Contract No. H2020 – 101014984

TECHNOLOGIES FOR THE AUTONOMOUS RAIL OPERATION

D3.2 – Contribution to enhanced TCMS for automatic diagnostic functionality regarding autonomous train.

ATO running capability - Automatic monitoring and auto-recovery functions

Due date of deliverable: 31/05/2023

Actual submission date: 09/05/2023

Leader/Responsible of this Deliverable: Angelo Grasso

Reviewed: Y

Document status		
Revision	Date	Description
01	14/04/2023	Version ready for SC review.
02	09/05/2023	Final
03		
04		
05		

Project funded from the European Union’s Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	

Start date: 01/12/2020 Duration: 30 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (JU) under the Grant Agreement no. 101014984. The JU receives support from the European Union's Horizon 2020 research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Merve Nalbant	DB	Fire Protection Traction TCMS
Roland Luecker	ALSTOM	Internal and External Lights Auxiliaries Power Supply Low Voltage System Perception System Horn
Andreas Degenhardt	ALSTOM	Internal and External Lights Auxiliaries Power Supply Low Voltage System Perception System Horn
Denes Der	ALSTOM	Internal and External Lights Auxiliaries Power Supply Low Voltage System Perception System Horn
Angelo Grasso	FTI	Passenger Alarm Brake
Paolo Giraudo	FTI	Passenger Door Brake
Josef Schmucker	KB	Brake Air Generation and Treatment
Markus Fischer	KB	Brake Air Generation and Treatment
Josè Antonio Gimenez	INDRA	Communication between Train and Ground
Unai Irigoyen Marcuello	CAF SIG	ATO ATP Positioning System Communication between Train and Ground

Ales Lieskovsky	AZD	Perception System ATO
Francesco Inzirillo	MERMEC	ATO ATP Positioning System Communication between Train and Ground

DISCLAIMER

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

EXECUTIVE SUMMARY

CONTEXT AND OBJECTIVES

One of the new frontiers for railway market is the Train operation with no driver and no human assistance while Train is in daily service.

Enabling autonomous operation means that every system shall be re-designed to be able to manage by automatic procedure and by proper interfaces with the ground all the functionalities which currently are **operator related**.

The focus of the WP3 is on two diagnostic functionalities necessary to enable the autonomous operation:

- Testing of functionalities at the start of the mission
- Permanent diagnosis of the systems during the mission and degraded mode management in case of failure, compatible with the autonomous operation and the maximisation of the mission reliability

These functionalities are complementary to the current development of ATO and TCMS and refer to all the systems the rolling stock is composed of.

The subject of this document is the permanent diagnosis of the systems during the mission and degraded mode management in case of failure (auto-recovery)

If the main goal of the tests at the start of the mission is to guarantee the mission safety and reliability (see D3.1), **the main goal of permanent diagnosis and auto-recovery functions is the running capability.**

The permanent monitoring of the train functionalities permits to detect any fault which could impact the running capability or the safety as soon as it happens and to react accordingly in order to continue the run.

Permanent monitoring and auto-recovery functionalities are already implemented in GoA1/2 trains. Most of them can be handed over to autonomous train without big changes because already independent from the human support. The focus of this document shall be on the permanent monitoring and auto-recovery functionalities impacted by the transition to autonomous train.

Train systems, TCMS and ATO are all the systems impacted by the transition to autonomous train.

An impact analysis of the transition to autonomous train is already performed in D3.1 document and becomes the basis for the development of this document.

All the train systems are therefore supposed to be in the functional configuration consistent with the one defined in document D3.1 for autonomous train (including any new functionality there defined) and in a condition consistent with *successful test result* at the start of the mission.

Any failure impacting the mission reliability or safety can become active during the mission. The document D3.2 has the objective to analyse how the autonomous train shall react in case such failures become active and which new functionalities are required by TCMS and ATO to manage the situation. High level use cases are then defined for such cases, which can be taken as reference by WP that are currently developing new generation of TCMS and ATO for autonomous trains.

A functional approach is adopted, therefore the degraded condition which will be considered will refer to failure of “functions”, independently from the component that can be involved in that function.

The functions that D3.1 identifies as impacting the mission safety and reliability are the object of the analysis. In case of failure, the train shall recognize them and react with an auto-recovery procedure.

The contributors are therefore initially requested to extract from D3.1 document the functions impacting the running capability on autonomous train. The functions are split among safety related and mission failure.

As second step contributors are requested to identify the monitoring functions necessary to identify the above defined train functional failures impacting the running capability of autonomous trains. The identification is done by critical comparison between the existing diagnostic functions on GoA1/2 trains and the required ones for GoA3/4 trains, evidencing any update of them or adding of new ones.

The investigation of any safety requirement in case of failure of safety related function is also required.

The updated/new monitoring functionalities are formalized in use cases.

As third step the contributors are required to identify the auto-recovery functions necessary to react to the failures. The auto-recovery options considered for autonomous trains are the following, result of the adaptation of the GoA1/2 to GoA3/4 trains:

- Automatic reconfiguration of the system and mission continuation without restriction
- Automatic degraded condition activation and ending of the mission in restricted conditions
- Remote driving

Again, the identification is done by critical comparison between the existing auto-recovery functions on GoA1/2 trains and the required ones for GoA3/4 trains, evidencing any updating of them or adding of new ones. The transition impact is mainly replacing the manual operation with automatic ones or remote-controlled ones.

The remote control is the last option, if other possibilities by self-controlled train functions are not available.

The investigation of any safety requirement in case of failure of safety related function is also required.

The updated/new functionalities are formalized in use cases.

The train functionalities detailed analysis is conducted in independent way by each single contributor of the WP and periodically reviewed by other contributors.

A common analysis method has been defined, based:

- on the evaluation of functional failures impact on running capability and of monitoring capabilities of GoA1/2 trains
- on a critical analysis of consequences of the transition from GoA1/2 to GoA3/4 trains.

The critical analysis done by each contributor, according to the given method, lead to the following main results:

1) New monitoring functions

On board existing GoA1/2 monitoring functions are generally applicable to GoA3/4, new ones are necessary for new functionalities introduced due to transition to GoA3/4.

Autonomous train monitoring and remote monitoring by control centre are both considered.

In certain cases, adaptations or new tests to be executed at the start of the mission have been identified. These new tests integrate the tests identified during Task 3.1.

Innovative monitoring or auto-recovery solutions are also proposed (for example Broadcasting warning among the train to detect failed external light)

2) Auto-recovery solutions for GoA3/4 trains

Auto-recovery solutions already implemented in GoA1/2 are generally applicable to GoA3/4.

Redundant/single fault tolerant systems remain a standard solution implemented to mitigate the single failure impact on running capability.

New functionalities are identified to replace the driver and train crew role in managing the degraded conditions:

- On-board automatic reset or isolations or other autonomous auto-recovery actions
- Remote controlled reset or isolations or auto-recovery actions

3) Examples of new technologies which are proposed as auto-recovery solutions:

Back-up door closing and isolation system of passenger doors (passenger doors single failure resistant).

Passenger Emergency Egress device auto reset or remote controlled.

Remote controlled mechanical isolations (pneumatic cocks).

On board digital maps, used as an autonomous on-board positioning system to continue the mission or lead the train into a safe position or to the next railway station.

ABBREVIATIONS AND ACRONYMS

AC	Alternating Current
ACS	Adaptable Communication System
ADD	Automatic Drop Device
ATO	Automatic Train Operation
ATP	Automatic Train Protection
BC	Battery Charger
CB	Circuit Breaker
CTA	Connecta
DC	Direct Current
EmBr	Emergency Brake
EN	European Norm
ETCS	European Train Control System
FMECA	Failure Mode Effect Critical Analysis
GoA	Grade of Autonomy
HVAC	Heating Ventilation Air Conditioning
LIM	Limiter Switch (train protection switch)
LRU	Last Replaceable Unit
LV	Low Voltage
MCB	Main Circuit Breaker
N.A.	Not Applicable
OCC	Operative Control Centre
PAD	Passenger Alarm Device
PC	Personal Computer
SIL	Safety Integrity Level
SoA	State of the Art
SW	Software
TAURO	Technologies for the AUtonomous Rail Operation
TBC	Traction/Brake Controller
TCMS	Train Control and Monitoring System
THL	Train Heating Line
THR	Tolerable Hazard Rate
TSI	Technical Specification of Interoperability

VAC	Volt AC (unit to measure AC voltage)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The objective of the document is to define the TCMS and ATO new functionalities necessary to manage functional failures impacting the running capability of autonomous train.

Autonomous train new functionalities defined in document D3.1 (result of the impact analysis of transition from GoA1/2 trains to GoA3/4 trains) are considered as well.

Even if the autonomous train has passed all the tests at the start of the mission defined in document D3.1, any failure can happen during the mission impacting the running capability.

This document investigates which can be the possible reaction in such a case to guarantee the running capability (automatic recovery, degraded condition operation, remote driving) and make a critical analysis of TCMS and ATO new functions eventually necessary.

High level use cases are defined, which can be taken as reference by WP that are currently developing new generation of TCMS and ATO for autonomous trains.

The document is organized as follow:

In chapter 2 the context of autonomous train is described, specifying the reference communication and control architecture considered; the justification of the train functions analysed is provided, referring to former task 3.1 output and work splitting; the rationale adopted to arrive at the definition of the main outputs of the document (new monitoring functions and auto-recovery solutions) is defined

In chapter 3 a general analysis method is defined, with clear decision point definition, in order to provide a common way of working for all contributors analysing single functionalities according to the split of work defined before

Chapter 4 collect the critical analysis of every function defined in chapter 2 in accordance with the method described in chapter 3. The output for each function is a collection of new monitoring or new auto-recovery use cases.

In chapter 5 the main results derived from the contribution are summarised and relevant outcomes underlined.

2 CONTEXT

The general context for the management of an autonomous train is shown in the following picture.

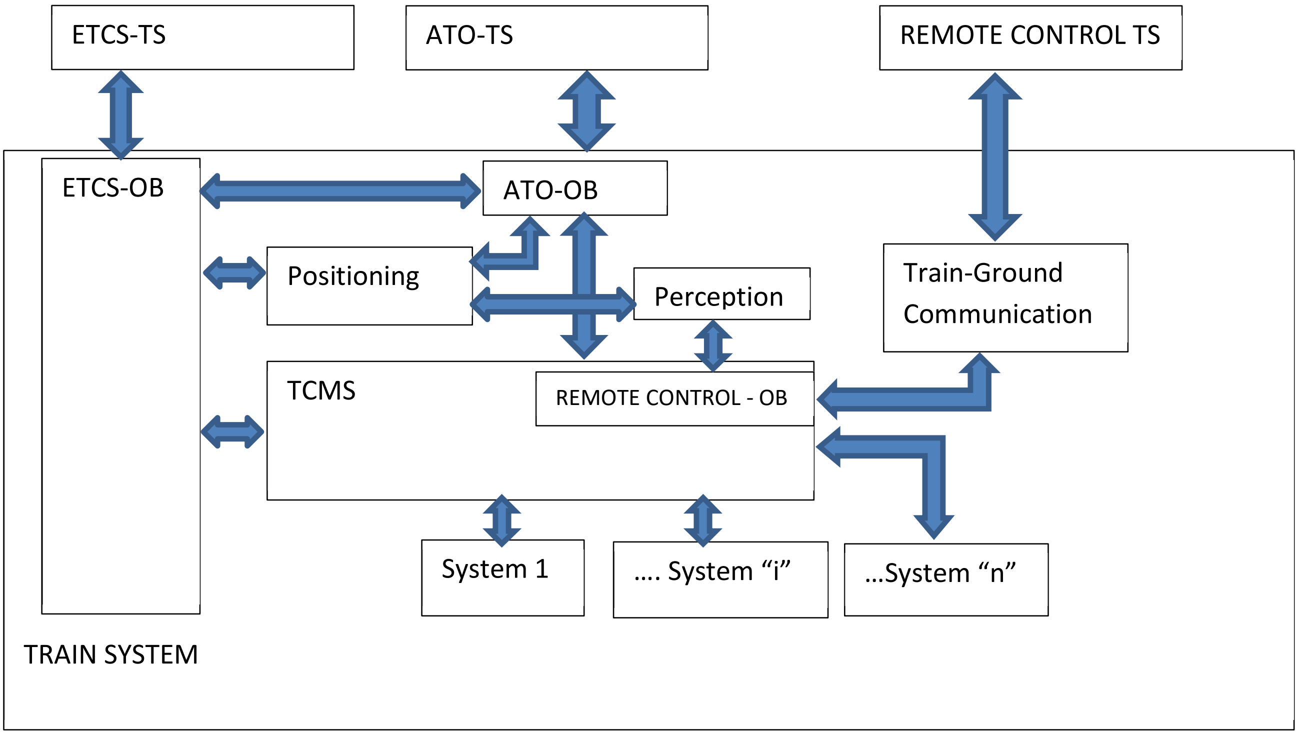


Figure 1 – Autonomous train context

- Train system: it includes all sub-systems performing the different functionalities required for train operation,
- ETCS system (ground and on-board): it is in charge of the safe integration of the train in the network,
- ATO system (ground and on-board): it is in charge of automatic train operation in normal condition.
- Remote control system (ground and on-board): it is in charge of remote-controlled train operation. It is composed of Track side control, part of the operative control centre (OCC) and of On-Board side, which is supposed to be integrated inside TCMS. The communication between TS and OB is done by Train Ground communication, in addition to all the other train-ground data communication.
- TCMS: it is in charge of the integration of all the train functionalities, collection of all system diagnosis and of the train management of degraded mode in case of failure.

Note 1: "Positioning" system can alternatively be an integrated part of the ETCS in specific design solutions

Note 2: ATO considered interface concept is the one described in document D3.1 and here below reported, where DMI is external to the ETCS OB, communicating via Subset 121.

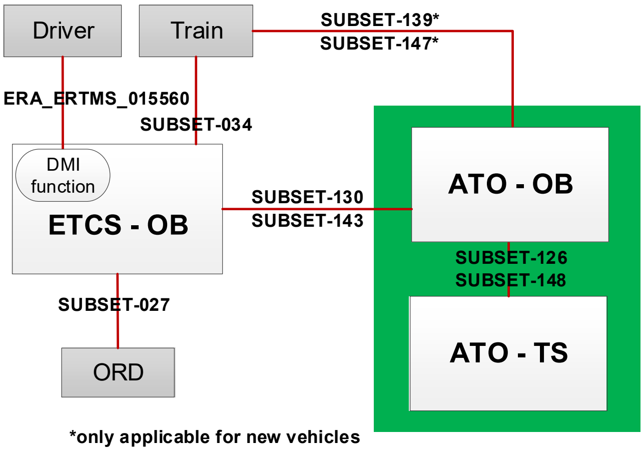


Figure 2 - ATO interface concept

The communication sub-sets there defined are considered. If the analysis recognizes the necessity to update them it is evidenced formally.

The running capability is affected by loss of functionality on any function essential for the train run.

A functional FMECA is generally performed to identify these failures.

During the development of D3.1 contribution an high level functional FMECA has been conducted, analysing all the train functions defined in EN15380-4 and identifying the ones affecting the train safety and the mission reliability because this was the criteria driving the choice of functional test to be performed at the start of the mission (the test at the start of the mission has the goal to guarantee that the train is as much as possible reliable and the mission can be completed without problems).

Not all identified functions are tested before the start of the mission for different reasons, but all those functions could fail during the mission.

The D3.1 document also analysed the impact of transition from GoA1/2 trains to GoA3/4 trains, evidencing any new functionalities necessary to manage the autonomous train.

The D3.1 document therefore provides a quite complete set of train functions to be analysed in terms of monitoring and auto recovery actions. Chapter 0 summarises the results of D3.1, preparing the basis for the development of this document.

Some considerations about functions monitoring are done in chapter 2.2, because the monitoring is a key sub-function for the management of the running capability.

An overall management strategy in case of major failure to any of the 3 communication channels between train and Ground is defined in chapter 2.3 and shall be taken in consideration in the analysis of each single system failure

2.1 AUTONOMOUS TRAIN FUNCTIONS

The functionalities identified in D3.1, derived from EN15380-4, are considered.

In below table they are listed with the main related systems in charge of the single functions.

