can be properly identified only if the coupling and decoupling operational process are clarified. Such operational details are out of scope for the SRS and are thus expected to be included in the relevant operational Use Cases. The following topics are expected to be covered by the operational hazard analysis:

- Coupling and decoupling processes;
- Emergency processes, including evacuation procedures, communication with and from passengers (e.g. monitoring passenger alarm);
- Specific reaction to dangerous situation by APM;
- Driving Rules.

5.3 Next Steps

According to the final results of WP8.3, based on the WP6.5 deliverable with version 1.0.0 [1], The next steps concern the closure of the known open points and the cooperation with design to explain, discuss and integrate the safety results into the design specification (SRS). In particular all Safety Barriers reported in ANNEX D, shall be validate by Design team as safety requirements in order to confirm the feasibility of implementation and integrate the requirements in the next SRS version, in case of the requirements are already covered by other System requirements or SW requirements, it

is needed only a feedback for the acceptance of requirements. Furthermore, when the subsequent versions of the SRS will be released, the safety team will perform an impact analysis to understand the changes compared to the previous version and integrate any changes that may have an impact on safety (i.e. addition of new functions, modification of existing functions, etc.).

Furthermore, as next steps, we could consider, a list of all the improvements that can be considered for next phases in view of evolutions of solutions of safety analysis of WP8.3, that can be made to this document is reported below:

1) D8.3 clause 4.1.1

List of actions for next phases in view of evolutions of solutions about the railway system view and functions and integration aspects. Aim: provide a systematic top-down view over the ATO GoA3/4 safety analysis results, by harmonizing and integrating the outputs from WP8.1, 8.2, 8.3 and 8.4

- List of actions:
  - Compare and integrate hazards from the WP, using the WP8.1 standardized hazard list as a top-down starting list
  - Compare and integrate assumptions, safety requirements, SRAC (safety related application conditions) and TFFR / SIL (safety integrity level)
- Deliverables:
  - Consolidated hazard log
  - Automation processes cluster hazard report

2) D8.3 clause 4.3.1.1

List of actions for next phases in view of evolutions of solutions, about the railway system view and functions and integration aspects. To consider Clause by clause in the future actions (to add this open point).

Aim: safety impact analysis on TSI: which TSI are affected, how, what are the proposed modifications to the existing text, which new safety requirements are needed

- List of actions:
  - Clause by clause for each TSI and each existing TSI requirement:
    - Evaluate safety relevant modification needed to enable or support GoA3/GoA4
    - If there are no relevant modification needed (as in the point above) it is necessary to evaluate whether the requirement is relevant as an external safety barrier (i.e. we need the existing TSI requirement as a prerequisite for GoA3/4, but we won't modify it)
  - New safety relevant clauses for each TSI
    - Add new safety relevant clauses to the TSIs
- Deliverables:
  - Clause by clause safety impact analysis of GoA3/4 on each TSI

- TSI safety impact report (summary and overview)

6 CONCLUSIONS

The objective of WP8.3 is to carry out the safety analysis for the ATO functions (related to ADM,APM and REP modules) described by the SRS [1], the main results of safety analysis are related Safety barriers and Final TFFR calculated for each APM,ADM and REP functions. The safety analysis identified different kinds of external safety barriers (independent on APM,ADM and REP):

- Already existing safety barriers;
- New proposed safety barriers, to mitigate hazards related to GoA3/4 operation.

The identified external safety barriers have been considered as mitigation factors to identify the tolerable function failure (TFFR) for ADM,APM and REP functions.

The identified safety barriers need to be verified and checked by Design team. After the feedback from design team the TFFR of ADM, APM and REP functions might be further improved.

7 REFERENCES

The following chapter includes the documents used as a reference.

7.1 INPUT DOCUMENTS

The input document are the documents containing the system definition.

Ref.	Document ID	Document title	Version
[1]	LA_GoA34_S2R_1.0.0_20231214	Deliverable D5.1 WP5 GoA3/4 Specification	1.0.0
[2]	SRS ATO up to GoA34 Logical Architecture Layer (Annex 3 of D6.2)_v1.2.0	SRS ATO up to GoA4 Logical Architecture layer	1.2.0

Table 10: Input documents

7.2 SAFETY PROCESSES

The following laws, regulations and standards deal mainly with the safety processes necessary to perform the safety analysis.

7.3 LEGAL SAFETY FRAMEWORK

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.

Ref.	Document ID	Document title	Version
[3]	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
[4]	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

Table 11: Legal safety framework

7.3.1 Other standards concerning the safety processes

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.

Ref.	Document ID	Document title	Version
[5]	EN 50126-1	Railway applications-The Specification and Demonstration of Reliability , Availability , Maintainability and Safety (RAMS) - Part 1 : Generic RAMS Process	2017
[6]	EN 50126-2	Railway applications-The Specification and Demonstration of Reliability , Availability , Maintainability and Safety (RAMS) - Part 2 : Systems Approach to Safety	2017
[7]	EN 50129	Railway applications-Communication, signalling and processing systems – Safety related electronic systems for signalling	2018
[8]	IEC 62267	Railway applications - Automated urban guided transport (AUGT) - Safety Requirement	2009
[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

Table 12: Safety standards – processes

7.4 TECHNICAL STANDARDS

Technical standards, including the technical specifications for interoperability, have been consulted as a support for the hazard identification and the identification of safety requirements. Overall conformity[5] 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 D). The identified requirements from ANNEX C shall be fulfilled.

7.4.1 Technical specification for interoperability

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

Table 13: TSI list

[5] "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.

7.4.2 Other technical standards

Ref.	Document ID	Document title	Version
[17]	EN 14752:2019+A1:2021	Railway applications- Bodyside entrance systems for rolling stock	2021
[18]	ETCS Subset-026-3	ERTMS/ETCS - System Requirements Specification Chapter 3 Principles	V4.0

7.5 RELATED WP8.3 DOCUMENTATION

The overall processes and results from the WP8.3 safety analysis are included within this report. The hazard log, i.e. the working tool used to document the safety analysis, as well as the description of the methods used for the quantitative explicit risk estimation, are available as separate attachments.

Ref.	Document ID	Version
[19]	R2DATO_WP8.3_Functions_hazard_identification_And_Risk_Assessment.	00.02
[20]	Methods for the explicit risk estimation	1.0

Table 14: Other WP8.3 documentation

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 different companies involved in R2DATO project: each company was in charge of the safety analysis and / or the of the cross review for one or more functions.

The hazard log is attached as a separate Excel file, see “Hazard Log”. The most relevant results from the hazard log, namely the list of hazards, external safety barriers and the final TFFR, are presented in the following annexes.

COLUMN	DECRIPTION	EXPLANATION
Column A	ID	The numbering of the line
Column B	Logical function	The logical function name considered in the analysis.
Column C	Logical Component	The logical component from SRS chapter xx
Column D	Input	All inputs need for the logical function
Column E	Output	
Column F	Failure Mode	The failure mode of the input for each Logical function we aim to analyse. The failure modes are as follows : • Omission : the input is missing. • Incorrect : the input is incorrect. • Commission
Column G	failure description	The context description of failure on functions
Column H	Assumptions	Description of assumptions of safety analysis, Used to have rules to continue with the safety analysis in case some SRS specification is not clear or missing.
Column I	Questions	Questions to Design team, in case of SRS description is not clear
Column J	Initial effect	Describes the first effect of the analyzed module in case a failure occurs on the function
Column K	Intermediate effect	Description of what happens in case of error propagation in the logic of the analyzed module
Column L	Final Effect	Description of the final effect in case of error propagation until the train operation
Column M	Accident	The list of accidents happened in case of failure condition happen on functions
Column N	Failure chain	brief description of the chain of failures that follows from the initial effect to the final effect
Column O	Hazard ID	Hazard ID (you can find the description in the Hz Description sheet) with the description of the hazard in case of function failure
Column P	Impact	Safety classification oin case of function failure