EN15380-4 ID	FUNCTION	MAIN RELATED SYSTEMS
B E	Protect against fire	Fire protection (chapter 4.1)
C C	Provide external view	External Lights (4.2)
C D	Provide interior lighting	Internal Lights (4.2)
C F D a	Manage alarm from passengers	Passenger Alarm (4.3)
C F F a C	Provide passenger alarm intercommunication	Passenger Alarm (4.3)
D B	Provide external access functions associated with the management of the external doors	Doors (4.4)
F B	Provide electrical energy for traction	Pantograph (4.5)
F C	Provide electrical energy for auxiliaries- Manage electrical auxiliary energy provisioning configure the auxiliary power supply system	Auxiliary Power supply (4.6) Low Voltage System (4.7)
F E	Provide fluid energy for auxiliaries fluid energy refers to hydraulic/pneumatic media	Air supply and Treatment (4.8)
G B	Provide acceleration	Traction (4.9)
G C	Provide deceleration and keep the train at standstill (dynamic brake force included)	Brake (4.10)
G D a	Improve adhesion	Sanding (4.10)
K B	Indicate the presence of the vehicle to others persons and other vehicles (e. g. pedestrians, car drivers)	External Lights (4.2) Horn (4.11)
K D	Provide operational communication and train/ground data transmission	Communication between train and ground (4.12)
K E	Provide Automatic Train Control (ATC)	ATO (4.13) ATP (4.14) Positioning (4.15) Perception (4.16)

Table 1 –Functions list

TCMS performs or contributes to controlling and monitoring several train functions. The failure of TCMS, intended as HW and SW system, therefore, can impact several of the above functions. For this reason, TCMS, intended as system, is also part of the analysis, as it was in D3.1. The failure of the control and monitoring of each function is instead part of every main function analysis.

EN15380-4 ID	FUNCTION	MAIN RELATED SYSTEMS
	Communication among train systems and train management of SW logics	TCMS (4.17)

The functionality *Degraded scenario management* introduced in D3.1, as per TCMS, is a sub-function of all main functions. It is one of the 2 objects of the D3.2 document (diagnosis and auto recovery), and therefore it is convenient not to consider as separate function, but to be part of every main function analysis.

The functionalities *On-board test results automatic management* and *non-automatic management (from ground station)* are strictly linked to the management of the test at the start of the mission, therefore are no more considered.

Based on above considerations the list of main functionalities/systems analysed in D3.1 are mostly confirmed. It is also confirmed, for similarity, the relation between functions and main system and therefore the chapters titles referring to the systems instead than functions.

The D3.1 safety and reliability impact critical analysis of all the main functions are considered to identify the failures to be monitored and auto recovered.

Part of this critical analysis is also the definition of new functionalities necessary to manage the mission of autonomous trains. They are considered as well.

All functionalities shall comply of course with EN50553 standard, guaranteeing the running capability in case of fire on board. Any new functionality that shall be introduced due to the transition to GoA3/4 shall be developed accordingly. The development of the new functionalities is not scope of this document.

The work is split among all the contributors according following Table 2, derived from task 3.1 work splitting.

Contr. ID	Resp.	Reviewer.	Contribution	Chapter
D3.2_1	DB	ALSTOM	Fire Protection	4.1
D3.2_2	ALSTOM	DB	Internal and External Lights	4.2
D3.2_3	FTI	ALSTOM, SNCF-V	Passenger Alarm	4.3
D3.2_4	FTI	KB	Passenger Door	4.4
D3.2_5	DB	ALSTOM	Pantograph	4.5
D3.2_6	ALSTOM	DB	Auxiliaries Power Supply	4.6
D3.2_7	ALSTOM	DB	Low Voltage System	4.7
D3.2_8	KB	FTI	Air Generation and Treatment Unit	4.8
D3.2_9	DB	ALSTOM	Traction	4.9
D3.2_10	KB	FT	Brake	4.10
D3.2_11	ALSTOM	DB	Horn	4.11
D3.2_12	INDRA	MERMEC, CAF SIG	Communication between Train and Ground	4.12
D3.2_13	CAF SIG	AZD, MERMEC	ATO	4.13
D3.2_14	CAF SIG	MERMEC	ATP	4.14
D3.2_15	CAF SIG	MERMEC	Positioning System	4.15
D3.2_16	ALSTOM	CAF SIG, AZD	Perception System	4.16
D3.2_17	DB	ALSTOM	TCMS	4.17

Table 2 – Scope of work splitting among contributors

2.2 FUNCTIONS MONITORING RATIONALE

The train functions monitoring is a functionality already well developed in GoA1/2 trains, detecting failures (generally till the LRU) and performance out of the nominal ones. In these cases diagnostic messages and/or alarms are generated and, when necessary, automatic reaction activated. Monitoring output can be used:

- to organize the maintenance activity as soon as the train arrive in the depot and have 100% train functions always available
- to activate automatic reconfiguration of the train which recover totally or partially the functionality/performance, waiting for the maintenance
- to inform the driver about failures affecting the safety of the mission, so that he put in place the necessary action to continue the mission without safety problems.

- to inform the driver about failures affecting the nominal functionality of the systems, so that he put in place the necessary actions to continue the mission without problems or to isolate the function in failure.
- To transmit environmental data to recorder or to ground to collect information for CBM or another database.

The transition to autonomous train doesn't introduce new rationales on monitoring.

The difference can be that monitoring data transmitted to the driver and influencing the train driving in autonomous train shall be used by ATO or by remote control to drive the train and that new functions monitoring are necessary.

In this document monitoring essential to manage the running capability are considered only.

2.3 AUTO-RECOVERY RATIONALE

On not autonomous train the consequences of failures of any train's function are generally the following:

- The function is not safety related:
  - certain performances are reduced but remain in an acceptable level.
    The train mission is not affected by the failure.
    No actions are put in place and the failure is repaired when the train is in depot.
  - certain performances are reduced below an acceptable level.
    The train mission is affected by the failure (traction cut-off, speed reduction, stopping, ….)
    Actions are put in place to recover the function at least till an acceptable level of the performances:
    - automatic: reconfiguration/isolation of the system at the activation of the failure
    - manual: redundancy activation/isolations/bypass by operator

    If the recovery is not possible the train rescue could be necessary or the stop of the mission at the next station/safe location
- The function is safety related:
  - certain performances are reduced but remain in an acceptable level in terms of safety:
    - the time to hazard is reduced at a still acceptable level to continue the mission.
      The train mission is not affected by the failure.
      No actions are put in place and the failure is repaired when the train is in depot.
    - The time to hazard is reduced below an acceptable level to continue the mission.
      The train enters in a safe state (traction cut-off, speed reduction, stopping, door closing, fresh air damper closing, ventilation switching off, …)
      Actions are put in place to exit from the safe state and recover an acceptable level of safety to continue the mission or to end the run and then train is removed from the service.

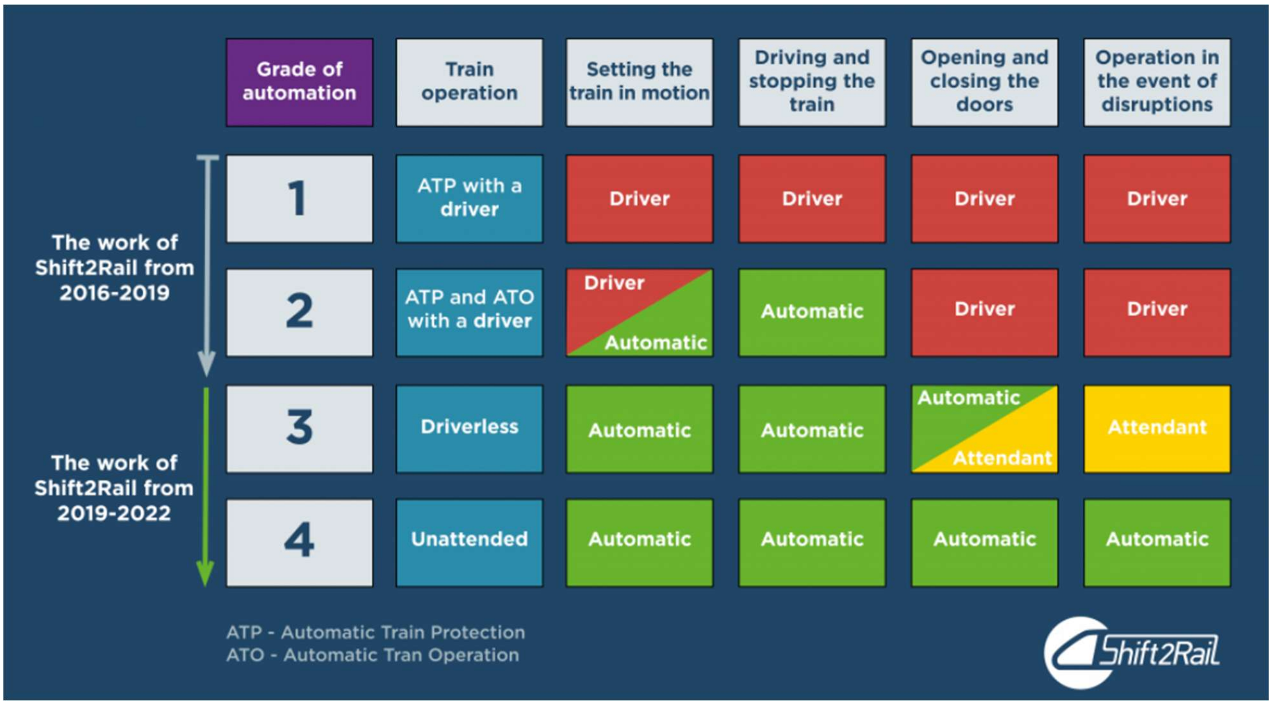
- automatic: reconfiguration/isolation of the system at the activation of the safe state
- manual: redundancy activation/isolations/bypass by operator

- certain performances are reduced below an acceptable safety level.
  The train is immediately stopped.
  Once the train is stopped, only manual actions are put in place to permit the train again to move.

If the recovery is not possible the train rescue could be necessary or the stop of the mission at the next station

The transition to autonomous train should permit to carry over the automatic recovery actions but introduces the necessity to replace the manual operations with automatic ones or to be remotely controlled.

For reference here after the concept used in Shift 2 Rail in relation to GoA1/2/3/4 trains differences:



	Grade of automation	Train operation	Setting the train in motion	Driving and stopping the train	Opening and closing the doors	Operation in the event of disruptions
The work of Shift2Rail from 2016-2019	1	ATP with a driver	Driver	Driver	Driver	Driver
	2	ATP and ATO with a driver	Driver Automatic	Automatic	Driver	Driver
The work of Shift2Rail from 2019-2022	3	Driverless	Automatic	Automatic	Automatic Attendant	Attendant
	4	Unattended	Automatic	Automatic	Automatic	Automatic

ATP - Automatic Train Protection
ATO - Automatic Tran Operation

Figure 3 - Train grades of automation

This document considers the worst case of GoA4, which requires all automated reactions to any failure.

The train operation hypothesis considered in this document are the following:

ETCS manages the train safety and the ATO manages the normal train operation during the mission. In case one or both the systems are not operative the control centre can manage the train by the Remote-Control system in accordance to project specific safety procedures and national relevant degraded mode operation procedures.

In case of ETCS or ATO failure, the auto-recovery is remotely controlled by Control Centre via the Train-Ground communication system. The reaction hypothesis to disrupted train-ground communication are the following

- ETCS-TS vs ETCS-OB system/communication failure: the train is immediately stopped and the ground takes the control of the train by Remote control. This means that Remote control and ETCS functionality are independent,
- ATO-TS vs ATO-OB communication failure: the train goes into a degraded mode (TBD) and the ground takes the control of the train by Remote control. This means that Remote control and ATO system functionalities are independent (no common cause failures or single fault resistant)
- RC-TS vs RC-OB communication failure: the trains can continue normal operation until a second failure disrupting ETCS or ATO system will occur. When such a failure happens in addition to the remote-control failure the train is no more capable to be auto-recovered

Case by case functional failures analysis is the goal of the document, considering the above train operation hypothesis and train - ground communication failure management hypothesis.

3 ANALYSIS METHOD

As mentioned above, the D3.1 already provided a new functional configuration of the autonomous train, composed of EN15380-4 functions and new functions identified. This configuration shall be considered in the analysis method.

For each of the above groups of functions the following analysis is done:

- Sub-functions running capability impact analysis

  Review of the D3.1 document with the goal to list the functions and sub-functions impacting the running capability

  Filtering of the failures between safety related and mission failures.

  - Safety related functional failures: failure activating safe state impacting the running capability (traction, braking, door locking, fire protection or passenger alarm availability, …)
  - Mission functional failures: failures interrupting the traction capability of the train or the passenger transportation (door no more opening, …)

- Sub-functions monitoring capability analysis

  check of the monitoring availability on not autonomous train of the above identified functional failures impacting running capability.

  The monitoring capability analysis is done considering single failures only.

  - Yes: critical evaluation if it can be re-used or adapted to autonomous train (in such a case use case to be prepared)
  - No: new use case to be defined to describe the new monitoring function for autonomous train

  A critical analysis about any particular safety requirement is required for the diagnosis of *safety* relevant functional failure to be performed.

- Sub-functions failure auto-recovery capability analysis

  check of the auto-recovery capability availability <u>on not autonomous train</u> of the above monitored functional failures

  - Yes: critical evaluation if it can be re-used or adapted to autonomous train
    - Auto-recovery requiring operator action -> adaptation needed
      - Self recovery possible: new use case to be defined involving systems, TCMS
      - Remote control necessary: new use case to be defined involving systems, TCMS, ATO-OB, ATO-TS (eventually ETCS)
    - Auto-recovery not requiring operator action-> existing solution confirmed
  - No: new use case to be defined to describe the new auto-recovery function of autonomous train
    - Auto-recovery by self-controlled train functions involving systems, TCMS

- Auto-recovery requiring remote control involving systems, TCMS, ATO-OB, ATO-TS (eventually ETCS)

Evaluation of the new monitoring function defined in former chapter

- Auto-recovery by self-controlled train functions involving systems, TCMS
- Auto-recovery requiring remote control involving systems, TCMS, ATO-OB, ATO-TS (eventually ETCS)

In all cases a critical analysis about any particular safety requirement is required for the auto-recovery process of safety relevant functional failure to be performed.

○

4 GOA3/4 AUTOMATIC FUNCTIONAL TESTS AT THE START OF THE MISSION

4.1 Fire Protection System

Main function “B E Protect against Fire” is realized in autonomous train by the implementation of the sub-functions of Fire protection system below:

B E B Manage / Provide smoke detection
B E C Manage / Provide fire detection
B E D Manage signaling of fire
(management of fire alert (system), fire warning
(system), notification of fire)
B E E a Manage / Provide fire extinguishment
B E E a Manage automatical fire extinguish system
B E E a Monitor volume of extinguishing agent
B E E a Provide manual fire extinguish facilities

4.1.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Manage / Provide smoke detection	YES	Failure of this function is at local level. Failure of the occurrence of any kind of fault of the fire control system or fire control unit which prevents smoke or fire detection and/or fire extinction (even partially).. Manage & provide smoke detection is safety relevant in relation to the fire protection system, because in GoA3/4 no driver is on the train and the fire protection system should observe its own. Train should be stopped.	safety
Manage / Provide fire detection	YES	Failure of this function is at local level.	safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		Manage & provide fire detection is safety relevant in relation to the fire protection system, because in GoA3/4 no driver is on the train and the fire protection system should observe its own. Fire detection is not available. Train should be stopped.	
Manage signalling of fire	YES	Failure of this function is at local level. Manage signalling is safety relevant in relation to the fire protection system, because in GoA3/4 no driver is on the train and the fire protection system should observe its own. Failure of fire warning system. Train should be stopped.	safety
Manage / Provide fire extinguishment	YES	Failure of this function is at local level. Manage & provide fire extinguishment is safety relevant in relation to the fire protection system, because in GoA3/4 no driver is on the train and the fire protection system should observe its own. Fire extinguisher could not be activated. Train should be stopped.	safety
Manage automatically fire extinguish system	yes	Failure of this function is at local level. This function already compatible with GoA3/4 since it is managed automatically without driver control. Automatic extinguisher could not be activated. Train should be stopped.	safety
Monitor volume of extinguishing agent	NO		
Provide manual fire extinguish facilities	NO		

Table 3 – Fire protection running capability impact critical analysis

4.1.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Manage / Provide smoke detection	yes	The monitoring of fire control unit is done on GoA1/2 train by driver because the failures are safety relevant. **Safety impact:** The risk of injuries to crew, passenger and train itself in case of safety relevant fault are generally mitigated by highly reliable components or single fault tolerant architecture or SIL2 sw functions (high integrity) or by single fault leading to the safe state condition. Automated action needed for GoA3/4	yes
Manage / Provide fire detection	yes	The monitoring of fire control unit is done on GoA1/2 train by driver because the failures are safety relevant. **Safety impact:** The risk of injuries to crew, passenger and train itself in case of safety relevant fault are generally mitigated by highly reliable components or single fault tolerant architecture or SIL2 sw functions (high integrity) or by single fault leading to the safe state condition. Automated action needed for GoA3/4	yes
Manage signalling of fire	yes	The monitoring of fire control unit is done on GoA1/2 train by driver because the failures are safety relevant. **Safety impact:** The risk of injuries to crew, passenger and train itself in case of safety relevant fault are generally mitigated by highly reliable components or single fault tolerant architecture or SIL2 sw functions (high integrity) or by single fault leading to the safe state condition. Automated action needed for GoA3/4	yes
Manage / Provide fire extinguishment	yes	The monitoring of fire control unit is done on GoA1/2 train by driver because the failures are safety relevant. **Safety impact:** The risk of injuries to crew, passenger and train itself in case of safety relevant fault are generally mitigated by highly reliable components or single fault tolerant architecture or SIL2 sw functions (high integrity) or by single fault leading to the safe state condition.Automated action needed for GoA3/4	yes

Table 4 – Fire protection system monitoring function critical analysis

4.1.3 New/Upated monitoring function use cases

Use Case	Failure of B E sub-function
ID	UC4.1.1
Actors	Remote Driver, TCMS, fire protection system
Goal	Enable remote actions in case of failure of fire protection system sub-functions
Safety relation	Yes
Precondition	Fire protection system failed
Flow of events	1. TCMS sends train diagnostics of fire protection system 2. Remote Driver observes the failure. 3. Remote Driver decides further steps such as -Lock out the system (doors, etc.) -Lock out the brake system of bogie -Stop Train or move to a safe position -Reduce speed -Reroute the track or speed limitation -Rescue Passengers -Call fire department -Provide information to the passengers -Inform other trains on the track
Post condition	Remote Driver / TMCS informed Fire Protection system needs to be repaired / replaced and tested.
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 5 – Fire protection system failure new monitoring use case

4.1.4 Auto-recovery functions critical analysis

Depending on the failure a reset of the fire protection system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.

4.1.5 New/Upated auto-recovery function use cases

Use Case	Reset of B E sub-function
ID	
Actor	remote driver
Goal	Reset the fire protection system
Safety relation	yes
Precondition	Faulty on sub functions
Flow of events	- Send status of fire protectin system to remote driver - Send the diagnostic data to remote driver - Wait for commands from remote driver. - Remote driver reacts action for system configuration and/or restarts the system
Post condition	Sub functions
Things that can go wrong	Failure remains
Already implemented risk reduction measures	
Observations	

Table 6 – Fire protection system reset use case

4.2 INTERNAL AND EXTERNAL LIGHTS

Main function “Manage illumination system” is realized in autonomous train by the implementation of the here below sub-functions, where new-*n* are the new function which D3.1 introduce as possible impact of the transition to GoA3/4:

The following sub-functions of EN15380-4 are involved by internal and external lights test:

•	C	C	C	a	Provide view in the darkness by illumination of the track and reflective signals by headlights
•	C	D			Provide interior lighting
•	C	D	B	a	Provide workplace lighting
•	E	B	B	a	Manage exterior lights in coupled mode
•	H	E	J	a	Manage exterior lighting
•	K	B			Indicate the presence of the vehicle to others

New-1 broadcast warning system on railway system level – to warn other trains.

The back-up illumination system includes the following sub-functions:

a. *Detection of failing lamps of illumination system*
b. *Provide warning system on railway system level*

4.2.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	**RUNNING CAPABILITY IMPACT**		**MISSION/SAFETY FAILURE**
*External front light - **one** fails*	NO	This is a function failure on locomotive or consist level. Today by design three separated front lights are installed (in A form) distant away from each other. The probability is low that all lights are impacted by demolition or dirt at the same time. Further driving should be possible with reduced speed (e.g., 40 km/h) till next railways station for inspection/mitigation.	Safety
*External front lights - **all** fails*	YES	If the failure is at local level, then external front light (in driving direction of train) is not providing illumination. No mitigation is foreseen with today design. Mitigation is possible only	Safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		with additional independent redundant lights. Further driving should be possible with low speed (e.g., 20 km/h) till next railways station for inspection/mitigation. Warning must be issued on railway system level, to warn other trains running in surrounding area of impacted train.	
***One** external rear light fails – vehicle alone or as last vehicle in train*	NO	This is a function failure on vehicle level. Today by design two separated rear lights are installed distant away from each other, which make simultaneous damage probability neglectable. Further driving should be possible till next railways station for inspection/mitigation. Warning must be issued on railway system level, to warn other trains running in surrounding area of impacted train.	Safety
***Both** external rear light fails – vehicle alone or as last vehicle in train*	YES	This is a function failure on vehicle level. No mitigation is foreseen with today design. Mitigation is possible only with additional independent redundant lights. Further driving with **no reduced** speed should be possible till next railways station for inspection/mitigation. Warning must be issued on railway system level, to warn other trains running in surrounding area of impacted train.	Safety
*Interior lighting fails – **one** lighting fails in one coach*	NO	This is a function on coach level.	Safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		Passenger coaches are equipped with multiple lights and emergency lights. So, fail of one light will reduce the performance of internal lighting, but will provide enough illumination, so not cancel the illumination functionality. Beside diagnostics entry no further actions are needed on mission.	
*Interior lighting fails – **whole coach** lighting fails*	NO	This is a function on coach level. In case of full fail of lights in one passenger coach, depending on external light (when it is dark) the passenger should be warned by acoustic and text massage to move to the next coach (with correct lighting). Warning inside an outside the coach should be placed to avoid re-occupation of the coach with faulty lights by new passengers. The mission can be continued	Safety
*Interior lighting fails – **whole train** lighting fails*	YES	This is a function failure on train level. In case of full fail of lights in all passenger coaches, thus on whole train, depending on external light (when it is dark) the passenger should be warned by acoustic and text massages to remain at place. At daylight mission could be continued till next railway station, else the train should cancel the mission.	Safety
Workplace lighting fails	NO	This is a function failure on vehicle level. Because in GoA3/4 no driver will be physically present, the workplace lighting seems to have no function.	No safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		However, if workplace is remotely monitored by cabin internal camera, then illumination can be an issue. Assuming all controls, indicators and displays are sensed anyhow, then this illumination fail would be not an issue. At normal daylight conditions (with not to low light conditions) the workspace illumination is not needed.	

Table 7 – Internal and external lights system running capability impact critical analysis

4.2.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Switch external lights on	YES	Independently from the technical solution used, the monitoring of the release command is done on GoA1/2 train because the failure is safety relevant. Also, at local level consistency checks are done for each diagnostic system to detect any local failure. **Safety impact:** The risk of hazard of train in case of fault is always mitigated by single fault resistant architecture of electronics. The light functions are monitored by plausibility check of voltage and current values during ON state.	NO
Check illumination level	NO	This is done during the mission by the vehicle driver – who will be not available during GoA3/4 driving.	YES

Table 8 – Internal and external lights system monitoring function critical analysis

4.2.3 New/Updated monitoring function use cases

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Activate external front lighting: ***No external front available - on one light***	The GoA1/2 external lighting system is resistant to this type of failure (single fault), with UIC light pattern - 2 other lights remain - no need of auto-recovery function. Warning must be issued to other trains – because function "Indicate the presence of the vehicle to others" is not given anymore. Drive till next railway station.	YES
Activate external front lighting: ***No external front lighting available - on all lights***	No backup system in GoA1/2 on the lights foreseen. Warning must be issued to other trains – because function "Indicate the presence of the vehicle to others" is not given anymore. Function "Provide illumination of track and signals" in not given anymore, so adaptation depending on environmental light, e.g., during daylight a mission can be continued with reduced speed till next railway station, but in dark environmental conditions the mission must be aborted.	YES
Activate external rear lighting: ***No external rear available - on one light***	The GoA1/2 external lighting system is resistant to this type of failure (single fault), with the UIC light pattern - one other lights remain - no need of auto-recovery function. Drive till next railway station.	NO
Activate external rear lighting: ***No external rear available - all lights fail***	At daylight replacement of train rear lights are possible with signal tables – which are manually placed at last coach. For GoA3/4 this would be no option – here additional redundancy could be introduced (additional backup rear light) in combination with warning broadcast to following trains to command them to reduce maximal speed. Drive till next railway station.	YES

Table 9 – Internal and external lights system new monitoring use case

4.2.4 Auto-recovery functions critical analysis

As per above critical analysis there is new uses cases to be defined to facilitate the auto-recovery of a GoA3/4 train in case of failure to the activate external front lighting function failure:

- Broadcast warning on railways system in case of all lights fail of front or rear lighting to warn all other trains.
- In case of daylight conditions continue mission with reduced maximal speed till next railway station should be possible.
- Add redundant illumination to rear light system.

4.2.5 New/Updated auto-recovery function use cases

Use Case	***External Front Lighting Broadcast Warning***
ID	***UC4.2.1***
GUID	*65939BCF-70FA-48B1-A432-8FB6898CD2F6*
Actor	*Our train, Control centre, other trains in region*
Goal	*Warn trains in region that our trains presence indication is degraded or missing*
Safety relation	*Yes*
Precondition	*Presence indication by external front lighting degraded or not available*
Flow of events	*1. Failure of one or all front lights* *2. Status committed to control centre* *3. Control centre issues warning to affected other trains running in region* *4. All trains reduce speed till our faulty train is on track* *5. Our trains leave track* *6. Broadcast warning can be lifted*
Post condition	*All trains in region are warned to reduce speed*
Things that can go wrong	*Warning does not reach all affected trains*
Already implemented risk reduction measures	*New function*
Observations	*Function would be like KOLIBER system used in Poland.* *KOLIBER is triggering via train-radio EmBr for all trains in defined region.*

Table 10 – External Front Lighting Broadcast Warning new auto-recovery use case

Use Case	***External Front Lighting Failing - on all lights***
ID	**UC4.2.2**
GUID	4A754CBC-A087-4061-8D9D-53F94E456ABA
Actor	Our Train, Control centre
Goal	Bring train till to the next railways station
Safety relation	yes
Precondition	No external front lighting available
Flow of events	1. Failure of all front lights 2. Broadcast Warning to all trains in region 3. Our train reduce speed till we are on main track 4. Our train approaches next railway station 5. Our train aborts mission on secured track 6. Broadcast warning can be lifted
Post condition	Train must be inspected – lights must be repaired and positively tested
Things that can go wrong	Failing lights are not detected, or not timely Presence indication of train is not provided anymore.
Already implemented risk reduction measures	Electronics of light control is redundantly built up. Multiple lights showing presence of train. Lights are permanently monitored for proper operation by voltage and current consumption,
Observations	Monitoring, and plausibility checks of changes in light intensity to be considered by either additional light sensors or camera picture evaluation.

Table 11 - External Front Lighting failure new auto-recovery use case

Use Case	*External Rear Lighting Failing - on all lights*
ID	**UC4.2.3**
GUID	EE654B43-56B0-4842-9CA9-5F3DF2872C51
Actor	Train
Goal	Bring train till to the end of mission
Safety relation	yes
Precondition	No external rear lighting available
Flow of events	1. Failure of rear lights 2. Switch over to redundant rear lighting system 3. Continue mission 4. After mission finish check/repair primary rear lighting system
Post condition	Train must be inspected – lights must be repaired and positively tested
Things that can go wrong	Failing lights are not detected, or not timely Presence indication of train is not provided anymore.
Already implemented risk reduction measures	Electronics of light control is redundantly built up. Multiple lights showing presence of train. Lights are permanently monitored for proper operation by voltage and current consumption,
Observations	Monitoring, plausibility check of changes in light intensity to be considered by either additional light sensors or camera picture evaluation.

Table 12 - External Rear Lighting failure new auto-recovery use case

4.3 PASSENGER ALARM SYSTEM

Main function “Manage emergency alarm from passengers” is realized in autonomous train by the implementation of the here below sub-functions (see document D3.1 chapter 4.3).

CFDaA – Manage alarm requests from passengers

CFDaB – Manage passenger alarm request

CFFaC – Provide passenger alarm intercommunication (which is a subfunction of the passenger information system)

Note: Document D3.1 didn’t consider passenger - driver communication function in case of alarm among the ones impacting the reliability or the safety of the mission because today TSI (GoA1/2 based) don’t define hazard scenario for it (TSI chapter 4.2.5.2).
For this reason, CFFaC subfunction was not considered safety related, but the alarm request only (TSI 4.2.5.3), having safety requirement (4.2.5.3.5)
Revision of the actual TSI hypothesis due to the transition to GoA3/4 should be considered if the communication with the passenger in case of alarm request will be considered safety related in GoA3/4 trains (and function CG “Provide surveillance” as well).
Of course, the main functions CFD “Manage emergency alarm from passengers” and CG shall be integrated in autonomous or remotely driven trains with the function KDC “communication train – to ground” of chapter 4.12

The document D3.1 chapter 4.3.1 and 4.3.2 analysis of transition to GoA3/4 evidenced the following impacts related to main function “Manage emergency alarm from passengers”:

- When permitted, brake override command shall be managed by remote control in a very restricted time after alarm request (within 10s).
- Passenger alarm request reset shall be managed by remote control.
- Passenger alarm system shall guarantee a sufficient reliability OR any safety relevant failure shall move the system into a safe state corresponding to degraded condition compatible with the running capability OR local passenger alarm device isolation shall be remote controlled.

4.3.1 Functional failure impacting running capability

Taking as reference the above conclusions of the document 3.1, the functional failure critical analysis is defined in next table, taking as hypothesis that the system is compliant with the section 9 of the EN16334_1+A1:2022

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Manage alarm request from passenger	YES	This is a function managed both at local level (alarm request generation by passenger) and train/ground level (transmission of the alarm from the passenger to the central control, acknowledgement signal from the central control to the train, automatic braking by the train or override of the automatic braking. Failures at local level (PAD) - Missing alarm request: another device shall be operated by passenger. - Undue alarm request: parallel information available to the OCC (images by the on-board cameras, …) permit the OCC to acknowledge the alarm and override the automatic braking. OCC can reset or isolate local device giving wrong alarm, if possible, to diagnose it (isolation not allowed by remote control by existing standard, see new function proposal in document 3.1) and continue with the mission The running capability is not affected, it is always possible to continue the mission at least till the next station. Failures at train level, like faulty transmission of the signal from passenger to train - ground communication, faulty train-ground alarm communication: - Missing alarm to the ground: OCC is not informed and therefore cannot acknowledge the alarm when necessary. The brake is applied automatically. The running capability is impacted. It has also a safety impact (OCC cannot override the brake whenever is necessary) - Permanent/undue alarm request: the permanent diagnosis (crosscheck with local PAD status) and parallel information available to the OCC (images by the on-board cameras, …) allow the OCC to manage the impact of the failure and to avoid impact on running capability and safety **Safety**: As written above, failure in transmitting the alarm request is one of the hazards considered by TSI. The system shall be designed to comply with the safety level required by TSI.	Mission/Safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Manage passenger alarm request	YES	The passenger alarm request management involve two separate sub-functions: the alarm acknowledgement by OCC and the automatic brake application or override by the train. Failure of alarm acknowledgement: - Missing acknowledgement: the brake is applied automatically impacting the running capability and the safety (OCC cannot override the braking when required) - Undue/Permanent acknowledgement: the automatic brake application could be overridden even when not required, with safety impact. Failure of automatic brake application. This failure can happen at train level (command of the brake to the brake system) or brake level (brake application by brake system). In both cases the result is the same: - Missing application or Undue/permanent override: the brake is not applied, impacting the safety, but not the running capability. - Missing override or Undue/permanent application: the brake is applied when not requested, impacting safety and running capability. **Safety**: As written above, failure in applying the brake is one of the safety hazards considered by TSI. The system shall be designed to comply with the safety level required by TSI	Mission/Safety
Provide passenger alarm intercommunication	YES	As described at the beginning of the chapter, the communication train ground is not considered a safety relevant function in GoA1/2. The impact on the running capability depends if running till the next station without communication is admissible or not on GoA3/4 train. The hypothesis considered is that OCC in this case apply the brake (even if not required) until communication is not possible. Failure of passenger alarm communication: - Missing communication: automatic brake is applied in case of PAD activation, running capability is impacted. Safety is also impacted because train can be braked when not required. - Undue/permanent communication: it creates disturbance to OCC or passenger, but has no impact on safety and running capability. -	Mission/Safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		Safety: Even if TSI is not reporting any specific safety requirement about communication between passenger and driver, this functionality has generally a safety relevance because it permit the driver to have a better understanding of the situation and take the proper decision. For this reason, this functionality should be part of a safety evaluation in GoA3/4 train.	