COLUMN	DECRIPTION	EXPLANATION
Column Q	Safety Barriers	Suggested Safety Barriers raised during the Hazard identification phase.
Columns R,S,T	Risk Evaluation without safety barriers • Safety Category (column S), • Severity Justification (column T), • Initial TFFR without safety barriers (column U)	Initial safety category according to severity of accidents
		Justification of severity allocation
		Initial TFFR without safety barriers allocated according to severity
Columns U-X	Code of practice	Reference to an external Subsets,TSI etc, which can be compared to the concept of failure described above
	Justification of code of practice applicability	Description why the Code of practive is applicable to the Failure condition of functions
	Is the Hazard completely controlled by the code of practice?	Description of level of coverage of the code of practice
	Related Subhazards	IDs of Related Subhazards that can be traced
Columns Y-AB	Similar reference system	Reference to another function of another subsystem, which behavior can be compared to the concept of failure described above
	Justification of the similar reference system applicability (same function, same interface, same operational context)	Description why the similar reference system is applicable to the Failure condition of functions
	Is the hazard completely controlled by the similar reference system?	Description of level of coverage similar reference system
	Related Hazards	IDs of Related hazards that can be traced
AC	Safety barriers description	List of all type of safety barriers that can be used to cover the functions
AD-AH	Technica Safety barriers	These columns describe the external technical barriers which can intervene in case the failure condition occurs on the analyzed functions (i.e ATP, TCMS etc..), according to the inspection interval applied on barriers (column AG) and function failure rate of barriers (column AG) it is possible to calculate a factor for the risk reduction (columns AH, AI) which contributes to the initial risk reduction applied to the initial TFFR (see column U)
AI-AP	Human barrier	These columns describe the Human barriers with humans which can intervene in case the failure condition occurs on the analyzed function, in accordance with the following risk reduction choices: • Risk reduction based on task (column AK) • Risk reduction based on work condition (column AM) • Risk reduction based on stress level (column AP) It is possible to calculate the total risk reduction factors based on human safety barriers (column AQ) which contributes to the initial risk reduction applied to the initial TFFR (see column U).
AQ-AT	N/A	
AU-AX	Physical barrier	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 AW), it is possible to

COLUMN	DECRIPTION	EXPLANATION
		calculate a factor for the risk reduction (column AY) which contributes to the initial risk reduction applied to the initial TFFR (see column U)
AY	Final Risk	In this column is reported the sum of all the contributions calculated for each external barrier is reported and represents the final risk factor to be applied to the initial TFFR of the function
AZ-BC	Final TFFR	In these columns have been reported the final values of final TFFRs of functions according to the Final risk reduction factors reported in column BB and according to which initial TFFR was chosen on functions according to the following initial TFFRs choices: • TFFR=1E-08 (column BC) • TFFR=1E-07 (Column BD) • TFFR=1E-06 (Column BE) • TFFR=1E-05 (Column BF)
BD	Final Impact	In this column is reported the final impact of functions after the external safety barriers application
BE	Comments	In this column are reported all comments related risk evaluation analysis
BF	Assumptions	In this column are reported all assumptions related risk evaluation analysis
BJ	SRAC description	In this column are reported all Safety related application condition (SRAC) applicable on the functions safety analysis
BK	Exported to	it is reported to which external module, body, natural person, manual etc. the SRAC is exported

Table 15: Hazard log columns explication

ANNEX B. HAZARD LIST AND HAZARD MANAGEMENT

The following table summarizes the identified hazards and mitigations. Each hazard is linked to the function which, in case of failure could cause it. The same hazard can also be caused by failures of different functions. For instance, a train might be moving with open doors if

- the doors open request is unduly sent (function “Start door opening and closing sequence”), or
- traction is applied too early, when doors are still open (function “check departure conditions”).

This is captured in the table below when a hazard is linked to different functions.

A failure of the ADM, APM or REP functions could cause a hazard, i.e. a dangerous situation; that does not mean that each ADM, APM or REP failure directly and immediately leads to an accident with harm to persons or loss of human lives. Safety barriers outside of APM, ADM and REP can also independently prevent an accident from occurring, even in case of a hazard caused by an ADM, APM or REP failure. For instance, the door-traction interlock by TCMS inhibits traction when the doors are open. The table below lists down the identified external safety barriers which are completely independent on the ADM, APM or REP functions.

If the external safety barriers are adequate on their own to completely control the hazard6 caused by an ADM, APM or REP failure, then the ADM, APM or REP failure can be accepted with a TFFR corresponding to Basic Integrity. If, on the contrary, the risk cannot be reduced to an acceptable level by means of the external safety barriers alone, then the ADM, APM or REP function is required to fulfil a specific TFFR, indicated in the table below.

Hazard ID	Hazardous description	Functions
Hitachi_Haz_ID_SRS_003	Wrong or Missing application of Safe reaction	Command and supervise horn
Hitachi_Haz_ID_SRS_007	Wrong or missing application of Safe reaction in case of Fire On Board	Monitor Fire Alarm
Hitachi_Haz_ID_SRS_008	Brake release application not acceptable for particular location along the track	Acquire train and ADM data
Hitachi_Haz_ID_SRS_009	Wrong or missing application of initial traction effort of a loco with consequent train Roll Back (in case of missing traction effort) or loss of train integrity (in case of excessive traction effort)	Control initial traction effort
Hitachi_Haz_ID_SRS_014	Wrong selection of the Virtual cab	Determine APM state
Hitachi_Haz_ID_SRS_016	Wrong train condition acquired for the mission and consequent movement of the train with train parameters not complient	Acquire JP
Hitachi_Haz_ID_SRS_016	Wrong train condition acquired for the mission and consequent movement of the train with train parameters not complient	Acquire Train parameters
Hitachi_Haz_ID_SRS_020	Trackside and OnBoard implausibility operational context (i.e OnBoard is in Goa2 context but trackside is informed of a GoA3/4 context)	Determine APM state
AZD_ATOGoA3/4_HZD_001	Wrong MP sent to train leads to collision with another train	Define if consist is master or slave
AZD_ATOGoA3/4_HZD_002	Assigning of two units as master leads to violation of train integrity	Define if consist is master or slave
AZD_ATOGoA3/4_HZD_003	No APM becomes master and ATO is not engaged	Define if consist is master or slave

[6] the related risk can be accepted according to the selected risk acceptance criteria

AZD_ATOGoA3/4_HZD_004	ATO engaged when not expected	Determine ADM state
AZD_ATOGoA3/4_HZD_005	ATO is not engaged when it should	Determine ADM state
AZD_ATOGoA3/4_HZD_008	MP and JP are not updated by REP	Determine REP state
CAF_aATOGoA3/4_HZD_001	Train running with safety critical system failures	Monitor system status

CAF_aATOGoA3/4_HZD_004	Calculated Maximum authorised speed is less restrictive than it should.	Determine Maximum authorized speed
CAF_aATOGoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	-Compute Operational Speed and Acceleration

CAF_aATOGoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	Acquire train and ADM data
CAF_aATOGoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	Respect JP Timing Points and Optimize the consumption
SBB_ATOGoA3/4_HZD_004	The train fails to acoustically warn persons or road and rail vehicles of its presence	- Define evaluated reaction depending on incident

SBB_ATOGoA3/4_HZD_004	The train fails to acoustically warn persons or road and rail vehicles of its presence	- Monitor shunting circuit compensator default
SBB_ATOGoA3/4_HZD_005	The trains runs in GoA1 or GoA2 with a deactivated vigilance device (dead man / SiFa)	Deactivate Driver Activity Control
SBB_ATOGoA3/4_HZD_006	External doors opened outside of a safe area for passenger exchange	-Start door opening or closing sequence
SBB_ATOGoA3/4_HZD_006	External doors opened outside of a safe area for passenger exchange	Acquire train and ADM data
SBB_ATOGoA3/4_HZD_006	External doors opened outside of a safe area for passenger exchange	Stop exactly at the intended location
SBB_ATOGoA3/4_HZD_008	External doors open for an out of service train	Start door opening or closing sequence
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	- Regulate traction and braking effort
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	Request holding brake
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	Check departure conditions
SBB_ATOGoA3/4_HZD_011	Door closing while people are boarding or leaving the train	Start door opening or closing sequence
SBB_ATOGoA3/4_HZD_012	People onboard on an out of service train	Start door opening or closing sequence
SBB_ATOGoA3/4_HZD_015	Train moving with open doors	Monitor doors and platform gap incidents

SBB_ATOGoA3/4_HZD_016	Person stuck in a door	Monitor doors and platform gap incidents
SBB_ATOGoA3/4_HZD_017	Train not secured against movement in case of obstacle in the gap between platform and train	Monitor doors and platform gap incidents
SBB_ATOGoA3/4_HZD_020	Undesired train movement	Check departure conditions
SBB_ATOGoA3/4_HZD_021	Train movement in the wrong direction (e.g. backward instead of forward)	Determine running direction
SNCF_ATOGoA3/4_HZD_001	Absence / lack of reaction in case of incident / danger	Manage low adhesion
SNCF_ATOGoA3/4_HZD_003	Incorrect service brake supervision	Supervise service brake efficiency during operation
SNCF_ATOGoA3/4_HZD_008	Unextraction of mandatory information from infrastructure database	Map REP with route
ALSTOM_ATOGoA3/4_HZD_009	No reaction or reaction with delay in case of incident / danger	Acquire Segment Profile information
ALSTOM_ATOGoA3/4_HZD_012	The doors train are closed and passengers are closed in the train in emergency situation	Manage supervision orders
ALSTOM_ATOGoA3/4_HZD_013	Panic in train while shutdown activated and train on tracks	Manage mission execution
DB_ATOGoA3/4_HZD_001	Passenger stuck on the train in emergency situation and cannot leave the train	Start door Opening or closing sequence
DB_ATOGoA3/4_HZD_002	Door open while the train is moving	Start door Opening or closing sequence
DB_ATOGoA3/4_HZD_003	Incorrect management of the ATO speed profile lead to Train Overspeed	Regulate traction and braking effort
DB_ATOGoA3/4_HZD_004	Incorrect management of the ATO speed profile lead to Excessive traction effort	Regulate traction and braking effort
DB_ATOGoA3/4_HZD_005	Brake overheating when holding brake is applied while traction is applied, ultimately leading to fire or collision / derailment due to reduced braking performance	Request holding brake
DB_ATOGoA3/4_HZD_006	Coupling process start when train is not ready.	Start coupling
AZD_Haz_ID_SRS_003	Sanding is not used on section where it is requested	Inhibit sanding
AZD_Haz_ID_SRS_004	Sanding is used on section where sanding is prohibited	Inhibit sanding

Hitachi_Haz_ID_SRS_021	Wrong Train movement due to to wrong Driver emulation	Emulate action from driver
Hitachi_Haz_ID_SRS_003	Wrong or Missing application of Safe reaction	Emulate action from driver

Table 16: Hazard list and hazard management

ANNEX C. TRACEABILITY MATRIX

The following sections list the down the traceability between Functions and Requirements implemented in a design phase as reported in the §12 of [2] and all Hazards detected during the safety analysis as reported in ANNEX B.