Table 13 – Passenger alarm system running capability impact critical analysis

4.3.2 Monitoring function critical analysis

The functional single failure impacting running capability among the § 4.3.1 list is already diagnosed in GoA1/2 train. See below table for critical evaluation.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Manage alarm request from passenger. AND Manage passenger alarm request.	YES	The monitoring of the passenger request AND of the request management (Missing/undue/permanent request, acknowledgement, or brake application) is generally done on GoA1/2 train because the failures are safety relevant. **Safety impact:** The risk of injuries to passenger in case of safety relevant fault are generally mitigated by highly reliable components or single fault tolerant architecture or SIL2 SW functions (high integrity) or by single fault leading to the safe state condition. In case of single fault tolerant system, the fault monitoring prevents hidden failures which can cause double failure along the time, with related safety impact.	NO
Provide passenger alarm intercommunication	NO	The monitoring of passenger-driver communication from each passenger alarm device is not part of today GoA1/2 train state of art	YES

Table 14 – Passenger alarm system monitoring function critical analysis

4.3.3 New/Updated monitoring function use cases

A new use case is necessary to be sure of the availability of the communication between passenger and OCC.

The proposal is to introduce a new sub-test of the function at the start of the mission.

The use case in table 15 of document TAU-T3_1-D-FTI-039-02 can be updated as follow:

Use Case	**Testing of Passenger Alarm**
ID	**UC4.3.1**
Actor	Passenger Alarm System, Brake system. TCMS, Train-ground communication and Ground Operation Control Centre
Goal	Check the functionality of the Passenger alarm request, passenger alarm request transmission to OCC, acknowledgement transmission to train, automatic brake application or override
Safety relation	The use case is safety relevant with relation to the hazards related to the automatic brake application at station, delayed brake application during the run and brake override by ground operator acknowledgment
Precondition	Train in standstill and immobilized by parking brake, holding brake not active (forced), emergency brake not active, train status “out of station” (forced) brake system, TCMS, train-ground communication system, operative and tested
Flow of events	Following flow of events to be repeated for every PAD. 1. The Passenger Alarm system simulate the activation of the PAD. 2. The train-ground communication system checks the passenger alarm request is active. 3. The ground operation control centre checks the passenger alarm request is active, the communication with position of activated PAD is active and acknowledge the request within 10 s from alarm activation. 4. The Passenger Alarm system check that the acknowledgment is received. 5. TCMS check that brake is not applied automatically. 6. The Passenger Alarm system reset the simulation of activation of the PAD. 7. TCMS check again that brake is not applied. 8. The Passenger Alarm system simulate again the activation of any PAD. 9. The ground operation control centre checks the passenger alarm request is active and **doesn’t** acknowledge the alarm request 10. The Passenger Alarm system check that the acknowledgement is not received within 10 s from alarm activation. 11. TCMS check that brake is automatically applied. 12. The Passenger Alarm system reset the simulation of activation of the PAD. 13. TCMS check that the brake is released
Post condition	Train in standstill and immobilized by parking brake, holding brake not active (forced), emergency brake not active, train status “out of station” (forced)
Things that can go wrong	Train operation control centre doesn’t receive the alarm. Train operation control centre doesn’t communicate with the position of the active PAD. Train operation control centre doesn’t transmit the acknowledgment. Passenger Alarm doesn’t receive the acknowledgement signal. Passenger Alarm doesn’t override the automatic brake application. Passenger alarm doesn’t request the brake application. Brake system doesn’t apply the brake when requested. Brake system apply the brake when not requested
Already implemented risk reduction measures	
Observations	Use case linked to Passenger Alarm architecture as described in in Figure 3 of TAU-T3_1-D-FTI-039-02

Table 15 – Testing of passenger alarm new monitoring use case

4.3.4 Auto-recovery functions critical analysis

The auto-recovery critical analysis is done for functional failures impacting the running capability.

If the overall mission reliability is not achievable, possible solutions are:

- to have more reliable components/SW implementing the functions that in case of failure impact the running capability.
- to review the architecture implementing those functions (for example single fault tolerant)
- to improve permanent diagnosis of that functions, to prevent the effect of the fault.
- to determine functional failure safe state of that functions compatible with running capability.

The implementation of the first solution means to develop components robust enough to guarantee the mission reliability target (out of the scope of this document), without the necessity to define new use cases.

The definition of safe states compatible with running capability (if there are the condition) should be the output of a safety analysis which is not in the scope of this document.

In below table a critical analysis is done about improved diagnostic solution with single fault tolerant system architecture.

If system architectures implementing functionalities which can impact the running capability become single fault tolerant and the diagnostic system is capable to detect the single failure, the running capability is not affected, and the OCC can take one of the following decisions based on the failure message:

- removal from the service at the next station if the time to risk of interrupting the run of the train (mission reliability) or to have a failure impacting the safety is no more compatible with the mission targets (each failure mode time to risk evaluation and mission target shall be output of project mission reliability/safety studies)
- maintenance activity planning at the end of the mission if both risks are compatible with the mission target.

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Missing alarm from train to OCC	The architecture is single fault tolerant if the whole signal flow from PAD to OCC has not a common cause single failure leading to interrupt the alarm signal flow. The possibility to have permanent diagnosis depend on the architecture and technical solution used. In any case, even if the failure diagnosis cannot be permanent, but available only in the moment of the PAD activation, the single fault tolerant architecture permit to guarantee the functionality and the OCC is informed of the degraded condition in parallel to the passenger alarm signal activation and can take the decision about the mission continuation. **Safety impact:** If the level of safety of the transmission of the signal after the fault occurrence is tolerable, the mission can continue. If not tolerable the train shall be removed from the service at the next station (time to risk from the failure occurrence to the next station shall be acceptable)	NO
Missing acknowledgement from OCC to train.	The architecture can be single fault tolerant if the whole signal flow from OCC to Passenger Alarm System has not a common cause single failure leading to interrupt the acknowledgement signal flow. The possibility to have permanent diagnosis depend on the architecture and technical solution used. In any case, even if the failure diagnosis cannot be permanent, but available only in the moment of the acknowledgement activation, the single fault tolerant architecture permit to guarantee the functionality and the OCC is informed of the degraded condition in parallel to the acknowledgment signal activation and can take the decision about the mission continuation. **Safety impact:** If the level of safety of the transmission of the signal after the fault occurrence is tolerable, the mission can continue. If not tolerable the train shall be removed from the service at the next station (time to risk from the failure occurrence to the next station shall be acceptable)	NO
Missing override of automatic brake request by Passenger alarm system	The architecture is single fault tolerant if the whole signal flow from Passenger Alarm to Brake System has not a common cause single failure leading to interrupt the override signal flow. The possibility to have permanent diagnosis depend on the architecture and technical solution used. In any case, even if the failure diagnosis cannot be permanent, but available only in the moment of the override activation, the single fault tolerant architecture permit to guarantee the functionality and the	NO

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	OCC is informed of the degraded condition and can take the decision about the mission continuation. **Safety impact:** If the level of safety of the transmission of the signal after the fault occurrence is tolerable, the mission can continue. If not tolerable the train shall be removed from the service at the next station (time to risk from the failure occurrence to the next station shall be acceptable)	
Undue/permanent brake application command from passenger alarm system to brake system.	The architecture is single fault tolerant if the whole signal flow from Passenger Alarm to Brake System has not a common cause single failure leading to interrupt the brake application command signal flow. The possibility to have permanent diagnosis depend on the architecture and technical solution used. In any case, even if the failure diagnosis cannot be permanent, but available only in the moment of the brake activation command, the single fault tolerant architecture permit to guarantee the functionality and the OCC is informed of the degraded condition and can take the decision about the mission continuation. **Safety impact:** If the level of safety of the transmission of the signal after the fault occurrence is tolerable, the mission can continue. If not tolerable the train shall be removed from the service at the next station (time to risk from the failure occurrence to the next station shall be acceptable)	NO
Undue/permanent brake application by brake system	The activation of this failure could lead to the impossibility to release the brake. This failure is not related to passenger alarm function, but to brake system local application function. The auto-recovery of this functional failure is managed in chapter 4.10 as well as the information to OCC. **Safety impact:** When the auto-recovery solution is the local brake application control isolation, the safety of the brake application at train level is guaranteed because the performances of the train are generally adapted accordingly in case of isolation. Only multiple isolations can lead to train unsafe performances.	NO
Missing passenger communication from train to OCC	The architecture is single fault tolerant if the whole communication flow from Passenger Alarm OCC has not a common cause single failure leading to interrupt the communication flow. The possibility to have permanent diagnosis depend on the architecture and technical solution used. In any case, even if the failure diagnosis cannot be permanent, but available only in the moment of the communication activation, the single fault tolerant architecture permit to guarantee the functionality and the OCC is informed of the degraded condition in parallel to	NO

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	the communication activation and can take the decision about the mission continuation. **Safety impact:** If the level of safety of the communication after the fault occurrence is tolerable, the mission can continue. If not tolerable the train shall be removed from the service at the next station (time to risk from the failure occurrence to the next station shall acceptable)	

Table 16 – Passenger alarm system auto-recovery function critical analysis

4.3.5 New/Updated auto-recovery function use cases

New/Updated use cases to manage the auto-recovery function in GoA3/4 train are not needed, but suitable architectures and/or technical solutions to be implemented to guarantee the passenger alarm functionality with mission reliability/safety level compatible with the project targets.

Main function "Provide external access/egress" is realized in autonomous train by the implementation of the here below sub-functions, where new-*n* are the new function which D3.1 introduce as possible impact of the transition to GoA3/4:

D B B a	Release external doors
D B C a	Open external doors
D B D a	Close external doors
D B E a	Manage door system upon obstacle
D B F a	Lock external doors
D B G	Unlock external doors
D B H a	Enable selective external door opening in order to make certain vehicles of the train inaccessible
D B J	Provide entrance lighting
D B K	Isolate external doors
D B L	Signal all external door closed and locked state
D B M a	Signal external door status change/open/close by visual or audible signals
D B N a	External door opening in emergency
D B P a	Reduce the gap between vehicle and platform
D B Q a	Ensure passenger access by external doors for people with reduced mobility
D B R	Provide access for driver and crew to the train
D B S a	Provide special emergency exits functions (emergency front doors and other emergency exits (i.e. windows))
New-1	Back-up door closing
New-2	Automatic door mechanical isolation

The real necessity of the new sub-functions depends by requirements on specific project. Considering the entity of the modification, the specific project requirements most probably will not include these functionalities, managing by station staff the door manual closing and isolation. For completeness, this document suppose that these new functionalities are implemented.

The back-up door closing includes the following sub-functions.

a. *Video-monitoring of the area around every door*
b. *Transmission of the images of every door to the Ground Operation Control Centre,*
c. *Activation of the Ground to train passenger communication.*
d. *Transmission of the back-up door closing by Ground Operation Control Centre*
e. *Closure of the door by back-up system*

Note: differently from what supposed in D3.1 related use case, the Automatic door mechanical isolation is supposed to be autonomously managed by the train at the end of the back-up closure, without the involvement of the Train-Ground communication.

Video-surveillance, Train-Ground and TCMS-doors communication are part of the train functions.

CF-Provide public address, passenger information, intercommunication and entertainment.

KD- Provide operational communication and train/ground data transmission.

H- Provide train communication, monitoring and control.

Failures of CF/KD/H Main function can therefore cause a functional failure of the function "New-1 Back-up door closing". As explained in the impact analysis, this would be a case of double failure, which shall not be considered (low probability of occurrence).

4.4.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Release external doors	YES	This is a function managed both at train level and local level. If the failure is at train command level all passenger doors cannot be opened (permanently false release signal) or could be opened as soon as the zero speed signal is active and any passenger require the door opening by local command (permanently true release signal) or can be opened on wrong side If the failure is at local level single door cannot be opened or could be opened as soon as the zero-speed signal is active and any passenger require the door opening	Safety
Open external doors	NO	This is a function managed both at train level and local level. If the failure is at train command level all passenger doors cannot be opened (permanently false opening signal) or are immediately opened as soon as the release signal is active (permanently true opening signal) If the failure is at local level single door cannot be opened. In GoA1/2 already redundancies exist to guarantee train command is	

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		single fault resistant and local failure are covered by the presence of other doors. No impact on Mission and Safety	
Close external doors	YES	This is a function managed both at train level and local level. If the failure is train level closing command permanently true or flickering all passenger doors cannot be closed by dedicated signal, but door can be alternatevily closed by removal of the door release signal. If the failure is train level closing command permanently false all passenger doors cannot be closed by dedicated signal, but door can be alternatively closed by removal of the door release signal. If the failure is local level closing function single door cannot be closed and therefore the door and close locked signal is not available.	Mission
Manage door system upon obstacle.	YES	This is a function managed locally, failure can affect single door only. Passengers are no more protected against injuries during door closing on the affected door. The door needs to be isolated	Safety
Lock external doors	YES	This is a function managed locally, failure can affect single door only. Passengers are no more protected against injuries during door closing on the affected door. The door needs to be isolated	Safety
Unlock external doors	NO	This is a function managed locally, failure can affect single door only Passenger are no more allowed to use the affected door. Another door can be used.	
Enable selective external door opening in order to make certain vehicles of the train inaccessible	YES	This is a function managed both at train level and local level. Passenger doors can be opened in no safe area	Safety
Provide entrance lighting	NO	This is a function managed locally, failure can affect single door only. Impact depending on the PHA of the train. It is considered for the moment a mitigation of a risk; its failure should not impact the mission reliability	

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Isolate external doors	NO	In autonomous train during the run this function is replaced by new function “Automatic door mechanical isolation”. In GoA1/2 train is a function managed at local level, in GoA3/4 train the new function involve both train and local level. In any case this function become relevant in the moment that another function enters in a safe state requiring the isolation (major fault). This means that the failure of this function become relevant only in case of double fault. No mission impact	
Signal all external door closed and locked state	YES	This is a function managed both at train level and local level. The consequence of a fault is traction block (in case of permanently false) or Traction release with door open (in case of permanently true)	Safety
Signal external door status change/open/close by visual or audible signals	NO	This is a function managed locally, failure can affect single door only. The risk of injury during closing is limited by obstacle detection, during opening by labels asking not to lay on the door leaf	
External door opening in emergency	NO	Double failure case (like isolation): if emergency exit is needed means that there is another failure on the train. In any case other doors available.	
Reduce the gap between vehicle and platform	YES	This is a function managed locally, failure can affect single door only. Risk of injuries during passenger exchange	Safety
Ensure passenger access by external doors for people with reduced mobility	YES	This is a function managed locally, failure can affect single door only. People with reduced mobility detrainment delayed due to back-up solution to be put in place (station staff operate the detrainment from standard door in case of dedicated PRM door or the person with reduced mobility call for aid and train shall wait for detrainment from another door)	Mission
Provide access for driver and crew to the train	NO	This is a function managed locally, failure can affect single door only. Passenger doors can be used	

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Provide special emergency exits functions (emergency front doors and other emergency exits (i.e. windows))	NO	Double failure case: if emergency exit is needed means that there is another failure on the train	
Back-up door closing	NO	Double failure case: back-up door closing necessity means that there is another failure on the same door. The back-up door closing, if present, shall be designed to be fully independent from other door functionalities (no common failure cause possible)	
Automatic door mechanical isolation	NO	Double failure case: automatic door mechanical isolation necessity means that there is another failure on the same door.	