Hazard ID	Hazardous description	Functions	Requirements ID as [2]
Hitachi_Haz_ID_SRS_003	Wrong or Missing application of Safe reaction	Command and supervise horn	APM-2.1 APM-2.2
Hitachi_Haz_ID_SRS_007	Wrong or missing application of Safe reaction in case of Fire On Board	Monitor Fire Alarm	APM-19.1

Hitachi_Haz_ID_SRS_008	Brake release application not acceptable for particular location along the track	Acquire train and ADM data	ADM-6.1 SS-125 7.1.5.4 SS-125 7.13.1.1 SS-125 7.13.1.2 SS-125 7.13.1.3 SS-125 7.13.1.4 SS-125 7.13.1.5 SS-125 7.13.1.6 SS-125 7.13.1.7 SS-125 7.13.1.8 SS-125 7.13.1.9 SS-125 7.13.2.1 SS-125 7.13.2.10 SS-125 7.13.2.11 SS-125 7.13.2.12 SS-125 7.13.2.13 SS-125 7.13.2.14 SS-125 7.13.2.15 SS-125 7.13.2.16 SS-125 7.13.2.17 SS-125 7.13.2.18 SS-125 7.13.2.19 SS-125 7.13.2.2 SS-125 7.13.2.20 SS-125 7.13.2.21 SS-125 7.13.2.22 SS-125 7.13.2.23 SS-125 7.13.2.24 SS-125 7.13.2.25 SS-125 7.13.2.26 SS-125 7.13.2.27 SS-125 7.13.2.28 SS-125 7.13.2.29 SS-125 7.13.2.3 SS-125 7.13.2.30 SS-125 7.13.2.31 SS-125 7.13.2.32 SS-125 7.13.2.4 SS-125 7.13.2.5 SS-125 7.13.2.6 SS-125 7.13.2.7 SS-125 7.13.2.8 SS-125 7.13.2.9 SS-125 7.13.3.1 SS-125 7.13.3.2 SS-125 7.13.3.3 SS-125 7.13.3.4 SS-125 7.13.3.5 SS-125 7.13.3.6 SS-125 7.13.4.1

			SS-125 7.13.4.2 SS-125 7.13.4.3 SS-125 7.13.4.4
Hitachi_Haz_ID_SRS_009	Wrong or missing application of initial traction effort of a loco with consequent train Roll Back (in case of missing traction effort) or loss of train integrity (in case of excessive traction effort)	Control initial traction effort	SS-125 7.1.5.15 SS-125 7.1.5.16 SS-125 7.1.5.17 SS-125 7.1.5.18 SS-125 7.1.5.19 SS-125 7.1.5.20 SS-125 7.1.5.21 SS-125 7.1.5.22 SS-125 7.1.5.23 SS-125 7.1.5.27
Hitachi_Haz_ID_SRS_014	Wrong selection of the Virtual cab	Determine APM state	APM-9.1

Hitachi_Haz_ID_SRS_016	Wrong train condition acquired for the mission and consequent movement of the train with train parameters not complient	Acquire JP	REP-1.1 REP-1.2 REP-1.3 REP-1.4 SS-125 7.9.1.1 SS-125 7.9.1.2 SS-125 7.9.1.3 SS-125 7.9.1.4 SS-125 7.9.1.5 SS-125 7.9.1.6 SS-125 7.9.2.1 SS-125 7.9.2.2 SS-125 7.9.2.3 SS-125 7.9.2.4 SS-125 7.9.2.5 SS-125 7.9.3.1 SS-125 7.9.3.2 SS-125 7.9.3.3 SS-125 7.9.3.4 SS-125 7.9.3.5 SS-125 10.1.7.1 SS-125 10.1.7.2 SS-125 10.1.7.3 SS-125 10.1.7.4 SS-125 10.1.7.6 SS-125 10.1.7.8 SS-125 10.1.7.17 SS-125 10.1.7.18 SS-125 10.1.7.18.1 SS-125 10.1.7.19 SS-125 10.1.7.20 SS-125 10.1.7.26
Hitachi_Haz_ID_SRS_016	Wrong train condition acquired for the mission and consequent movement of the train with train parameters not complient	Acquire Train parameters	REP-4.1 REP-4.2 REP-4.3 REP-4.4 REP-4.5 REP-4.6
Hitachi_Haz_ID_SRS_020	Trackside and OnBoard implausibility operational context (i.e OnBoard is in Goa2 context but trackside is informed of a GoA3/4 context)	Determine APM state	APM-9.1
AZD_ATOGoA3/4_HZD_001	Wrong MP sent to train leads to collision with another train	Define if consist is master or slave	APM-8.1 APM-8.2 APM-8.3
AZD_ATOGoA3/4_HZD_002	Assigning of two units as master leads to violation of train integrity	Define if consist is master or slave	APM-8.1 APM-8.2 APM-8.3

AZD_ATOGoA3/4_HZD_003	No APM becomes master and ATO is not engaged	Define if consist is master or slave	APM-8.1 APM-8.2 APM-8.3
AZD_ATOGoA3/4_HZD_004	ATO engaged when not expected	Determine ADM state	ADM-13.1 SS-125 7.12.1.1 SS-125 7.12.1.2 SS-125 7.12.1.3 SS-125 7.12.1.4 SS-125 9.1.1.1 SS-125 9.1.1.2 SS-125 9.1.2.1 SS-125 9.1.2.1.1 SS-125 9.1.2.2
AZD_ATOGoA3/4_HZD_005	ATO is not engaged when it should	Determine ADM state	ADM-13.1 SS-125 7.12.1.1 SS-125 7.12.1.2 SS-125 7.12.1.3 SS-125 7.12.1.4 SS-125 9.1.1.1 SS-125 9.1.1.2 SS-125 9.1.2.1 SS-125 9.1.2.1.1 SS-125 9.1.2.2
AZD_ATOGoA3/4_HZD_008	MP and JP are not updated by REP	Determine REP state	REP-5.1
CAF_aATOGoA3/4_HZD_001	Train running with safety critical system failures	Monitor system status	APM-11.1 APM-11.2 APM-11.3 APM-11.4 APM-11.5 APM-11.6
CAF_aATOGoA3/4_HZD_004	Calculated Maximum authorised speed is less restrictive than it should.	Determine Maximum authorized speed	SS-125 7.1.3.2 SS-125 7.1.3.3 SS-125 7.1.3.4 SS-125 7.1.3.5 SS-125 7.1.3.6 SS-125 7.1.3.7 SS-125 7.1.3.8 SS-125 7.1.3.9 SS-125 7.1.3.10
CAF_aATOGoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	-Compute Operational Speed and Acceleration	SS-125 7.1.1.1 SS-125 7.1.1.2 SS-125 7.11.1.1 SS-125 7.11.1.2

CAF_aATO GoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	Acquire train and ADM data	ADM-6.1 SS-125 7.1.5.4 SS-125 7.13.1.1 SS-125 7.13.1.2 SS-125 7.13.1.3 SS-125 7.13.1.4 SS-125 7.13.1.5 SS-125 7.13.1.6 SS-125 7.13.1.7 SS-125 7.13.1.8 SS-125 7.13.1.9 SS-125 7.13.2.1 SS-125 7.13.2.10 SS-125 7.13.2.11 SS-125 7.13.2.12 SS-125 7.13.2.13 SS-125 7.13.2.14 SS-125 7.13.2.15 SS-125 7.13.2.16 SS-125 7.13.2.17 SS-125 7.13.2.18 SS-125 7.13.2.19 SS-125 7.13.2.2 SS-125 7.13.2.20 SS-125 7.13.2.21 SS-125 7.13.2.22 SS-125 7.13.2.23 SS-125 7.13.2.24 SS-125 7.13.2.25 SS-125 7.13.2.26 SS-125 7.13.2.27 SS-125 7.13.2.28 SS-125 7.13.2.29 SS-125 7.13.2.3 SS-125 7.13.2.30 SS-125 7.13.2.31 SS-125 7.13.2.32 SS-125 7.13.2.4 SS-125 7.13.2.5 SS-125 7.13.2.6 SS-125 7.13.2.7 SS-125 7.13.2.8 SS-125 7.13.2.9 SS-125 7.13.3.1 SS-125 7.13.3.2 SS-125 7.13.3.3 SS-125 7.13.3.4 SS-125 7.13.3.5 SS-125 7.13.3.6 SS-125 7.13.4.1