Table 17 – Passenger doors system running capability impact critical analysis

4.4.2 Monitoring function critical analysis

The functional failures, impacting running capability among the § 4.4.1 list, are all generally diagnosed in GoA1/2 train. See below table for critical evaluation:

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Release external doors	YES	Independently from the technical solution used, the monitoring of the release command is generally done on GoA1/2 train because the failure is safety relevant. Also, at local level consistency checks are done any diagnostic system to detect any local failure **Safety impact:** The risk of injuries to passenger in case of fault (permanently true release command or wrong side) is always mitigated by single fault resistant architecture (high integrity). Therefore, the single fault permanently false lead to the safe state condition of door not enabled), with impact on the mission reliability (see next chapter). The monitoring is important to prevent hidden failures which can cause double failure along the time, with related safety impact.	NO
Close external doors	YES	Independently from the technical solution used, the monitoring of the close command is generally done on GoA1/2 train (to inform the driver that a door is not closing, blocking the mission, and therefore need to be isolated).	NO
Manage door system upon obstacle	YES	The monitoring of the obstacle detection is generally done on GoA1/2 train because the	NO

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
		failure is safety relevant (note: obstacle detection is generally done at least by motor current monitoring, but if current cannot be monitored also the open and close door functionality is affected) **Safety impact:** The fault can be only local. In case of fault, the door needs to be isolated because also other functionalities are affected. The isolation is implemented by driver/train captain in GoA1/2 trains, it can be done by new function “Automatic door mechanical isolation” in GoA3/4 trains	
Lock external doors	YES	Independently from the technical solution used, the impossibility to lock external door is diagnosed on GoA1/2 train because the failure is safety relevant. **Safety impact:** The risk of injuries to passenger in case of fault is always mitigated by single fault resistant architecture (high integrity). Therefore, the single fault lead in the worst case to the safe state condition of permanently false signal only (door not locked) with impact on the mission reliability (see next chapter). The monitoring is important to prevent hidden failures which can cause double failure along the time, with related safety impact.	NO
Enable selective external door opening in order to make certain vehicles of the train inaccessible	YES	The train side failure monitoring is already present on existing GoA1/2 trains with this function implemented, involving different system of the train (train-ground communication, TCMS, doors) because the function is safety relevant. The local failure can be linked to local problem, causing the impossibility to open an enabled door by the train or not disabling a disabled door by the train. The diagnosis in such a case is already present on existing GoA1/2 trains because the function is safety relevant.	NO
All external door closed and locked state	YES	Independently from the technical solution used, the external door is diagnosed on GoA1/2 train because the failure is safety relevant. **Safety impact:** The risk of injuries to passenger in case of fault is always mitigated by single fault resistant architecture (high integrity). Therefore, the single fault lead in the worst case to the safe state condition of permanently false signal only	NO

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
		(doors not locked) with impact on the mission reliability (see next chapter). The monitoring is important to prevent hidden failures which can cause double failure along the time leading to false closed and locked doors signal, with related safety impact.	
Reduce the gap between vehicle and platform	YES	Independently from the technical solution used, the steps of platform deployment is diagnosed on GoA1/2 train because the failure is safety relevant. **Safety impact:** If the step/platform doesn't open the door doesn't open (safe state). If the step/platform doesn't close the door closed and locked state remain false (safe state). This function is therefore strictly linked to the other functions of door opening and door closed and locked state definition	NO
Ensure passenger access by external doors for people with reduced mobility	YES	Independently from the technical solution used, the GoA1/2 trains PRM doors or standard doors provided with PRM facilities are monitored as the standard doors (above functions critical analysis is therefore applicable) and a call for aid is provided close to the door, to permit the driver to manage the situation of a door that, due to the failure, cannot ensure a PRM to egress/access the train	NO

Table 18 – Passenger door system monitoring function critical analysis

4.4.3 New/Updated monitoring function use cases

As per above critical analysis new or updated monitoring functions use cases are not necessary in case of transition from GoA1/2 trains to GoA3/4 train.

4.4.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Release external doors: ***Train level*** *command permanently false*	The activation of this failure could lead to the impossibility to open all the passenger doors (safe state condition, see §4.4.2). In such a case the passenger can detrain by operating the emergency egress device present on each door. Specific message shall be provided to the passenger by information system. Afterward the train is removed from the service, closing all the door by reset of the EED before the train departure to the depot. Condition to reset is to be sure that the train is empty. On GoA1/2/3 (with operator on board) the reset can be done manually, therefore new functionalities are not requested, same as actual state of art On GoA4 train the EED could be manually operated by the station staff or by remote control. Due to that, it would be better if this operation is done by station staff. In any case, to also cover the case of not available station staff, new use case is generated providing a remote control EED reset. Note: the new use case impacts the technical solution of the passenger door, because actual state of art has only manual EED reset **Safety impact:** The safety of the release external door function is guaranteed by original design of the function. The EED reset by remote control in principle has not safety impact because safety is guaranteed by door visible and audible warning signals and obstacle detection during the closing after the EED reset. There is the risk that somebody remain in the train, but this is not considered a safety issue if mitigated by passenger information messages asking people to exit from the train and by video-monitoring of the train compartment	NEW
Release external doors: ***Train level*** *command permanently true*	The GoA1/2 train door systems are resistant to this type of failure (single fault), no need of auto-recovery function	NO
Release external doors: ***Train level*** *command on wrong side*	The GoA1/2 train door systems are resistant to this type of failure (single fault), no need of auto-recovery function	NO

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Release external doors: ***Local level*** *release status fault*	GoA1/2 trains door system has SIL2 control of door release signal, if failures to the function are diagnosed the system goes into safe state (major fault). In GoA3/4 trains the new functions "Back-up door closing" and "Automatic door mechanical isolation " can be used as auto-recovery, isolating the door. **Note: This can be a general auto-recovery function to be activated at any major fault activation by local door.** In case the system is not capable to detect the failure the affected door cannot be opened, but the passenger can detrain from another door, therefore no auto-recovery is necessary. **Safety impact:** The new functions "Back-up door closing" and "Automatic door mechanical isolation" shall be designed to mitigate any risk of not having door safely isolated and to have not injuries to passenger during back-up closing.	YES, new door functions to be used as auto-recovery
Close external doors: ***Train level*** *command*	The activation of this failure lead to the impossibility to open all the doors at train level (close command has priority on opening). Existing GoA1/2 trains already have redundancies avoiding that a single failure can affect the capability to open or close all the doors (bus and HW redundant command, redundant TCMS, …). Therefore, no need of auto-recovery solutions (the simplest alternative way to close the door is generally the removal of the door release	NO
Close external doors: ***Local level*** *fault*	If failures to the function is diagnosed the door system goes into safe state (major fault). In such a case the new functions "Back-up door closing" and "Automatic door mechanical isolation" can be used as auto-recovery, isolating the door. See above comments at local release status fault case	YES, new door functions to be used as auto-recovery
Manage door system upon obstacle: **Local level** fault	If failures to the function is diagnosed the door system goes into safe state (major fault). In such a case the new functions "Back-up door closing" and "Automatic door mechanical isolation" can be used as auto-recovery, isolating the door. See above comments at local release status fault case, in particular the obstacle detection capability of the back up door closing function	YES, new door functions to be used as auto-recovery
Lock external doors: **Local level** fault	If failures to the function is diagnosed the door system goes into safe state (major fault). In such a case the new functions "Back-up door closing" and "Automatic door mechanical isolation" can be used as auto-recovery, isolating the door and locking by isolation system the door. See above comments at local release status fault case.	YES, new door functions to be used as auto-recovery

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Enable selective external door opening: **Train level command fault**	The function is safety relevant, GoA1/2 trains implementing this function use SIL2 control for it, if failures to the function are diagnosed the system goes into safe state (major fault). The safe state is defined during the design. If the worst scenario of safe state is that all doors are not enabled to be opened, the auto-recovery could be the same of the door release failure (emergency exit).	NEW
Enable selective external door opening: **Local level fault**	The function is safety relevant, GoA1/2 trains implementing this function use SIL2 control for it, if failures to the function are diagnosed the system goes into safe state (major fault), guaranteeing the safety (door remain close). In such a case other door can be used.	NO
All external door closed and locked state always false. **Train level fault**	In GoA1/2 trains the safe state is generally the traction block (and in some cases also braking if the train is running). The driver, once checked the situation, decide what to do: to stop immediately the train and isolate the door (bypassing the local door closed and locked signal) or to bypass the traction block and isolate later the door. For train level fault (broken wire or whatever fault not allowing to transmit to the cab the closed and locked signals by all the doors) the only action the driver can do is to bypass the traction block by dedicated switch. In case of GoA3/4 train if a train level fault occur, such operation should be put in place via train – ground communication. To do the job of the driver the control centre need to receive from the train reliable information about the status of the doors before deciding to bypass the traction block (and the braking, if activated). This means that there should be a parallel information to the one use to command the traction block with at least the same level of integrity. But in such a case it is convenient to use this redundant safe circuit to avoid the traction block and don't impact the running capability. A new use case is not necessary, but a redundant control system of all external door close and locked state signal could be necessary **if the reliability is not considered sufficient to guarantee the expected target of running capability**. This redundancy shall be implemented at train level only, because the local door level is covered by next case.	NO, but redundant safe system is mandatory
Signal all external door closed and locked state **Local level fault**	In GoA1/2 trains in case of single fault the worst case leads to door closed and locked false state (safe state) and consequently traction block controlled at train level (see above). In case of GoA3/4 train, the isolation can be immediately done by new defined function "Back-up door closing" and "Automatic door mechanical isolation ", isolating immediately the door in the case this failure is detected (train level all doors	YES, new door functions to be used as auto-recovery

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	closed and locked signal not active AND local door not closed and locked). **Safety impact:** The new functions “Back-up door closing” and “Automatic door mechanical isolation” shall be designed to mitigate any risk of not having door safely isolated and to have no injuries to passenger during back-up closing.	
Reduce the gap between vehicle and platform. **Local fault:** step/platform not deployed	As written in chapter 4.4.2, the safe state is door not opening, therefore the passenger shall use another door. No need of auto-recovery function	NO
Reduce the gap between vehicle and platform. **Local fault:** step/platform permanently deployed	As written in chapter 4.4.2, the safe state is door closed and locked signal always false, therefore the reaction shall be the “Back-up door closing” and “Automatic door mechanical isolation” functions activation. This analysis evidence as the “Back-up door closing” function shall manage both step/platform and door back-up independent closing.	YES, new door functions to be used as auto-recovery
Ensure passenger access by external doors for people with reduced mobility	Consideration done for all above failures are applicable also to this function for what applicable to the egress/access of a PRM, with the difference that the use of another door cannot be considered auto-recovery solution, but call for aid is the solution, as per existing trains	NO

Table 19 – Passenger door system auto-recovery function critical analysis

4.4.5 New/Updated auto-recovery function use cases

As per above critical analysis there are 2 new uses cases to be defined to facilitate the auto-recovery of a GoA3/4 train in case of failure to the passenger access/egress function failure:

- Emergency exit

Additionally, the use case of new functions already identified in document D3.1

- Back-up door closing
- Automatic door mechanical isolation

shall be specified, providing evidence of the back-up closing and isolation of door and step/platform.

As already evidenced in document D3.1, a benchmarking with automatic Metro applications should be done to evaluate if the identified use cases, consequence of most conservative assumptions, can be the solution to manage the failures of doors or less conservative assumptions are applicable on regional/intercity trains, avoiding to introduce functions which could have a very heavy impact on door design (in particular back-up door closing and automatic door mechanical isolation)

In case of transition to GoA3/4A, redundant train control system of the function generating the state of all doors closed and locked (to guarantee the safe functionality also in case of single failure) could be also necessary if the reliability of the train control system is not compatible with the running capability target.

In the next pages the proposal for the 3 new use cases is provided

Use Case	Emergency exit
ID	UC4.4.1
Actors	Control centre, Train-Ground communication, TCMS, Door system, Passenger information system
Goal	Train passengers' evacuation, resetting all the EED of the train, door closing and train departure to the depot (mission failure)
Safety relation	no
Precondition	Train is stopped, release external door failure permanently false, people need to be detrained
Flow of events	1) The release external door failure is transmitted by TCMS to Train-Ground communication and by Train-Ground communication to Control Centre. 2) Control Centre activate the communication with passenger information system of the train via Train-Ground communication and ask people to exit from the train within next x minutes. 3) After x minutes Control Centre activate the communication with passenger information system of the train via Train-Ground communication and inform people that doors are going to be closed and train departing to the depot 4) After y s Control Centre activate the communication with TCMS via Train-Ground communication and send the EED reset command 5) TCMS send the EED reset command to all the passenger doors. 6) The passenger doors are closed and locked by door systems. 7) Once the doors are closed and locked the control centre command the train to depart to depot via the Remote control.
Post condition	Train is running without passenger to the depot, EED reset, door closed.
Things that can go wrong	EED reset not successful, door remain open, traction block.
Already implemented risk reduction measures	Messages to the passenger to exit from the train, traction block in case of door open
Observations	

Table 20 – Emergency exit new auto-recovery use case

Use Case	**Back-up door closing**
ID	UC4.4.2
Actors	Door system
Goal	Close the door in case of failure to the main closing system
Safety relation	Yes, injuries to passengers during closing
Precondition	Major fault activation at door level with door open
Flow of events	1) The door system detects a major fault avoiding the door to be closed. 2) The door system, if all safety preconditions are satisfied, command the door closing by back-up independent door closure device. 3) The door close and the back-up signal of door closed is activated.
Post condition	Major fault is still active, Door is closed
Things that can go wrong	Back-up door closure device is not able to close the door, door remain open, traction block
Already implemented risk reduction measures	Traction block in case of door open, limited closing force to avoid injuries to passengers
Observations	

Table 21 – Back-up door closing new auto-recovery use case

Use Case	**Automatic door mechanical isolation**
ID	UC4.4.3
Actors	Door system
Goal	To isolate a door which is in major fault
Safety relation	Yes, locking of the door
Precondition	Major fault activation at door level with door open, door closed signal true by standard closing function or by back-up closing function
Flow of events	1) The door system checks the condition major fault AND (door closed signal OR back-up door close signa) is true. 2) If the condition is true, the door system command the door isolation device. 3) The door isolation device successfully isolates mechanically the door. 4) The mechanical isolation bypasses the closed and lock status signal to the train
Post condition	Major fault is still active, the door is closed and locked both from mechanical and state to train point of view, the door enters in isolation status
Things that can go wrong	Mechanical isolation not successful: door is not mechanically locked, door state is not closed and blocked, traction block. Door isolated status not available, door is mechanically blocked, door state is not closed and blocked, traction block
Already implemented risk reduction measures	Traction block in case of door not closed and locked state false
Observations	

Table 22 – Automatic door mechanical isolation new auto-recovery use case

4.5 PANTOGRAPH

Main function “F B Provide electrical energy for traction” is realized in autonomous train by the implementation of some sub-functions of Pantograph System bellowed:

F B E a Collect electrical energy for traction

F B E a Manage collection device

F B E a Protect collection devices and catenary

F B E a Prevent damage to the catenary

4.5.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Collect electrical energy for traction	yes	This is a function failure on train level. Failure of this function, selected pantograph cannot collect energy from catenary. Train should be connected to the other pantographs. This is mainly not an issue for pantograph, but energy supply system.	Mission
Manage collection device	YES	This is a function failure on train level. Failure of this function, selected pantograph cannot collect energy from catenary. Train should be connected to the other pantographs.	Mission
Protect collection devices and catenary	YES	This is a function failure on train level. In case of failure of this function pantograph should be lowered by the Automatic Dropping Device(ADD).	Mission
Prevent damage to the catenary	YES	This is a function failure on train level.In case of failure of this function pantograph should be lowered by the ADD	Mission

Table 23 – Pantograph system running capability impact critical analysis

4.5.2 Monitoring function critical analysis

The functional failures impacting running capability among the § 4.4.1 list are all generally diagnosed in GoA1/2 train. See below table for critical evaluation

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Collect electrical energy for traction	yes	The monitoring function of the electrical energy collection system involves monitoring the electrical parameters of the power supply, such as voltage and current, and ensuring that the power is collected and supplied to the traction motors in a safe and efficient manner. This is important because any disruptions or malfunctions in the collection system can result in a loss of traction power, which can cause delays, breakdowns, or even accidents. The monitoring of pantograph is done on GoA1/2 train by driver because the failures are safety relevant. Automated action needed for GoA3/4	yes
Manage collection device	yes	The monitoring function of managing the collection device involves monitoring the condition of the collection device and ensuring that it is functioning properly. This includes monitoring the contact pressure between the collection device and the power source, as well as the wear and tear on the collection device components. If the collection device is not functioning properly, it can result in a loss of power or even a potential safety hazard. The monitoring of pantograph is done on GoA1/2 train by driver because the failures are safety relevant. Automated action needed for GoA3/4	yes
Protect collection devices and catenary	yes	The monitoring of pantograph is done on GoA1/2 train by driver because the failures are safety relevant. Automated action needed for GoA3/4Automated action needed for GoA3/4	yes
Prevent damage to the catenary	yes	The monitoring of pantograph is done on GoA1/2 train by driver because the failures are safety relevant. Automated action needed for GoA3/4Automated action needed for GoA3/4	yes

Table 24 – Pantograph system monitoring function critical analysis

4.5.3 New/Upated monitoring function use cases

For all functions, indication should go the control centre instead of Driver for GoA3/4.