			SS-125 7.13.4.2 SS-125 7.13.4.3 SS-125 7.13.4.4

CAF_aATO GoA3/4_HZD_006	Calculated Journey related speed and distance is less restrictive than the SSEM	Respect JP Timing Points and Optimize the consumption	SS-125 7.1.2.1 SS-125 7.1.2.2 SS-125 7.1.2.3 SS-125 7.1.2.4 SS-125 7.1.2.5 SS-125 7.1.2.6 SS-125 7.1.2.7 SS-125 7.1.2.8 SS-125 7.1.2.9 SS-125 7.2.1.1 SS-125 7.2.1.2 SS-125 7.2.1.3 SS-125 7.2.1.4 SS-125 7.2.1.5 SS-125 7.2.1.6 SS-125 7.2.1.7 SS-125 7.2.1.8 SS-125 7.3.1.2 SS-125 7.3.1.3 SS-125 7.3.1.5 SS-125 7.3.1.6 SS-125 7.3.1.7 SS-125 7.3.1.8 SS-125 7.3.1.9 SS-125 7.3.1.1 SS-125 7.3.1.4 SS-125 7.3.1.10 SS-125 7.3.1.11 SS-125 7.4.1.3

SBB_ATOGoA3/4_HZD_004	The train fails to acoustically warn persons or road and rail vehicles of its presence	- Define evaluated reaction depending on incident	APM-13.1 APM-13.2.1 APM-13.2.2 APM-13.2.3 APM-13.2.5 APM-13.2.6 APM-13.2.7 APM-13.2.8.1 APM-13.2.8.2 APM-13.2.9 APM-13.2.10 APM-13.3.1 APM-13.3.2 APM-13.3.3 APM-13.4.1 APM-13.4.2 APM-13.5 APM-13.6 APM-13.7 APM-13.8.1 APM-13.8.2 APM-13.8.3 APM-13.9 APM-13.10 APM-13.12 APM-13.13 APM-13.14 APM-13.15
SBB_ATOGoA3/4_HZD_004	The train fails to acoustically warn persons or road and rail vehicles of its presence	- Monitor shunting circuit compensator default	APM-20.1
SBB_ATOGoA3/4_HZD_005	The trains runs in GoA1 or GoA2 with a deactivated vigilance device (dead man / SiFa)	Deactivate Driver Activity Control	APM-3.1

SBB_ATOGoA3/4_HZD_006	External doors opened outside of a safe area for passenger exchange	-Start door opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10
SBB_ATOGoA3/4_HZD_006	External doors opened outside of a safe area for passenger exchange	Acquire train and ADM data	ADM-6.1 SS-125 7.1.5.4 SS-125 7.13.1.1 SS-125 7.13.1.2 SS-125 7.13.1.3 SS-125 7.13.1.4 SS-125 7.13.1.5 SS-125 7.13.1.6 SS-125 7.13.1.7 SS-125 7.13.1.8 SS-125 7.13.1.9 SS-125 7.13.2.1 SS-125 7.13.2.10 SS-125 7.13.2.11 SS-125 7.13.2.12 SS-125 7.13.2.13 SS-125 7.13.2.14 SS-125 7.13.2.15 SS-125 7.13.2.16 SS-125 7.13.2.17 SS-125 7.13.2.18 SS-125 7.13.2.19 SS-125 7.13.2.2 SS-125 7.13.2.20 SS-125 7.13.2.21 SS-125 7.13.2.22 SS-125 7.13.2.23 SS-125 7.13.2.24 SS-125 7.13.2.25 SS-125 7.13.2.26 SS-125 7.13.2.27 SS-125 7.13.2.28 SS-125 7.13.2.29 SS-125 7.13.2.3 SS-125 7.13.2.30

			SS-125 7.13.2.31 SS-125 7.13.2.32 SS-125 7.13.2.4 SS-125 7.13.2.5 SS-125 7.13.2.6 SS-125 7.13.2.7 SS-125 7.13.2.8 SS-125 7.13.2.9 SS-125 7.13.3.1 SS-125 7.13.3.2 SS-125 7.13.3.3 SS-125 7.13.3.4 SS-125 7.13.3.5 SS-125 7.13.3.6 SS-125 7.13.4.1 SS-125 7.13.4.2 SS-125 7.13.4.3 SS-125 7.13.4.4
SBB_ATOG oA3/4_HZD_ 006	External doors opened outside of a safe area for passenger exchange	Stop exactly at the intended location	SS-125 7.1.4.1 SS-125 7.1.4.2 SS-125 7.1.4.3 SS-125 7.1.4.4 SS-125 7.1.4.5

SBB_ATOGoA3/4_HZD_008	External doors open for an out of service train	Start door opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	- Regulate traction and braking effort	SS-125 7.1.5.1 SS-125 7.1.5.2 SS-125 7.1.5.3 SS-125 7.1.5.5 SS-125 7.1.5.6 SS-125 7.1.5.7 SS-125 7.1.5.8 SS-125 7.1.5.9 SS-125 7.1.5.10 SS-125 7.1.5.11 SS-125 7.1.5.12 SS-125 7.1.5.13 SS-125 7.1.5.14 SS-125 7.1.5.24 SS-125 7.1.5.25 SS-125 7.1.5.26 SS-125 7.1.5.28 SS-125 7.1.5.29 SS-125 6.2.1.6 SS-125 6.2.1.6.1
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	Request holding brake	SS-125 6.2.1.7 SS-125 6.2.1.8 SS-125 6.2.1.9 SS-125 6.2.1.10
SBB_ATOGoA3/4_HZD_009	Train moving while it is supposed to be secured against movement (i.e. during passenger exchange, coupling and uncoupling)	Check departure conditions	SS-125 7.2.3.1 SS-125 7.2.3.2 SS-125 7.2.3.3 SS-125 7.2.3.4 SS-125 7.2.3.5

SBB_ATOGoA3/4_HZD_011	Door closing while people are boarding or leaving the train	Start door opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10
SBB_ATOGoA3/4_HZD_012	People onboard on an out of service train	Start door opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10
SBB_ATOGoA3/4_HZD_015	Train moving with open doors	Monitor doors and platform gap incidents	APM-18.1.1 APM-18.1.2 APM-18.2
SBB_ATOGoA3/4_HZD_016	Person stuck in a door	Monitor doors and platform gap incidents	APM-18.1.1 APM-18.1.2 APM-18.2
SBB_ATOGoA3/4_HZD_017	Train not secured against movement in case of obstacle in the gap between platform and train	Monitor doors and platform gap incidents	APM-18.1.1 APM-18.1.2 APM-18.2
SBB_ATOGoA3/4_HZD_020	Undesired train movement	Check departure conditions	SS-125 7.2.3.1 SS-125 7.2.3.2 SS-125 7.2.3.3 SS-125 7.2.3.4 SS-125 7.2.3.5
SBB_ATOGoA3/4_HZD_021	Train movement in the wrong direction (e.g. backward instead of forward)	Determine running direction	APM-1.1 APM-1.2 APM-1.3

SNCF_ATO GoA3/4_HZ D_001	Absence / lack of reaction in case of incident / danger	Manage low adhesion	SS-125 7.5.1.1 SS-125 7.5.1.2 SS-125 7.5.1.3 SS-125 7.5.1.5 SS-125 7.5.1.6
SNCF_ATO GoA3/4_HZ D_003	Incorrect service brake supervision	Supervise service brake efficiency during operation	ADM-8.1
SNCF_ATO GoA3/4_HZ D_008	Unextraction of mandatory information from infrastructure database	Map REP with route	REP-7.1.1 REP-7.1.2 REP-7.1.3 REP-7.1.4 REP-7.2.1 REP-7.2.2 REP-7.3 SS-125 7.8.1.1 SS-125 7.8.1.2 SS-125 7.8.2.1 SS-125 7.8.2.2 SS-125 7.8.3.1 SS-125 7.8.3.2
ALSTOM_A TOGoA3/4_ HZD_009	No reaction or reaction with delay in case of incident / danger	Acquire Segment Profile information	REP-3.1 REP-3.2 REP-3.3.1 REP-3.3.2 REP-3.4 REP-3.5 SS-125 10.1.7.21 SS-125 10.1.7.22 SS-125 10.1.7.24 SS-125 10.1.7.25 SS-125 10.1.7.26
ALSTOM_A TOGoA3/4_ HZD_012	The doors train are closed and passengers are closed in the train in emergency situation	Manage supervision orders	APM-5.1 APM-5.2.1 APM-5.2.2 APM-5.2.3 APM-5.3.1 APM-5.3.2 APM-5.5 APM-5.6

ALSTOM_ATOGoA3/4_HZD_013	Panic in train while shutdown activated and train on tracks	Manage mission execution	APM-10.1 APM-10.2 APM-10.3 APM-10.4.1 APM-10.4.2 APM-10.5 APM-10.6.1 APM-10.6.2 APM-10.6.3 APM-10.6.4 APM-10.6.5 APM-10.6.6 APM-10.6.7 APM-10.6.8.1 APM-10.6.9 APM-10.6.10 APM-10.11
DB_ATOGoA3/4_HZD_001	Passenger stuck on the train in emergency situation and cannot leave the train	Start door Opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10
DB_ATOGoA3/4_HZD_002	Door open while the train is moving	Start door Opening or closing sequence	ADM-10.1 ADM-10.2.1 ADM-10.2.2 ADM-10.3 SS-125 7.2.2.1 SS-125 7.2.2.2 SS-125 7.2.2.3 SS-125 7.2.2.4 SS-125 7.2.2.5 SS-125 7.2.2.6 SS-125 7.2.2.7 SS-125 7.2.2.8 SS-125 7.2.2.9 SS-125 7.2.2.10

DB_ATOGoA3/4_HZD_003	Incorrect management of the ATO speed profile lead to Train Overspeed	Regulate traction and braking effort	SS-125 7.1.5.1 SS-125 7.1.5.2 SS-125 7.1.5.3 SS-125 7.1.5.5 SS-125 7.1.5.6 SS-125 7.1.5.7 SS-125 7.1.5.8 SS-125 7.1.5.9 SS-125 7.1.5.10 SS-125 7.1.5.11 SS-125 7.1.5.12 SS-125 7.1.5.13 SS-125 7.1.5.14 SS-125 7.1.5.24 SS-125 7.1.5.25 SS-125 7.1.5.26 SS-125 7.1.5.28 SS-125 7.1.5.29 SS-125 6.2.1.6 SS-125 6.2.1.6.1
DB_ATOGoA3/4_HZD_004	Incorrect management of the ATO speed profile lead to Excessive traction effort	Regulate traction and braking effort	SS-125 7.1.5.1 SS-125 7.1.5.2 SS-125 7.1.5.3 SS-125 7.1.5.5 SS-125 7.1.5.6 SS-125 7.1.5.7 SS-125 7.1.5.8 SS-125 7.1.5.9 SS-125 7.1.5.10 SS-125 7.1.5.11 SS-125 7.1.5.12 SS-125 7.1.5.13 SS-125 7.1.5.14 SS-125 7.1.5.24 SS-125 7.1.5.25 SS-125 7.1.5.26 SS-125 7.1.5.28 SS-125 7.1.5.29 SS-125 6.2.1.6 SS-125 6.2.1.6.1
DB_ATOGoA3/4_HZD_005	Brake overheating when holding brake is applied while traction is applied, ultimately leading to fire or collision / derailment due to reduced braking performance	Request holding brake	SS-125 6.2.1.7 SS-125 6.2.1.8 SS-125 6.2.1.9 SS-125 6.2.1.10

DB_ATOGoA3/4_HZD_006	Coupling process start when train is not ready.	Start coupling	APM-6.1 APM-6.2.1 APM-6.2.3 APM-6.2.4 APM-6.3.1 APM-6.3.2
AZD_Haz_ID_SRS_003	Sanding is not used on section where it is requested	Inhibit sanding	APM-22.1
AZD_Haz_ID_SRS_004	Sanding is used on section where sanding is prohibited	Inhibit sanding	APM-22.1
Hitachi_Haz_ID_SRS_021	Wrong Train movement due to to wrong Driver emulation	Emulate action from driver	APM-4.1 APM-4.2.1 APM-4.2.2 APM-4.2.4.1 APM-4.2.4.2 APM-4.2.4.3 APM-4.3.1 APM-4.3.2 APM-4.4.1.1 APM-4.4.1.2 APM-4.5 APM-4.6.1 APM-4.6.2 APM-4.7.1 APM-4.7.2 APM-4.7.3 APM-4.7.4 APM-4.7.5

Hitachi_Haz_ID_SRS_003	Wrong or Missing application of Safe reaction	Emulate action from driver	APM-4.1 APM-4.2.1 APM-4.2.2 APM-4.2.4.1 APM-4.2.4.2 APM-4.2.4.3 APM-4.3.1 APM-4.3.2 APM-4.4.1.1 APM-4.4.1.2 APM-4.5 APM-4.6.1 APM-4.6.2 APM-4.7.1 APM-4.7.2 APM-4.7.3 APM-4.7.4 APM-4.7.5

Table 17: Traceability Matrix Functions-Requirements-Hazards

ANNEX D. EXTERNAL SAFETY BARRIERS

The following section lists down the external safety barriers considered within the risk analysis.

Barrier ID	Safety barrier description	Related Functions
CAF_SafBar_01 DB_SafBar _02 Hitachi_SafBar_01 Hitachi_SafBar_11 CEIT_SafBar_01	**ATP protects against overspeed** The ATP continuously supervises the speed during GoA3/4 operation. An emergency brake is triggered if the speed threshold is exceeded ("overspeed").	Compute Operational Speed and Acceleration Regulate traction and braking effort Supervise service brake efficiency during operation Manage low adhesion Determine APM state Respect JP Timing Points and Optimize the consumption Monitor battery protection mode

Barrier ID	Safety barrier description	Related Functions
CAF_SafBar_02	**TCMS interlock of traction** TCMS avoids the possibility of two consists tractioning in different directions when coupled.	Define if consist is master or slave
DB_ SafBar _01 Alstom_SafBar_01 Hitachi_SafBar_12	**TCMS: Door- Traction Interlock** Door-Traction Interlock as required by LOC&PAS TSI 4.2.5.5.7 Traction power shall be applied only when all doors are closed and locked. The door-traction interlock system shall prevent traction power being applied when not all of the doors are closed and locked.-	Regulate traction and braking effort Start door opening sequence Start door closing sequence Determine ADM state Monitor doors and platform gap incidents
DB_SafBar _03	**TCMS: holding brake release** Holding brake release is done by TCMS as soon as enough traction is applied. Traction against holding brakes can only be applied for a limited amount of time, e.g. 85 seconds for passenger trains and 40 seconds for freight trains. Enough traction = sufficient traction to avoid rolling back, e.g. in case of an uphill start	Request holding brake Start Door Closing Sequence
DB_SafBar _04a	**ATP and TCMS: holding brake application** When the train is at standstill (0 km/h), then TCMS (and / or ATP) automatically applies the holding brake. Note: this function is documented in the SRS, see section 12.6.16 (ATP) - Supervise runaway movement This function supervises standstill, roll away and reverse movement.	Request holding brake Regulate traction and braking effort
DB_SafBar _04b	**Brake Control Unit: holding brake application** In addition to DB_SafBar _04a (ATP and TCMS). When the train is stationary AND zero speed is detected, then the rolling stock	Request holding brake Regulate traction and braking effort

Barrier ID	Safety barrier description	Related Functions
	(Brake Control unit) automatically applies holding brake.	
DB_SafBar _04c Hitachi_SafBar_05 SBB_SafBar_01	**ATP: Roll Away Protection (RAP)** (SS-026 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. (SS-026 3.14.2.3) If the controller is in neutral position, the RAP shall prevent forward and reverse movements of the train. The RAP prevents movement by triggering a brake command after a distance specified by the national value Note: this function is documented in the SRS, see section 12.6.16 (ATP) - Supervise runaway movement This function supervises standstill, roll away and reverse movement.	Request holding brake Regulate traction and braking effort Control initial traction effort Determine running direction
DB_SafBar _08	**Door Control Unit (DCU): obstacle detection and reaction** Obstacle detection for doors as required by LOC&PAS TSI 4.2.5.5.3 External passenger access doors shall incorporate devices that detect if they close on an obstacle (e.g. a passenger). Where an obstacle is detected the doors shall automatically stop, and remain free for a limited period of time or reopen The function is documented in the SRS, see TCMS 11.16.20 "Manage access and loading" and 11.16.19 "Manage door system upon obstacle", for both functions the output is called "obstacle_in_doors" .	Start door closing sequence.