Use Case	Failure of B E sub-functions
ID	UC4.5.1
Actors	Remote Driver, TCMS, pantograph,
Goal	Enable remote actions in case of failure of pantograph system sub-functions
Safety relation	TSI Loc&Pas
Precondition	Pantograph System failed
Flow of events	TCMS sends train diagnostics of pantograph Remote Driver observes the failure. Remote Driver decides further steps such as -restart the system -switch direction -move pantograph up&down -call help -close doors -inform operation center
Post condition	Inform operation center / TCMS that mission has been failed.
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 25 – Failure of pantograph system new monitoring use case

4.5.4 Auto-recovery functions critical analysis

Depending on the failure a reset of the pantograph system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.

4.5.5 New/Upated auto-recovery function use cases

Use Case	Reset of F B sub-function
ID	
Actor	remote driver
Goal	Reset the pantograph system
Safety relation	yes
Precondition	Faulty on sub functions
Flow of events	- Send status of pantograph system to remote driver - Send the diagnostic data to remote driver - Wait for commands from remote driver. - Remote driver reacts action for system configuration and/or restarts the system
Post condition	
Things that can go wrong	Failure remains
Already implemented risk reduction measures	
Observations	

Table 26 – Pantograph system reset use case

4.6 AUXILIARIES POWER SUPPLY SYSTEM

The functional scope of the auxiliary power supply can be structured as defined by EN 15380. See the list of functions here below:

F C Provide electrical energy for auxiliaries

F C C Provide self protection configuration for storage

F C E Collect electrical auxiliary energy, Use Shop Power Supply

F C G Distribute electrical auxiliary energy, Protect distribution devices, Protect electrical devices against overvoltage, Protect electrical devices against overcurrent, Detects grounds or short circuits in the Auxiliary energy distribution network,

F C H Store electrical auxiliary energy, Provide Charging, Provide Discharging, Provide low voltage control status information, Provide low voltage DC supply, Ensure electrical protection

4.6.1 Functional failure impacting running capability

Depending on the individual architecture of the vehicle many auxiliary devices are essential to the health of the vehicle and so is their power supply.
Some examples are:

- Cooling fans
- Cooling pumps
- Battery chargers
- Air compressors

It is obvious that in case of a fault in the energy supply of any of these sub-systems the fault will stop the vehicle either immediately or at the latest after some discharging time. In most cases the vehicle would not be able to finish its mission or will need to continue in some degraded low performance mode.

On the other hand there are auxiliary functions that when disabled would not lead to a stopping failure.
Examples:

- Manage shore power supply
- Measure and provide charging state of an energy storage system
- Trainline power supply

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Auxiliary converter blocked	YES	All 3 phase cooling fans and pumps will stall. In electric powertrains this can be considered as stopping failure as the traction equipment will overheat quickly. The main compressor will stop as well so the train must stop when the main reservoir pressure is low. HVAC system will be dysfunctional, which might lead to dangerous temperature levels inside the passenger saloon.	Mission/Safety
Main battery charger faulty	YES	After a while leads to outage of the low voltage supply when battery is flat. Subsequent faults are: brake system fault, TCMS fault. This failure scenario is well known from GoA1/2 systems and the architectures are designed fail-safe. So this scenario rather impacts the mission than safety.	MISSION
24 V DC supply faulty	YES	The 24 V supply could be faulty though the main battery supply is running normally. 24 V supply is essential to many TCMS components. For this reason in GoA1/2 architectures a redundant supply is foreseen. Additionally the subsystems depending on 24 V supply are designed fail-safe. So only a total outage of the 24 V supply would lead to a stopping failure.	MISSION
Train line supply faulty	NO	The train line (TL) is a typical element of the loco hauled train. When the TL supply is blocked this does not affect the running capability of the loco. Hence the train can continue its mission. Regarding the HVAC as the most important subsystem dependent on TL supply there could be a safety issue under extreme weather conditions (overheating or lack of ventilation in the passenger cars).	MISSION/SAFETY

Table 27 – Auxiliary power supply system running capability impact critical analysis

4.6.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Auxiliary converter blocked	Self protection and healing is already quite advanced: converter control permanently monitors the health of the converter. Converter stops upon failure detection, several automatic restart attempts before permanent blockage is triggered. The root cause for a severe failure in the aux supply is more likely to be located in some aux device or other part of the aux network than in the aux converter itself. Severe failure in the aux network are detected but reaction to such failures is in the driver's responsibility only. GoA3/4 operation would require additional remote status diagnostics in order to facilitate fault analysis and fault response.	YES
Train line inverter faulty	The train line inverter is continuously monitored by the TCMS system and its own built-in functions. The faults bearing the risk of danger or damage lead to protective pulse lock of the inverter. These functions include a certain self-healing capability. The system locks out completely only in case of permanent severe errors. Missing TL supply does not lead to an immediate failure or threat nor does it affect the running capability. Nevertheless responsible persons must be informed. In GoA1/2 the train crew takes this responsibility and decides what measure to take in order to keep up the running capability and safety. For GoA3/4 the capability of emergency HVAC and lighting are to be re-assessed. New TL-independent HVAC functions might be required. Also remote communication to passengers and remote/automatic control of degraded modes will be necessary. Additional energy source or energy capacity per coach might be required in order to secure the operability.	YES

Table 28 – Auxiliary supply system monitoring function critical analysis

4.6.3 New/Updated monitoring function use cases

Use Case	**Fault diagnostics and remote control of aux devices**
ID	UC4.6.1
Actors	Virtual driver
Goal	Enable remote fault analysis and remote activation of degraded aux system configuration.
Safety relation	No additional safety case (local system architecture is fail-safe)
Precondition	Aux converter blockage alert active.
Flow of events	1. TCMS sends remote diagnostics of aux converter and aux devices. 2. Virtual driver analyses the fault situation. 3. Virtual driver decides further steps such as - unlock aux converter - lock/activate certain aux systems
Post condition	Vehicle aux supply recovered in degraded mode.
Things that can go wrong	Severe electrical failure might not be recovered.
Already implemented risk reduction measures	Aux supply hardware components are developed for high availability and reliability performance.
Observations	

Table 29 – Fault diagnostics and remote control of aux devices new monitoring use case

Use Case	**Trainline Supply Remote Fault Diagnostics**
ID	UC4.6.2
Actors	Virtual driver
Goal	Enable remote activation of degraded system configuration in passenger coaches.
Safety relation	HVAC and lighting failure can affect passenger health
Precondition	TL converter blockage active.
Flow of events	1. TCMS sends remote diagnostics of TL converter 2. TCMS sends live status of the aux devices in the coaches. 3. Virtual driver analyses the fault situation. 4. Virtual driver decides further steps such as - provide information to the passengers - lock/unlock certain devices - lock/activate emergency power supplies - activate emergency ventilation devices
Post condition	TL supply deactive, degraded mode in the coaches active
Things that can go wrong	Under extreme weather conditions the emergency HVAC functions may not be powerful enough.
Already implemented risk reduction measures	
Observations	

Table 30 –Auxiliary Supply Trainline new monitoring use case

4.6.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Auxiliary converter blocked	In GoA1/2 the aux converter would make several restart attempts before being locked out by the monitoring system. In case of severe electrical fault in the aux network (e.g. overload or ground error) the aux converter will be locked out. Failure analysis by on-board staff. Manual re-activation of the TL-converter after isolation of the defect. Corresponding automatic or remote activation of degraded aux configuration and re-start of the converter to be developed for GoA3/4	YES
Train line supply faulty	In GoA1/2 the TL is managed manually by the driver. Response to electric failure (e.g. ground failure) on the coaches is possible but dependent on the skills of the train staff. In GoA3/4 this role must be taken over by the ‚virtual driver or certain automated actions. Such as: - Automatic message to control centre. - Automatic message to passenger information. - Remote monitoring and control of coach electricals. - Activation of emergency power supply for the coaches.	YES

Table 31 – Power supply system auto-recovery function critical analysis

4.6.5 New/Updated auto-recovery function use cases

Use Case	**Aux device failure remote response capability**
ID	UC4.6.3
Actor	Virtual driver
Goal	Select and (de-)activate faulty aux devices on demand.
Safety relation	-none-
Precondition	Aux converter pulse lock due to electric fault on load side
Flow of events	1) Send status of each aux device to remote desk 2) Send all diagnostic codes to remote desk 3) Wait for commands from virtual driver. 4) Virtual driver adapts system configuration and/or restarts secondary aux converter
Post condition	Auxiliaries supplied by secondary aux converter
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 32 – Auxiliary device failure new auto-recovery use case

Use Case	Remote aux network failure analysis capability
ID	Aux-Rec-02
Actor	Virtual driver
Goal	Localize the root failure in the network.
Safety relation	No new safety case
Precondition	Aux supply de-active. Aux network equipped with remote controlled segment contactors.
Flow of events	1) Status of aux devices known and analysed 2) Isolate aux circuit syspecte to be faulty. 3) Prepare aux converter for manual re-start.
Post condition	Faulty sub-circuit isolated.
Things that can go wrong	When failure was not recovered by the remote actions the aux converter will stop again.
Already implemented risk reduction measures	Hardware redundancy, design for reliability implemented in the aux system architecture.
Observations	

Table 33 – Remote aux network failure new auto-recovery use case

Use Case	Aux converter failure remote response capability
ID	Aux-Rec-03
Actor	Virtual driver
Goal	Remote manual restart of aux converter
Safety relation	No additional safety-case due to fail-safe local architecture.
Precondition	Suspected fault in aux network solved by remote driver.
Flow of events	1) Status of aux devices known and analysed 2) Defective part of aux circuit isolated 3) Give manual remote command to unlock aux converter. 4) Monitor diagnostics of yux system after re-activation.
Post condition	Auxiliary supply re-established.
Things that can go wrong	When failure was not recovered by the remote actions the auc converter will stop again.
Already implemented risk reduction measures	Hardware redundancy, design for reliability implemented in the aux system architecture.
Observations	

Table 34 – Auxiliary converter failure new auto-recovery use case

Use Case	**Trainline failure remote response capability**
ID	Aux-Rec-04
Actor	Virtual driver
Goal	Remotely isolate faulty car, set faulty car into degraded mode.
Safety relation	
Precondition	Fault diagnostics of each separate car available to remote driver.
Flow of events	1) Select car to be isolated 2) Send remote command to set car into degraded mode 3) Defective car isolated and switched to degrade mode 4) Give manual remote command to unlock TL-converter. 5) Monitor diagnostics of TL-converter after re-activation.
Post condition	TL supply re-established.
Things that can go wrong	When failure was not recovered by the remote actions the TL-converter will stop again.
Already implemented risk reduction measures	
Observations	

Table 35 – Auxiliary supply Trainline failure new auto-recovery use case

4.7 Low Voltage System

The low voltage system as per definition is considered the part of the auxiliary network that directly or indirectly is supplied by the vehicle's main battery circuit. When primary energy is available the battery circuit is powered by the battery charger and so is the rest of the low voltage network.

The functional scope of the low voltage supply is identical to the high voltage auxiliary supply. See list of EN 15380 functions below:

F C Provide electrical energy for auxiliaries

F C C Provide self protection configuration for storage

F C E Collect electrical auxiliary energy, Use Shop Power Supply

F C G Distribute electrical auxiliary energy, Protect distribution devices, Protect electrical devices against overvoltage, Protect electrical devices against overcurrent, Detects grounds or short circuits in the Auxiliary energy distribution network,

F C H Store electrical auxiliary energy, Provide Charging, Provide Discharging, Provide low voltage control status information, Provide low voltage DC supply, Ensure electrical protection

In GoA1/2 architectures the function F C G is realized through miniature circuit breakers with manual re-set capability. In GoA3/4 the manual action is not possible, hence a electronically controlled re-set capability is required for the mini circuit breakers. This kind of feature will require a secondary and independent energy LV - supply otherwise remote recovery would not be possible in case of LV supply failure.

In some vehicles the supply architecture is structured in main energy --> Auxiliary converter --> Battery charger. In these architectures there is a direct dependency of low voltage supply from the auxiliary supply. In other architectures the low voltage supply is the only auxiliary electrical supply.

The voltage levels of the most important architectures are 110 VDC, 72 VDC, 24 VDC. The use-cases described below are written for 24 V-supply, but basically are valid also for the other voltage levels.

Low voltage energy storage systems play a key role in thermo-mechanical traction systems where supplying the engine start is essential to the availability of primary energy. The combustion engine start process requires an independent energy supply capable to deliver extreme current peaks. In many cases the architecture includes a separate energy storage system in order to supply these peaks.

4.7.1 Functional failure impacting running capability

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Auxiliary converter blocked	YES	The main battery charger will be without supply, which leads to the same consequences as "battery charger faulty" and "24V supply faulty" (see below).	MISSION
Main battery charger faulty	YES	After a while leads to outage of the low voltage supply when battery is flat. Subsequent faults are: brake system fault, TCMS fault. This failure scenario is well known from GoA1/2 systems and the architectures are designed fail-safe. So this scenario rather impacts the mission than safety.	MISSION
24 V DC supply faulty	YES	The 24 V supply could be faulty despite the main battery supply running normally. 24 V supply is essential to many TCMS components. The subsystems depending on 24 V supply are designed fail-safe. So safety is not impacted.	MISSION
Start energy storage fault	YES	Monitoring the battery voltage alone is not sufficient to measure the degradation state of a battery. So the engine start could fail even if the measured value was measured OK by the diagnostic function. This would impact the operability in case the engine will be shut down during the mission.	MISSION

Table 36 – Low voltage system running capability impact critical analysis

4.7.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Main battery charger faulty	Battery charger health is monitored by the charger's control electronics. Diagnostics for workshop and driver are implemented. Automatic degraded modes are missing, only protective shutdown of the vehicle when battery voltage drops under defined threshold. More sophisticated modes seem technically feasible, such as a mode to max out residual operation time after failure. For GoA3/4 operation it seems sensible to add a redundant emergency battery charger.	YES
Battery dependent sub circuits disturbed.	All subsystems supplied by the main battery voltage are equipped with individual circuit breakers or fuses. In GoA1/2 it is state of the art that the status of each circuit breaker is available in the TCMS. In GoA3/4 operation the status of each circuit breaker must be available to the virtual driver on the remote system. A subset of these circuit breakers shall be capable of being re-set by the virtual driver.	YES
24 V DC supply faulty	In GoA1/2 there are multiple redundant supply devices. These devices have a certain self-diagnostic capability and deliver a status signal to TCMS. Automatic degraded modes are activated based on the current availability of the 24V supply. It is a precondition for GoA3/4 to implement this feature for all vital systems depending on 24 V supply. 24 V circuits are secured by miniature circuit breakers. The position of the circuit breakers is available in the TCMS. In a degraded situation new automatic or remote controlled functions will be required to secure the vehicle availability in GoA3/4 In GoA3/4 it could be sensible to ensure running capability by increasing the redundancy in the supply system.	YES
Start energy storage fault	In GoA1/2 the corresponding charging devices have a certain self-diagnostic capability, the storage element itself is monitored by a voltage level sensor. Battery degradation state is not monitored. In GoA3/4 battery state monitoring might be sensible. This could be realized through an automated function or by an operative process (e.g. a workshop routine).	YES

Table 37 – Low voltage system monitoring function critical analysis

4.7.3 New/Updated monitoring function use cases

Use Case	Remote resetting of mini circuit breakers
ID	UC4.7.1
Actor	virtual driver
Goal	Failure analysis, manual degraded mode
Safety relation	none
Precondition	Battery charger has stopped due to fault
Flow of events	1) Provide status of all mini CBs to remote desk 2) Re-set mini CBs after individual command by remote driver. 3) Remote driver takes decision how to end the mission.
Post condition	Remote control system powered until train was set into safe state or end of mission position.
Things that can go wrong	Train might not have ended the (degraded) mission before main battery is flat.
Already implemented risk reduction measures	none
Observations	