Barrier ID	Safety barrier description	Related Functions
DB_SafBar _11a	**TCMS function "Manage access and loading": door opening inhibition at speed** 1. "TCMS shall inhibit door opening when the train is running"	Start door opening sequence
DB_SafBar _11b	**TCMS function "Manage access and loading": door release authorization below 3km/h** 3. TCMS shall authorise the door release when TCMS standstill signal = TRUE. This signal corresponds to a decreasing speed threshold (below 3 kph) ensuring the train stop in a few meters. Optionally, the feedback of holding brake application could be used for authorising the door release.	Start door opening sequence
DB_SafBar _13	**Manual check: Check by train attendant / RU staff at the end of passenger service** In GoA3, Train Attendant checks that the train is empty at the end of Passenger service. In GoA4, a check by RU staff is required before to go to the depot. If no Railway Undertaking (RU) staff is available to inspect the train before it is taken out of service, cameras must be installed on the train to ensure that all passengers leave the train before the train is out of service.	Start door opening sequence Start door closing sequence
DB_SafBar _14 Alstom_SafBar_03 Hitachi_SafBar_10	**Door system: Door emergency opening (or analogous solutions)** TSI LOC&PAS 4.2.5.5.9 Each door shall be provided with an individual internal emergency-opening device accessible to passengers, that shall allow the door to open; this device shall be active when the speed is below 10 km/h.	Start door opening sequence Manage supervision orders (door closure autorisation)

Barrier ID	Safety barrier description	Related Functions
	Alternatively: emergency exits are provided in case the external doors are blocked (e.g. through breakable external glasses).	
DB_SafBar _17	**Hot axle box detection** (TSI LOC&PAS 4.2.10.2.3). The hot box axle deection mitigate the risk for overheating brake pads and axles	Request holding brake
Alstom_SafBar_02	**ATP protection** Subset-035 : Specific Transmission Module FFFIS Subset-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2 The train is protected by ATP during using STM	Monitor system status (STM status)
Alstom_SafBar_05	**Signalling system: trackside protection** Tracks where the train is stopped is protected to prevent other trains to enter on zone	Manage mission execution (cmd shutdown mode)
Hitachi_SafBar_03	**ATP Protection** ATP shall perform a consistency check between the cab selected OnBoard and status provided to trackside and intervene in case of inconsistency	Determine APM state
NRD_SafBar_05	**Emergency/rescue points.** Emergency / rescue points are set up to allow a safe evacuation. If the distances between stations are too long to facilitate the requirements to running capability, the stations must be supplemented with emergency/rescue points where the evacuation can be safely accomplished, including standby services that would facilitate evacuation in the event of an emergency.	Monitor Fire Alarm

Barrier ID	Safety barrier description	Related Functions
NRD_SafBar_06	**Fire prevention in conformance with the EN 45545 series of standards.** EN 45545 specifies measures to "prevent fires occuring due to technical faults and due to equipment design or vehicle layout (Part 1, Part 4, Part 5 and Part 7)". Fire prevention reduces the frequency of occurrence of fire.	Monitor Fire Alarm
NRD_SafBar_07	**Fire resistance in conformance with the EN 45545 series of standards.** EN 45545 specifies measures to "minimise the possibility of ignition of materials installed in railway vehicles due to accidents or vandalism (Part 1 and Part 2)".	Monitor Fire Alarm
NRD_SafBar_08	**Fire detection in conformance with the EN 45545 series of standards.** EN 45545 specifies measures to "detect a fire should it occur (Part 6)". Detection must be followed up by appropriate reaction by means of barriers mitigating loss of staff presence on train.	Monitor Fire Alarm
NRD_SafBar_09	**Fire limitation and containment in conformance with the EN 45545 series of standards.** EN 45545 specifies measures to "limit the spread of fire by specification of materials according to their operational categories (Part 2) and by measures for containment (Part 3)". The barrier improves the possibility of passengers' reaction.	Monitor Fire Alarm
NRD_SafBar_10	**Fire effects minimisation in conformance with the EN 45545 series of standards.** EN 45545 specifies measures to "minimise the effects of fire in terms of heat, smoke and toxic gases on passengers or staff through the specification of materials installed in railway vehicles (Part 2)". The barrier improves the possibility of passengers' reaction.	Monitor Fire Alarm
NRD_SafBar_11	**Fire control and management in conformance with the EN 45545 series of**	Monitor Fire Alarm

Barrier ID	Safety barrier description	Related Functions
	standards. EN 45545 specifies measures to "control and manage a fire, for example by means of fire detection, suppression and/or emergency energy shut down (Part 6)". Automatic fire extinguishing systems could be made mandatory if there are no other risk-minimising measures on part of the operators. The barrier improves the possibility of passengers' reaction.	
NRD_SafBar_13	**Rescue operation.** Resources and planning shall be in place to initiate and accomplish a rescue operation when needed.	Monitor Fire Alarm
Siemens_SafBar_10	***Operational barrier*** Staff workers are trained to be safe around trains. Tracks are blocked while persons are working on them. The collision can be avoided by applying the brakes promptly when PERCEPTION detects an obstacle. The collision may be also avoided by another infrastructurual technical and operational barriers, such as (track works' indication of approaching train, safety lines or fences at platforms and laong the track,level crossing devices etc.). But also train lights blicking, colours etc. The conditions are not know nad depends on mission profile, so it will not be considered now. Track workers are also communicating with OCC to be allowed stay on the track.	Command and supervise horn
SNCF_SafBar_01	**Code of practice "Sanding device" (SAM S 901).** The comparison between train location with each predefined sand inhibition zone for inhibiting sanding box is done in order to start or end of sanding suppression to TCMS. An error leads to have a wrongly sanding, that means an excessive sanding (more than no sanding).	Inhibit sanding

Barrier ID	Safety barrier description	Related Functions
	(There is a code of practice "Sanding device Version n° 3 - 12/12/2016 - SAM S 901" which sets the safety requirement for excess sanding at 10-8/h. Except in cases of absolute necessity (emergency braking, starting a heavy train that is likely to cause severe wheel slip, etc.), sanding must not be used, particularly in areas with switches. When sanding are used, sanding must be limited to what is strictly necessary because of the disturbance it can cause to the operation of switches or signals attached to track circuits. on track circuits. Except in an emergency, the driver of a single locomotive must never use sanding.	
SNCF_SafBar_02	*Technical system ATP = ETCS-OB for FS AD and OS AD (1,00 E-9 /h).One of* the driving function of the ATO-OB is to establish the maximum speed the train can run without interfering with the ETCS speed limits (Cf. Subset 125 v1.0.0 §7.1.1.1). The ATO maximum speed is establish within the ETCS target (EBI intervention limit - cf. SS-125 7.1.3.3), ceiling (permitted speed - cf. SS-125 7.1.3.2) and release speed limits received (cf. SS-125 7.1.3.6) from ETCS-OB. Using the information sent by the ETCS-OB, the ATO-OB shall compute the EBD curves within the current MA as defined in SS-026 §3.13.8.3 (cf. SS-125 7.1.3.7) and the ATO-OB shall estimate the EBI supervision limits based on the computed EBD curves based on SS-026 §3.13.9.3.2 (cf. SS-125 7.1.3.8).	Determine maximum authorised speed

Barrier ID	Safety barrier description	Related Functions
	In accordance with the ERTMS/ATO Reference Architecture (Cf. Subset 125 v1.0.0 §6.1), Automatic Train Protection is provided by ETCS.	
SNCF_SafBar_03	***SNCF_SafBar_03 Code of practice "Passenger access system" (SAM C 305).*** There is a code of practice "Passenger access system Version n°1 - 30/12/2013 - SAM C 305" which sets the safety requirement for several risks. For example, Inopportune opening of one or more doors while moving (this hazard is referred to in the locomotive and rolling stock for passengers TSI 4.2.5.5.8 (1) and (2).	Emulate action from driver
SBB_SafBar_02	**Operational rules for maintenance activities and inspections** Maintenance and inspection activities are done under a specific train context where Automatic Train Operation are not applicable. This train context state called “Maintenance” can be reached only by manual switch of a dedicated switch (see also SBB_SafBar_03 and SBB_SafBar_04)	Determine running direction
SBB_SafBar_05	**Cab interlock** Cabs are interlocked so that only one cab can be active at the same time. It is technically impossible to have two cabs active at the same time.	Determine running direction

Table 18: Safety barrier list

The following safety barriers require a discussion with the design team; in some cases, the discussion has already been started and needs to be finalized.

The list below includes also proposals for new (not already implemented) safety barriers.

Barrier ID	Safety barrier description	Related Functions
DB_SafBar _05	**Proposed safety barrier (not already existing)** **TCMS - Traction control** 1. Traction control in locomotives is designed to manage the amount of power delivered to the wheels to prevent wheel slip and excessive forces when starting or accelerating. 2. In case of distributed traction (motorized axles), load Sensitive Traction control systems adjust the tractive effort based on the weight and load distribution of the train. **Answer by the Design team :** 1) ATO up to GoA3/4 shall be installed only on train equipped with ATP. ATP can only cut traction. ATO up to GoA3/4 can use freight information coming from function "11.7.1 Communicate freight parameters" of SRS 1.0.0. Description: In this function, Freight Customer informs the system about the parameters necessary to drive the train according to the nature of freight because it impacts the driving style (steel, coal, liquids, dangerous goods...)". **Reply from the safety team**: 1) ATP can cut traction: is there any system (e.g. TCMS) which can monitor and detect excessive traction and request ATP to cut traction? 2) The freight information delivered to ATO is not a safety barrier, as it does not mitigate the hazard in case ATO fails and requires excessive traction. **The following specification (reference X2Rail4 baseline 02 driving rules chapter 11) can be added in SRS:** 11.1.1.1.2 For the excessive longitudinal force limitations related to non-homogeneous braking or pushing along the train, we proposed to have a safety barrier in the TCMS based on additional information sent to ETCS (similar to ED brake inhibition), 11.1.1.1.5 When pushing in an area sensitive for longitudinal force, the TCMS would prevent that the	Regulate traction and braking effort Manage low adhesion

Barrier ID	Safety barrier description	Related Functions
	difference between the effort applied by the traction units in rear of the train and the effort applied by traction units in front of the train is higher than a given threshold value, 11.1.1.1.6 Sensitive areas for longitudinal forces are area with curves or area covering some deflecting switch, 11.1.1.1.7 This proposal will be studied by UNISIG and EUG before creating a formal change request to bring in the CCM process of ERA	
Hitachi_SafBar_06	**Proposed safety barrier (not already existing)** **TCMS: Traction monitoring** TCMS shall monitor the traction applied and in case the traction force is insufficient or excessive, it shall apply a safe reaction Note: this safety barrier is similar to the safety barrier above (DB_SafBar _05) and they should be discussed together	Control initial traction effort
DB_SafBar _06	**BCU or TCMS: application of emergency braking in case of service brake failure** The rolling stock (brake system) monitors the service brake efficiency. If the service brake fails or is insufficient, then the BCU or TCMS will apply an emergency brake. **Open point to be clarified with design** The reaction (application of emergency brake) prevents insufficient braking due to failures of the service brake control system. It is unclear whether this barrier is effective if the reduced braking efficiency is due to overheated brakes (e.g. overheated brake pads, due to constant brake application by ATO in a downhill section for a heavy train)	Supervise service brake efficiency during operation

Barrier ID	Safety barrier description	Related Functions
	Passenger alarm interface with rolling stock **Open point** The TSI LOC& PAS should be amended for GoA3/4 operation. The following safety barrier is documented within the TSI LOC& PAS; the safety barrier requires a train driver in the cab, or alternatively the constant presence of a train assistant in the cab . As a result, the safety barrier is not directly applicable to GoA3/4. **Safety barrier** Guide for the application of the LOC&PAS TSI'- 2.4.26. Point 4.2.5.3.2: Passenger alarm: When a passenger alarm is initiated, this results in a visual and an acoustic signs in the cab. In the case of no acknowledgement of the alarm by the driver, a brake will be initiated after 10 seconds, which will be perceived by passengers as a confirmation of the alarm. **Additional details from Safety Workshop 16/09/2024** The TSI LOC&PAS requirement is fine in GoA2, as the driver sees the passenger alarm and, even if a brake is triggered, the driver can bypass it or restart driving afterward. In an automated system (GOA3/GOA4) the passenger alarm might be forwarded to the OCC, bur communication to the OCC might not be ensured everywhere on the track. Initiating a brake in case of no acknowledgement by the OCC might be dangerous, e.g in case the train is running in a tunnel or in case of fire onboard. **Summary of the answer by design** The passenger alarm goes to TCMS and then from TCMS to APM. APM can report to trackside or apply an automatic reaction. **Status:** Can the TSI LOC& PAS be amended?	Monitor Passenger Alarm
DB_SafBar _07		
DB_SafBar _09a	**TCMS: speed restriction in coupling mode**:	Start Coupling

Barrier ID	Safety barrier description	Related Functions
	1. Speed restriction when train is in coupling mode. **Open point** This safety barrier exists for mass transit systems (metros). Does this apply to railway rolling stock as well (high speed / mainline / regional ...)? Which system is tasked with enforcing the speed restriction in case of coupling? 2. If a train receives a coupling mode request but the train does not enter coupling mode, then emergency brake shall be applied. **IEC 62267 - 8.5.15 Safe speed during automatic coupling process** If automated coupling of trains with passengers on board is provided for recovery of stranded trains or reconfiguration of trains, the system which ensures safe train separation shall, for this specific movement • overrule the conditions for safe train separation, • command a speed to be specified. The coupling speed shall be specified in accordance with relevant standards or by the TA and SRA so that remaining passengers are not endangered by an excessive coupling jerk. Note : 1.There is no confirmation from the design team whether TCMS/Rolling stock monitor or interlock when Rolling stock recive the request coupling mode or not. 2. In general, there is a hardwire Interlock for coupling mode, when the driver is change the switch to coupling mode, but hardware failure, rolling stock does not get the coupling mode, rolling stock will react with emergency brake. Anyway, there is not clear information here for TCMS interlock on rolling stock side. Need more information to do propoer analysis.	
DB_SafBar_18	**Proposed safety barrier (not already existing)** **TCMS** 1. If the train (TCMS) does not get coupling ready, the	Start Coupling

Barrier ID	Safety barrier description	Related Functions
	system should not allow both train to couple. 2. If the onboard for Master train does not get Coupling complete signal, then the train shall not allow to start the mission profile after coupling. 3. Perform Post coupling tests (brake, electrical and traction system checks) **Open point** Can TCMS implement these safety barriers ?	
Alstom_SafBar_04	**Proposed safety barrier (not already existing)** **Communication between passengers and OCC** Passengers have possibility to communicate with OCC	Manage supervision orders (door closure autorisation)
Hitachi_SafBar_02	**Proposed safety barrier (not already existing)** **ATP Protection** The ATP shall monitor the APM state and GoA and intervene in case of inconsistency	Determine APM state
Hitachi_SafBar_04	**Proposed safety barrier (not already existing)** **ATP Protection** ATP could protect the train against the hazard, since it verifies the parameters value (received by another source) and intervene in case of inconsistency or missing / late data received	Acquire Train parameters Acquire JP
Hitachi_SafBar_07 Hitachi_SafBar_08	**Proposed safety barrier (not already existing)** **ATP: train – platform alignment** ATP shall verify the correct alignment of the train to the platform and where this is not satisfied, the opening of the doors outside the platform shall be inhibited. Passengers shall also advised to move to another carriage	Stop exactly at the intended location Start door opening closing sequence

Barrier ID	Safety barrier description	Related Functions
Hitachi_SafBar_09	**Proposed safety barrier (not already existing)** **TCMS: supervision of the activation of the driver activity control** The TCMS monitors that in GoA2 the driver activity control is activated	Deactivate Driver Activity Control
NRD_SafBar_01	**Proposed safety barrier (not already existing)** **Conventional fire alarm.** A conventional fire alarm must be present on board and when the alarm is triggered the train must stop at a safe place (at a station or an emergency/rescue point) and the doors must open.	Monitor Fire Alarm
NRD_SafBar_02	**Proposed safety barrier (not already existing)** **Automated reaction to fire detection (running capability + evacuation).** The train should automatically stop in a safe place (at a station or an emergency/rescue point), ensure that trains in the opposite direction are stopped, announce the need for evacuation, and open the doors. The train should be designed to be able to continue its journey long enough to safely accomplish the evacuation, in conformance with the requirements in EN 50553.	Monitor Fire Alarm
NRD_SafBar_03	**Proposed safety barrier (not already existing)** **Passenger-actuated function for stopping the train in a safe place (at a station or an emergency/rescue point) and announcing the need for evacuation (opening the doors).** This safety barrier is a mitigation of the consequence in case of failure of the function “Monitor Fire Alarm”. Passengers or staff can detect the fire and manually generate the alarm. The barrier "fire detected by passengers" is a human barrier, and as such requires that it can be considered an "intuitive task with clear rules and good training". This can only be achieved with a good safety culture, intuitive pictograms, sufficient guidance, etc.	Monitor Fire Alarm
NRD_SafBar_04	**Running capability in case of fire.** EN 50553 "defines requirements for running capability under fire conditions which are applicable to passenger carrying railway rolling	Monitor Fire Alarm

Barrier ID	Safety barrier description	Related Functions
	stock". These are barriers intended to mitigate the consequences in case of fire by ensuring that the train will be able to reach a safe area. Even if the rules are known, it must be assurred that they can be fulfilled also with ATO. In any case, running capability requires effective monitoring. **Open point** How does ATO ensures the running capability? ADM needs to be Basic Integrity, but if the ADM function "12.2.7 Regulate traction and braking effort" fails, then the running capability is not ensured. Should ADM become safety relevant? Should APM handle traction commands in case of fire detection to ensure the running capability?	
NRD_SafBar_12	**Proposed safety barrier (not already existing)** **Information to passengers about safety precautions related to fire and evacuation.** Information corresponding to the safety information given to passengers on airplanes to prepare them for a possible emergency situation, including information on placards and safety manuals in the seat. The barrier improves the possibility of passengers' reaction including the efficiency of the human barrier "Fire detected by passengers".	Monitor Fire Alarm
NRD_SafBar_14	**Proposed safety barrier (not already existing)** **Infrastructure design to support the evacuation and rescue operation.** Additional measures might be needed for ATO to compensate for the lack of staff on the train to guide the passengers (see also the RENFE file). Possible measures include markings, clear pictograms, navigation lights, etc.	Monitor Fire Alarm
NRD_SafBar_15	**Proposed safety barrier (not already existing)** **Evacuation coordination.** The evacuation must be coordinated, duly compensating for the lack of staff on board the train. This includes informing the passengers about where to go in tunnels, which direction to evacuate	Monitor Fire Alarm