Table 38 – Remote resetting of mini circuit breakers new monitoring use case

Use Case	Remote control LV sub circuits
ID	LV-02
Actor	Auto recovery function, virtual driver
Goal	Maximize the time to keep up communication with control centre when in battery mode.
Safety relation	ETCS and remote control radio are crucial for passenger safety.
Precondition	Battery charger has stopped due to fault, train at standstill
Flow of events	1) TCMS de-activates non-vital aux devices 2) TCMS monitors battery voltage in order to adapt saving strategy. 3) TCMS waits for commands from virtual driver to re-activate required aux devices 4) Remote driver sets vehicle into degraded mode
Post condition	Vehicle is set into degraded mode and driven to safe place
Things that can go wrong	Train might not have ended the (degraded) mission before main battery is flat.
Already implemented risk reduction measures	none
Observations	

Table 39 – Remote control LV sub circuits new monitoring use case

Use Case	Advanced Battery Monitoring
ID	LV-03
Actor	Local TCMS
Goal	Monitor onboard battery ageing status
Safety relation	none
Precondition	None (always active)
Flow of events	1) Battery is charging or discharging 2) Monitor measures voltage, current, energy, load etc. 3) According to the long-term development of the monitored values the function predicts preventive maintenance. 4) Function creates workshop diagnostic inputs upon certain thresholds given.
Post condition	Monitoring starts new after reset by workshop technitian.
Things that can go wrong	Train might get stuck under cold weather conditions because the battery was weak, but no failure detected.
Already implemented risk reduction measures	none
Observations	

Table 40 – Advanced Battery Monitoring new monitoring use case

4.7.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Main battery charger faulty	Depending on the root cause some auto recovery is possible on a GoA1/2 train: - When main supply is interrupted the battery charger will automatically start after recovery of the main supply - When the battery charger is overheated the device will re-start once the temperature is valid again - When the battery charger detected overcurrent additional actions/analysis are required in order to detect the root cause. In GoA3/4 this won't be possible without additional remote diagnostics and/or automated circuit failure detection. In GoA3/4 operation automatic activation of an additional emergency battery charger could solve the issue.	YES
110/72/24 V DC supply faulty	Depending on the architecture, when 24 VDC is supplied by the main battery charger, GoA3/4 would require the same additional functions as a 110/72 VDC battery charger (see above). In GoA1/2 the DC-voltage supply is realized by multiple DC/DC converters working in parallel or by at least one LV battery charger. In GoA3/4 the redundancy of these devices, and automatic activation of additional degraded modes, such as energy saving mode will have to be developed.	YES
110/72/24 V DC supply faulty	In GoA1/2 miniature circuit breakers (mini CBs) are used to to cut out or reconfigure faulty subsystems. The affected circuits de-/re-activated in responsibility and by manual action of the driver. In GoA3/4 the same action requires miniCBs that can be set/re-set without the presence of the driver.	YES

Table 41 – Low voltage system auto-recovery function critical analysis

4.7.5 New/Updated auto-recovery function use cases

Use Case	**Battery charger autoheal**
ID	LV-Rec-01
Actor	Virtual driver
Goal	Acknowledge activation of emergency battery charger
Safety relation	none
Precondition	Battery charger has stopped due to internal fault
Flow of events	1) Send status of each aux device to remote desk 2) Send monitored live data to virtual driver 3) Block primary battery charger 4) Wait for remote activation command 5) Activate emergency battery charger
Post condition	Emergency battery charger active
Things that can go wrong	In case the root cause was not the charger but some external electric fault, also the emergency battery charger might fail.
Already implemented risk reduction measures	
Observations	

Table 42 – Battery charger autoheal new auto-recovery use case

Use Case	**Isolate faulty LV aux devices**
ID	LV-Rec-02
Actor	Virtual driver, TCMS
Goal	Select and (de-)activate faulty aux devices on demand.
Safety relation	
Precondition	Voltage supply disturbed due to fault in LV circuit.
Flow of events	1) Send status of each aux device to remote desk 2) Send all diagnostic codes to remote desk 3) Wait for commands from virtual driver. 4) Execute remote switching commands
Post condition	Circuit fault isolated, LV supply recovered.
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 43 – Isolate faulty LV aux devices new auto-recovery use case

Use Case	Remote setting of miniature circuit breakers
ID	LV-Rec-03
Actor	Virtual driver, TCMS
Goal	Select and (de-)activate faulty aux devices on demand.
Safety relation	none
Precondition	Voltage supply, subcircuit or LV device disturbed
Flow of events	1) Send status of each aux device to remote desk 2) Send all diagnostic codes to remote desk 3) Send status of all miniCBs to remote desk 4) Wait for commands from virtual driver. 5) Execute remote switching commands
Post condition	Fault isolated, LV supply recovered or faulty device cut out
Things that can go wrong	Not all faults can be recovered by this method (same situation as in GoA1/2)
Already implemented risk reduction measures	
Observations	

Table 44 – Remote setting of miniature circuit breakers new auto-recovery use case

4.8 Air Generation and Treatment system

The following functions are defined in the EN15380-4 involving Air generation and treatment system. They were considered within D3.1 when focusing on the start-up phase of the vehicles.

- F E Provide fluid energy for auxiliaries fluid energy refers to hydraulic/pneumatic media
- F E C a Generate fluid energy for auxiliaries pneumatic energy generation for brake system, doors, pantograph
- F E C a Manage generation process
- F E C a B Manage generation process
- F E C a Protect against over pressure
- F E C a C Protect against over pressure
- F E C a Ensure air quality
- F E C a D Ensure air quality
- F E D Collect fluid energy for auxiliaries seldom used: pneumatic energy taken from workshop storage
- F E E Store fluid energy for auxiliaries pneumatic energy storage vessel for air suspension

4.8.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Functions based on EN15380-4			
Provide fluid energy for auxiliaries. Fluid energy refers to hydraulic/pneumatic media	YES	If some of the auxiliaries are not supplied, the train cannot start/continue service and/or works in a backup mode. E.g. pantograph, power collector, air suspension.	Mission
Generate fluid energy for auxiliaries pneumatic energy generation for brake system, doors, pantograph	YES	If especially the brake system is not supplied, the train cannot start/continue service and the train is set to a safe state.	Mission/Safety
Manage generation process	YES	If especially the brake system is not supplied, the train cannot start/continue service and the train is set to a safe state.	Mission/Safety
Protect against over pressure	NO	Mission and Safety are not endangered but it is not recommended to work continuously with an over pressure protection being activated. A continuous generation of too much fluid energy has a negative impact regarding lifetime of the components. E.g. the compressor / over pressure valve… .	
Ensure air quality	NO	Mission and Safety are not endangered but it is not recommended to work continuously with too low air quality (air dryer disturbed, air filter polluted). A continuous operation with a too low air quality has a negative impact regarding lifetime of the components and could finally lead to safety critical failures. E.g. the piping, brake control, brake cylinders, … .	
Collect fluid energy for auxiliaries seldom used: pneumatic energy taken from workshop storage	NO	Workshop operation has no influence for the running capability.	
Store fluid energy for auxiliaries pneumatic energy storage vessel for air suspension	YES	If the air suspension is not supplied, the train cannot start/continue service and/or works in a backup mode.	Mission

Table 45 – Air generation system running capability impact critical analysis

4.8.2 Monitoring function critical analysis

The functional failures impacting running capability among the Table 45 list are all generally diagnosed in GoA1/2 train. See below table for critical evaluation.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Provide fluid energy for auxiliaries. Fluid energy refers to hydraulic/pneumatic media	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).
Generate fluid energy for auxiliaries pneumatic energy generation for brake system, doors, pantograph	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).
Manage generation process	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).
Protect against over pressure	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Ensure air quality	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).
Collect fluid energy for auxiliaries seldom used: pneumatic energy taken from workshop storage	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).
Store fluid energy for auxiliaries pneumatic energy storage vessel for air suspension	YES	Monitoring not different to GoA1/2 if the monitoring function is implemented in a state-of-the-art manner.	Function must potentially be implemented with a higher safety-level. The reporting chain will be different / automatised for GoA3/4 (train to trackside).

Table 46 – Air generation system monitoring function critical analysis

4.8.3 New/Updated monitoring function use cases

There were no new / updated monitoring functions identified

4.8.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Provide fluid energy for auxiliaries. Fluid energy refers to hydraulic/pneumatic media	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Generate fluid energy for auxiliaries pneumatic energy generation for brake system, doors, pantograph	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Manage generation process	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Protect against over pressure	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Ensure air quality	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Collect fluid energy for auxiliaries seldom used: pneumatic energy taken from workshop storage	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection	YES (limited)

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	
Store fluid energy for auxiliaries pneumatic energy storage vessel for air suspension	In case the air supply system has a redundancy, the main task to supply compressed is handled by the backup compressor. Depending on other failures a reset of the power supply system and/or the control system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)

Table 47 – Air generation system auto-recovery function critical analysis

4.8.5 New/Updated auto-recovery function use cases

Use Case	All failures limiting the air supply availability / performance
ID	UC4.8.1
Actors	Control centre, Train-Ground communication, TCMS, Air supply control system
Goal	Availability of compressed air for train operation
Safety relation	Yes
Precondition	Train is powered up, failure of air supply system is true
Flow of events	1) The failure of the air supply system is detected. Local master/slave switchover is performed as normal. 2) This information is transferred to the trackside control system via Train-Ground communication.
Post condition	Air supply is working again. Otherwise, air supply system is repaired in the depot at the end of the mission and a backup procedure is followed.
Things that can go wrong	Failure detection not successful. Consequence will appear in other subsystems. Safety critical situations will be handled by other subsystems (e.g. automatic emergency brake application by brake system in case of too low compressed air level)
Already implemented risk reduction measures	Usually air compressors are at least redundantly installed
Observations	

Table 48 –air supply new auto-recovery use case

4.9 Traction

Main function "G Accelerate, maintain speed, brake and stop" is realized in autonomous train by the implementation of the sub-functions of Pantograph System bellowed:

G B Provide acceleration

G C Provide deceleration, keep train at standstill

G D Improve adhesion

4.9.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Provide acceleration	yes	The running capability of providing acceleration depends on several factors, such as the power output of the train's traction system, the weight of the train, the condition of the track, and the gradient of the track. Modern trains typically use electric or diesel-electric propulsion systems that provide high levels of power and torque, allowing for rapid acceleration and efficient operation. This is a function failure on train level Failure of this occurrence, train cannot accelerate. Mission fails.	mission
Provide deceleration, keep train at standstill	yes	The running capability of providing deceleration of a train depends on several factors, such as the braking system, the weight of the train, the condition of the track, and the gradient of the track. Modern trains typically use advanced braking systems, such as regenerative brakes and electro-pneumatic brakes, that provide high levels of braking force and efficiency, allowing for rapid deceleration and safe operation. This is a function failure on train level Failure of this occurrence creates high danger, braking performance is needed.	safety
Improve adhesion	yes	The running capability of improving adhesion is critical for ensuring safe and efficient train operation, especially in regions with varying weather conditions. By using advanced adhesion methods and control systems, trains can maintain high levels of traction and grip on the track and maintain high levels of safety and reliability. This is a function failure on train level In case of failure of this function, reduce your brake effort is needed, to avoid risk of sliding, apply less braking force.	Safety/mission

Table 49 – Traction system running capability impact critical analysis

4.9.2 Monitoring function critical analysis

The functional failures impacting running capability among the § 4.4.1 list are all generally diagnosed in GoA1/2 train. See below table for critical evaluation

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Provide acceleration	yes	To monitor acceleration, various sensors and monitoring devices are installed in the train's traction system. These devices can include accelerometers, which measure the rate of acceleration, and speed sensors, which measure the train's speed. The data from these sensors is then fed into the train's control system, which adjusts the power supplied to the traction motors to achieve the desired acceleration. This should be control by control center in GoA3/4	yes
Provide deceleration, keep train at standstill	yes	To monitor deceleration, various sensors and monitoring devices are installed in the train's braking system. These devices can include pressure sensors that measure the pressure in the brake cylinders, speed sensors that measure the train's speed, and wheel sensors that detect the rotation of the train's wheels. The data from these sensors is then fed into the train's control system, which adjusts the braking force to achieve the desired deceleration. By monitoring the deceleration of the train and adjusting the braking force accordingly, the monitoring function helps to prevent excessive deceleration that can result in accidents or damage to the train's components, while also maintaining the efficiency and performance of the train's braking system. This should be control by control center in GoA3/4	yes
Improve adhesion	yes	the monitoring function of improving adhesion is critical for ensuring safe and efficient train operation, especially in adverse weather conditions. By using advanced monitoring and control systems, trains can improve adhesion and maintain high levels of safety and reliability. This should be control by control center in GoA3/4	yes

Table 50 – Traction system monitoring function critical analysis

4.9.3 New/Upated monitoring function use cases

For all functions, indication should go the control centre instead of Driver for GoA3/4

Use Case	Failure of G sub-functions
ID	UC4.9.1
Actors	Remote Driver, TCMS, traction system
Goal	Enable remote actions in case of failure of any traction system sub-function
Safety relation	TSI Loc&Pas
Precondition	Failure of Traction system
Flow of events	TCMS sends train diagnostics of traction Remote Driver observes the failure. Remote Driver decides further steps such as -restart the system -call help -inform operation center -isolate or connect propulsion system -provide dynamic brake status
Post condition	Inform operation center
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 51 – Traction system failure new monitoring use case

4.9.4 Auto-recovery functions critical analysis

Depending on the failure a reset of the traction system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.

4.9.5 New/Updated auto-recovery function use cases

Use Case	Reset of G sub-functions
ID	
Actor	remote driver
Goal	Reset the traction system
Safety relation	yes
Precondition	Faulty on sub functions
Flow of events	- Send status of traction system to remote driver - Send the diagnostic data to remote driver - Wait for commands from remote driver. - Remote driver reacts action for system configuration and/or restarts the system
Post condition	
Things that can go wrong	Failure remains
Already implemented risk reduction measures	
Observations	

Table 52 – Traction system reset use case

4.10 Brake and Sanding

The following brake/ adhesion management system functions are defined in the EN15380-4. They were considered within D3.1 when focusing on the start-up phase of the vehicles. In addition, further functions of the brake/ adhesion management system were defined which also need to be considered in the following.

- G B H a Reuse braking energy
- G B H a Condition braking energy for reuse
- G C Provide deceleration and keep the train at standstill
- G C B a Configure brake system
- G C C a Acquire brake demand
- G C D a Prioritize brake demand select braking mode
- G C E a Allocate braking effort
- G C F a Handle braking due to train configuration, brake mode and demand
- G C G a Apply and release braking forces
- G C H a Provide Wheel Slide Protection
- G D _ a Improve adhesion wheel/rail

Adhesion management sub functions based on EN15380-4 are the following

- G D B a / H E C a / H E C a E Manage sanding,
- G D B a / G D B a D Dry sand, (relevant, failure discovered by regular testing)
- G D B a / G D B a E Heat sand, (relevant, failure discovered by regular testing)
- G D B a / G D B a F Provide sand level (relevant)
- G D B a / G D B a G Command sanding, (relevant, especially also for retention)

When switching to automated rail traffic, there will be functions that are up to now done by the train driver, but in future need to be taken over by the automated system. Those functions are the following:

Brakes:

- Lock bogies in case of brake failures
- Adjust brake percentage, report to control centre (reduced speed, …).