Barrier ID	Safety barrier description	Related Functions
	(not where the wind is pushing the smoke), ensure that there is no live catenary, etc.	
SBB_SafBar_03	**Proposed safety barrier (not already existing)** **Manual switch to activate "maintenance" mode** The manual activation of a dedicated switch ensures that the "maintenance" state is reached. During "maintenance" state ATO is not active (e.g. ATO outputs are inhibited) and the train is secured against movement independently on ATO.	Determine running direction
SBB_SafBar_04	**Proposed safety barrier (not already existing)** **Training of staff concerning ATO hazards** Staff shall be trained to be safe while performing activities on automated trains or in their proximity. See also SBB_SafBar_02 and SBB_SafBar_03.	Determine running direction

Table 19: Safety barriers to be discussed (including proposals)

ANNEX E. FINAL TFFR FOR ADM, APM AND REP FUNCTIONS

In the following table the final TFFRs calculation have been reported for all **ADM** functions:

Function Title	Final TFFR
Check departure conditions	3,30E-07
Control initial traction effort	>10E-04
Determine ADM state	1,00E-07
Detect that final stopping point has been reached	No Impact
Determine maximum authorised speed	No Impact

Respect JP Timing Points and Optimize the consumption	1,00E-06
Compute Operational Speed and Acceleration	1,00E-06
Regulate traction and braking effort	1,00E-07
Manage low adhesion	1,00E-05
Supervise service brake efficiency during operation	1,00E-05
Start door opening sequence	1,00E-09
Stop exactly at the intended location	>10E-04
Request holding brake	1,00E-07
Acquire train and ADM data	>1,00e-04

Table 20: ADM TTFR per function

In the following table the final TFFRs calculation have been reported for all **APM** functions:

Function ID	Final TFFR
Define if consist is master or slave	1,00E-09
Command and supervise horn	1,00E-06
Monitor Fire Alarm	1,00E-05
Determine APM state	3,30E-06
Monitor system status	1,00E-09

Detrmine running direction	1,00E-05
Manage supervision orders	1,00E-06
Manage mission execution	>1e-04
Monitor shunting circuit compensator default	1,00E-07
Emulate action from driver	1,00E-09
Define evaluated reaction depending on incident	1,00E-07
Deactivate Driver Activity Control	3,30E-08
Monitor doors and platform gap incidents	1,00E-07
Monitor incidents affecting passengers	1,00E-07
Start coupling	1,00E-07
Monitor OMTS status	No Impact
Monitor Passenger Alarm	1,00E-05
Inhibit sanding	1,00E-08

Table 21: APM TTFR per function

In the following table the final TFFRs calculation have been reported for all **REP** functions:

Function Title	Final TFFR
Determine REP state	No impact
Acquire Train parameters	3,30E-06
Acquire JP	3,30E-06
Acquire Segment Profile information	1,00E-09

Acquire MP	No impact
Map REP with route	1,00E-09
Manage reporting	1,00E-07

Table 22: REP TTFR per function

ANNEX F. FAILURE MODES

Failure mode	Explanation	Remarks
Commission (also known as insertion)	The function executes when it should not.	
Omission	The function does not execute when it should.	
Early (includes sequence)	The function executes earlier than it should, or prior to another function.	
Late (includes sequence)	The function executes later than it should, or after another function.	
Partial	The function only partially executes.	For the scope of this analysis, the failure mode “Partial” has not been independently considered but is rather included in the concern of the failure mode “Incorrect”.
Incorrect (includes corruption)	The function executes in an incorrect way.	
Too much	The function executes more or for a longer time than it should.	For the scope of this analysis, the failure mode “Too much” has not been independently considered but is rather included in the concern of the failure modes “Commission” and “Early”.
Too little	The function executes less or for a shorter time than it should.	For the scope of this analysis, the failure mode “Too little” has not been independently considered but is rather included in the concern of the failure modes “Omission” and “Late”.

Corruption (also known as malicious intent)	The function is intentionally sabotaged (e.g. cybersecurity threats).	No malicious events are considered (e.g. cyber attacks), as they are expected to be covered by a dedicated Cybersecurity analysis

Table 23: Failure modes

ANNEX G. EXPLICIT RISK EVALUATION – RISK REDUCTION

The explanation of explicit risk evaluation can be found in the document [20].

.

ANNEX H. EXAMPLE OF WP8.1 AND WP8.3 INTEGRATION

An integration of the safety results from WP8.3 and WP8.1 is needed in the R2DATO context. The following picture depicts a proposal for such an integration. The proposal is based on the WP8.3 understanding of WP8.1; the blue parts, belonging to the WP8.1 scope, are expected to be modified be WP8.1 to better reflect the WP8.1 scope and activities. As a result, the proposal is not intended as a working concept but rather as a starting point for the discussion between WP8.1 and WP8.3 in the R2DATO context.

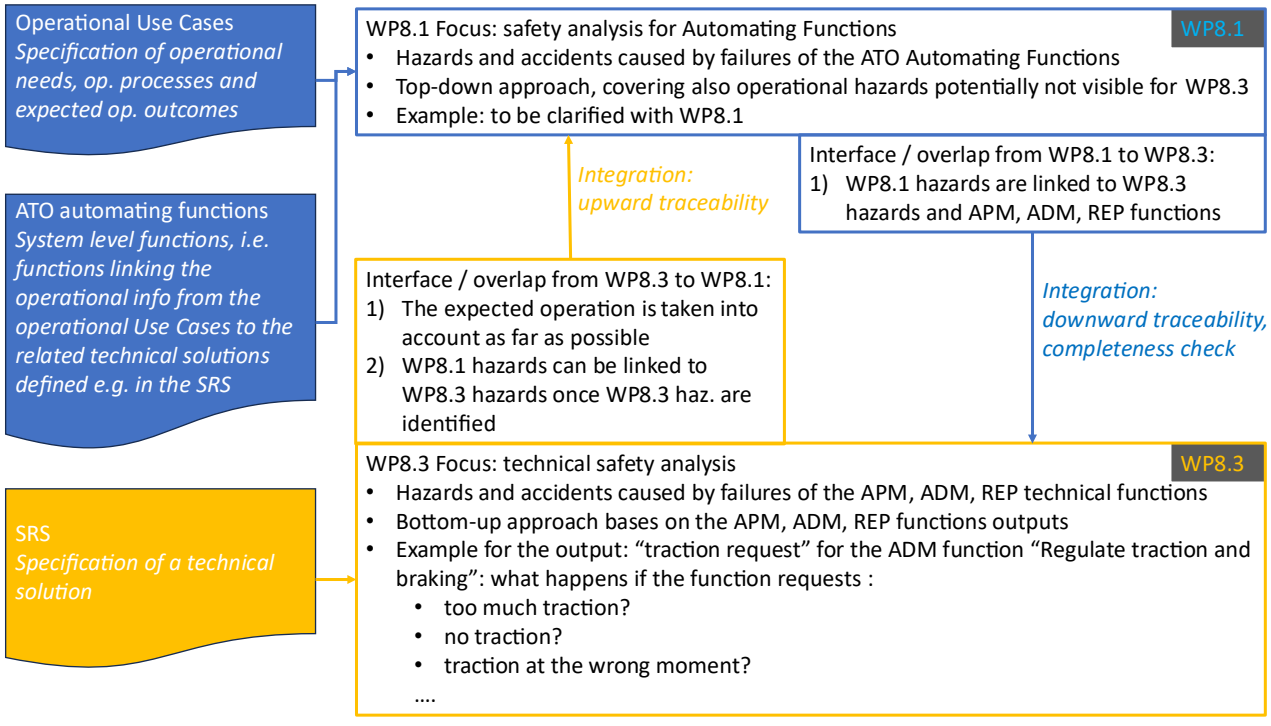

Figure WP8.3-WP8.1 Integration

ANNEX I. SAFETY ANALYSIS AND RISK EVALUATION

The document [19] contains the final Safety Analysis and Risk Assessment, documenting the Hazard identification and consequent Risk assessment of all functions allocated to APM,ADM and REP modules (see 4.2.1.1, 4.2.1.2, 4.2.1.3).

R2DATO_WP8.3_Functions_hazard_identifi