Adhesion Management:

- report availability of adhesion management systems, if considered in braking curves
- Report current adhesion condition based on weather condition or too high WSP activity

4.10.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Functions based on EN15380-4			
Brake: Reuse braking energy	NO	As long the friction brake system is able to handle all deceleration scenarios in the train the reuse of braking energy is only a question efficiency and maintenance intervals.	-
Brake: Condition braking energy for reuse	NO	As long the friction brake system is able to handle all deceleration scenarios in the train the reuse of braking energy is only a question efficiency and maintenance intervals.	-
Brake: Provide deceleration and keep the train at standstill	YES	The brake system is not able to decelerate the train with the requested value, this might cause unintended prolongation of the brake distance or might cause an unintended move of the train.	Mission/Safety
Brake: Configure brake system	YES	If the required configuration cannot be detected or configured the needed configuration is not available and can therefore cause a too high or low brake performance.	Mission/Safety
Brake: Acquire brake demand	YES	If the brake demand cannot be acquired, the brake system is not able to decelerate the train with the requested value, this might cause unintended prolongation of the brake distance or might cause an unintended move of the train.	Mission/Safety
Brake: Prioritize brake demand select braking mode	YES	If the required braking mode cannot be detected the set brake demand can be wrong and therefore cause a too high or low brake performance.	Mission/Safety
Brake: Allocate braking effort	YES	The brake system is not able to command/apply the needed brake effort to the brake (sub-)system.	Mission/Safety
Brake: Handle braking due to train configuration, brake mode and demand	YES	If the brake system is not able to decelerate the train with the requested value, this might cause unintended prolongation of the brake distance or might cause an unintended move of the train.	Mission/Safety

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Brake: Apply and release braking forces	YES	The brake system cannot apply and release brake forces as commanded. This might cause unintended prolongation of the brake distance.	Mission/Safety
Brake: Provide Wheel Slide Protection	NO	The brake system cannot provide the wheel slide protections functionality. A blocked axle gets wheel flats and from a certain wheel flat size the train needs to be put the maintenance shop.	Mission
Brake: Improve adhesion wheel/rail	NO	A wheel slide protection system can improve the wheel/rail adhesion usage and therefore improve the performed deceleration rate.	Mission
AM: Manage sanding	NO	When the sand flow is controlled incorrectly, the sanding effect is reduced. The braking distance might be prolonged compared to correct control. *Note:* *This function is rated mission critical only, as currently sanding is not a safety critical function. At the point adhesion management is accounted to the vehicles' braking curves (e.g. for operation at low adhesion conditions in autumn), the sanding function will be rated safety critical; this is not the case when considered within ATO (mission critical), but when accounted for ATP. This applies to all sanding related topics below. Applying too much sand could be safety critical as well (track circuits).*	Mission
AM: Dry sand, (relevant, failure discovered by regular testing)	NO	When the sand is blocked due to moisture/ water, the sander is not working correctly. The braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed).	Mission
AM: Heat sand, (relevant, failure discovered by regular testing)	NO	When the sand is blocked due to freezing, the sander is not working correctly. The braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed).	Mission
AM: Provide sand level (relevant)	NO	The sand level might be low/ the sand box empty due to missing determination. Operator-specific restrictions might apply (e.g. speed	Mission

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		reduction) or the braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed).	
AM: Command sanding, (relevant, especially also for retention)	NO	The sand extraction is not active due to missing command from outside the sanding system. The braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed).	Mission
Use cases newly defined within D3.1			
AM: Check sanding rate and consistency	NO	When the sand flow is controlled incorrectly, the sanding effect is reduced. The braking distance might be prolonged compared to correct control (e.g. signal/ platform passed).	Mission
AM: Check sand level	NO	When the sand level is low/ empty sand box due to missing measuring, operator-specific restrictions might apply (e.g. speed reduction) or the braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed).	Mission
AM: Check interlocks	NO	If the speed interlock of the sanding function fails, no sand or too much sand is applied between wheelset and rail. The braking distance might be prolonged compared to correct sand extraction (e.g. signal/ platform passed). This function could also be safety critical if too much sand is applied, and the train/ parts of the train are not recognized by track circuits.	Mission
Functions newly defined in D3.2			
Brake: Lock bogies in case of failures	NO	Non-working brakes are detected in a bogie. This requires the bogie to be locked and the brake performance to be reduced.	Mission
Brake: Adjust brake percentage	NO	Result of a failure detection, e.g. a bogie was locked. This requires the adaptation of the brake percentage which was up to then done by the driver.	Mission
AM: Report availability of the Adhesion Management systems	NO	Today e.g. the sanding systems are checked by the driver at start-up of the train who then triggers specific	Mission

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		measures. This needs to be done automatically in future. The same is true for availability detection during driving. If the function to report the availability fails, the safe state would be to consider it as unavailable.	
AM: Report current adhesion condition	NO	Currently the driver reports degraded wheel/rail adhesion conditions, e.g. based on WSP activation. This will in future be done automatically. In case of a failure of the system a backup procedure (running without knowledge on adhesion) will be needed.	Mission

Table 53 – Brake and sanding system running capability impact critical analysis

4.10.2 Monitoring function critical analysis

The functional failures impacting running capability among the Table 53 list are all generally diagnosed in GoA1/2 train. See below table for critical evaluation.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Brake: Provide deceleration and keep the train at standstill	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Configure brake system	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Acquire brake demand	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Prioritize brake demand select braking mode	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Allocate braking effort	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Handle braking due to train configuration, brake mode and demand	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Apply and release braking forces	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Provide Wheel Slide Protection	YES	Depending on existing monitoring function the function must be implemented.	YES
Brake: Improve adhesion wheel/rail	YES	Depending on existing monitoring function the function must be implemented.	YES
AM: Manage sanding	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Dry sand, (relevant, failure discovered by regular testing)	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Heat sand, (relevant, failure discovered by regular testing)	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect	YES

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
		“monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	
AM: Provide sand level (relevant)	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Command sanding, (relevant, especially also for retention)	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Check sanding rate and consistency	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Check sand level	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES
AM: Check interlocks	YES	In general, there can be an automated monitoring of this function for GoA1/2 which shows the status to the driver. Nevertheless, there can still be additional indirect “monitoring” as the driver indirectly experiences the (missing) deceleration when using sand. The reporting is done via the driver to trackside.	YES

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
AM: Report availability of the Adhesion Management systems	YES	The function of reporting the AM system availability cannot be realized by the driver anymore. If an automatic monitoring is available in GoA1/2 already, it can also be used for GoA3/4, but with different flow of information to trackside (not via the driver).	YES
AM: Report current adhesion condition	YES	The function of reporting the current adhesion condition cannot be realized by the driver anymore. If an automatic function is available in GoA1/2 already, it can also be used for GoA3/4, but with different flow of information to trackside (not via the driver).	YES

Table 54 – Brake and sanding system monitoring function critical analysis

4.10.3 New/Updated monitoring function use cases

As shown in the table above (critical analysis) some use cases need to be adjusted during the transition from GoA1/2 to GoA3/4.

The adjustments are in all use cases the same and shown in the table above. They are related to the safety level and the reporting chain will be different / automatised for GoA3/4 (train to trackside).

Use Case	All monitoring capability who needs improvement
ID	UC4.10.1
Actors	TCMS, Brake system
Goal	Monitoring capability must be improved to be ready for GoA3/4. Monitoring must be done with a higher SIL as the redundancy by the driver is not given anymore.
Safety relation	no for ATO, yes for ETCS
Precondition	Driver is for actions (Monitoring) not available. Train is operating (stopped, driving)
Flow of events	1) Any brake related monitoring event detected 2) Event will be sent to TCMS
Post condition	Train is running at lower speed using different deceleration curves for operation (ATO) and protection (ETCS).
Things that can go wrong	Defect not monitored. Prolonged braking distances.
Already implemented risk reduction measures	-
Observations	

Table 55 – Brake system new monitoring use case

Use Case	All monitoring capability who needs improvement
ID	UC4.10.2
Actors	TCMS, Adhesion management system
Goal	Monitoring capability must be improved to be ready for GoA3/4. Monitoring must be done with a higher SIL as the redundancy by the driver is not given anymore.
Safety relation	no for ATO, yes for ETCS
Precondition	Driver is for actions (Monitoring) not available. Train is operating (stopped, driving)
Flow of events	1) Any adhesion management related monitoring event detected 2) Event will be sent to TCMS
Post condition	Train is running at lower speed using different deceleration curves for operation (ATO) and protection (ETCS).
Things that can go wrong	Defect not monitored. Prolonged braking distances.
Already implemented risk reduction measures	-
Observations	

Table 56 – Adhesion management system new monitoring use case

4.10.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Brake: Provide deceleration and keep the train at standstill	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Configure brake system	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Acquire brake demand	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Prioritize brake demand select braking mode	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA4 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Allocate braking effort	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Handle braking due to train configuration, brake mode and demand	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)
Brake: Apply and release braking forces	Depending on the failure a reset of the brake system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.	YES (limited)

Table 57 – Brake and sanding system auto-recovery function critical analysis

4.10.5 New/Updated auto-recovery function use cases

Use Case	All failures limiting the braking capability
ID	UC4.10.3
Actors	Control centre, Train-Ground communication, TCMS, Brake system, ATO onboard/ trackside, ETCS onboard/ trackside
Goal	The train has the ability to move on its own.
Safety relation	no for ATO, yes for ETCS
Precondition	Train is operating (stopped, driving), failure of brake system is true
Flow of events	1) The failure of the brake system is detected. 2) Application dependent the local TCMS will trigger an emergency brake depending on the severity of the failure. 3) This information is transferred to the trackside ATO/ ETCS system via Train-Ground communication. 4) Beyond the failure information is transferred to the onboard ATO/ ETCS system via TCMS. 5) System tries to solve the problem with the auto recovery procedure. If it is successful, train can operate as intended. Otherwise continue with flow of events. 6) Control Centre (trackside ATO) switches to an adjusted different Journey Profile (most probably at reduced speed) and transfers it via Train-Ground communication to the ATO onboard. Control Centre isolates the root cause (failure) if necessary to release the potential emergency brake. 7) The ATO onboard and the ETCS onboard switch to other deceleration values (for ATO and ETCS). 8) Different Journey Profile could be used for TMS and passenger information systems.
Post condition	Train is running at lower speed using different deceleration curves for operation (ATO) and protection (ETCS). Brake system is repaired in the depot at the end of the mission.
Things that can go wrong	Failure detection not successful, prolonged braking distances in all operation modes
Already implemented risk reduction measures	Currently: Isolation of particular brake system(s) is bypassed in emergency brake.
Observations	

Table 58 –Brake system new auto-recovery use case

4.11 HORN

Main function "Manage acoustic warning system" is realized in autonomous train by the implementation of the here below sub-functions, where new-*n* are the new function which D3.1 introduce as possible impact of the transition to GoA3/4:

The following sub-functions of EN15380-4 is involved by horn test:

H E J a	Manage acoustic warning system
K B	Indicate the presence of the vehicle to others
New-1	Switch to backup acoustic warning system

The back-up acoustic warning system include the following sub-functions:

a. Detection of failing primary acoustic system
b. Switch-over to secondary (backup) system

4.11.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Primary horn fails	NO	This is a function failure on vehicle level. If the failure is at local level, then primary horn (in driving direction of train) is not sounding for any reason during requested horn signal. The secondary horn (in opposed travel direction) can act as backup. In this case full functionality is not anymore available, a reduced speed (e.g., to 80 km/h) can be an mitigation.	Safety
Secondary horn fails	YES	This is a function failure on vehicle level. If the failure is that primary horn (in driving direction of train) is not sounding, and switch to secondary horn also fails (as backup) for any reason during requested horn signal.	Mission

Table 59 – Acoustic warning system running capability impact critical analysis

4.11.2 Monitoring function critical analysis

4.11.3 New/Updated monitoring function use cases

4.11.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Activate primary High or Low tone horn: ***No sound available***	The GoA1/2 horn system are resistant to this type of failure (single fault), use High/Low tone horn - no need of auto-recovery function	NO
High and Low tone primary horn not available	By switching over to secondary horn system acoustic warning is possible – with reduced performance	YES

Table 60 – Acoustic warning system auto-recovery functions critical analysis

4.11.5 New/Updated auto-recovery function use cases

Use Case	**Horn Fails - Backup**
ID	**UC4.11.1**
GUID	46AA88DF-C678-46D4-83D1-8763BADF734C
Actor	Primary and secondary horn
Goal	Give acoustic warning
Safety relation	yes
Precondition	Horn activated
Flow of events	1. Horn activated 2. Microphone is not sensing any expected sound 3. Horn recognized as failed 4. Select backup horn on the primarily horn 5. If still no sound signal detected, then ask speed reducing to e.g., with 80 km/h 6. Switch secondary horn ON 7. If still no sound detected >> then ask for mission cancel
Post condition	Backup Horn activated >> acoustic warn signal provided
Things that can go wrong	Microphone senses acoustic warning – without existing signal
Already implemented risk reduction measures	New function – no already implemented measures Placement of horns on vehicle in distributed way to avoid common hit / physical damage
Observations	

Table 61 – Acoustic warning failure new auto-recovery use case

4.12 Communication between Train and Ground

4.12.1 Functional failure impacting running capability

The impact is considered medium/high. The ACS is agnostic in GoA3/4 also, but it must be considered that several services such as the Centralized traffic control (CTC) require an availability of 99.999% that enhance the criticality of the ACS due to the lack of driver (the driver is present into GoA1/2).

The ACS and its equivalents are designed by default to be resilient as it is a selector and monitor of multiple independent radios. Moreover, redundant modems are included in the On-Board certified devices (CENELEC 50129) from the hardware perspective..

The failure of the train-ground communication function is considered mitigated by redundancies foreseen on the system and by the 2.3 auto-recovery rationale.

The train to ground system (ACS, FRMCS, or its equivalents) provides different channels with different Qualities of Service that are provided to the rest of the systems in the train. It assign the channel providing a minimum KPI for the service, this system selects the best communication channel, making the service transparent with best choice available. In case of a service with a channel with not a minimum KPI, the Communication system try to search a new channel with a better quality that could be assigned to the service, transparently for it.

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Minimum bearers to provide communication services to every required GoA3/4 systems are not provided.	YES	- This is a function failure on train level or control centre. - The communication to the control centre is safety relevant in relation to the onboard system, because in GoA3/4 no driver is on the train and the system replaces the observations of the driver. - The virtual driver / control centre can take over the train / mission in a degraded mode when the communication is not provided with a minimum bearers in some services.	Mission
Communication status to the On Board and On Track systems.	YES	- This is a function failure on train level or control centre. - The communication to the control centre is safety relevant in relation to the onboard system, because in GoA3/4 no	Mission

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		driver is on the train and the system replaces the observations of the driver.	
Ground communications with train crew.	NO	- The communication to the train crew is relevant in relation to the onboard system. It is the same case that exist in GoA1/2.	Mission
Communications to passengers from the ground in case of need to inform on how to manage the emergency.	NO	- The virtual driver / control centre can't communicate to the passengers directly when the communication is missing, but Train Crew can communicate to the passengers the information.	Safety
Provision of train / control centre communication failed	YES	- This is a function failure on train level or control centre. - The communication to the control centre is safety relevant in relation to the onboard system, because in GoA3/4 no driver is on the train and the system replaces the observations of the driver. - The virtual driver / control centre can't take over the train / mission when the communication is missing. - .	Mission

Table 62 – Train-ground communication system running capability impact critical analysis

4.12.2 Monitoring function critical analysis

The following tests are defined:

- Test the minimum amount of bearers is available to provide communication services to every required GoA3/4 systems.
- Test communication status between the On-Board and On-Track systems.
- Ground communications with train crew or communication crew or with the PIS (Passenger Information System).

Communication of safety alarm due to failure in any subsystem. Need for action (evacuation, rescue, etc.) (Operation, maintenance)

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Minimum bearers to provide communication services to every required GoA3/4 systems are not provided.	YES	In GoA1/2 the ACS system makes test bearers to provide communication service with the best quality. In GoA3/4 is used the same system to select the best communication service.	NO
Communication status to the On Board and On Track systems.	YES	In GoA1/2 the ACS system makes use of the best channel. In GoA3/4 is used the same system to select the best communication service.	NO
Ground communications with train crew.	YES	In GoA1/2 the ACS system makes use of the best channel. In GoA3/4 is used the same system to select the best communication service.	NO
Communications to passengers from the ground in case of need to inform on how to manage the emergency.	YES	In GoA1/2 the ACS system makes use of the best channel. In GoA3/4 is used the same system to select the best communication service.	NO
Provision of train / control centre communication failed	YES	- The communication between the train and the control centre already exists in GoA1/2 train. ⇒ Monitoring available	NO

Table 63 – Train-ground communication system monitoring functions critical analysis

4.12.3 New/Updated monitoring function use cases

In this chapter, actions performed by the driver in GoA1/2 are examined in order to detect cases requiring manual action which shall be automatically mitigated in GoA3/4.

4.12.4 Auto-recovery functions critical analysis

The analysis of the auto-recovery functions is resumed in the following table.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Test minimum bearers to provide communication services to every required GoA3/4 systems.	In GoA1/2 the ACS system performs bearers tests to provide communication service with the best quality. If the ACS system has no channels, the driver may need to reboot the system. In GoA3/4 the same system is used to select the best communication service. Only in case of the ACS has no channels, as the driver is not present, an automatic reboot may be needed to reboot the system	YES
Communication status to the On Board and On Track systems.	In GoA1/2 the ACS system makes use of the best channel. If the ACS system has no channels, the driver may need to reboot the system. In GoA3/4 the same system is used to select the best communication service. Only in case of the ACS has no channels, as the driver is not present, an automatic reboot may be needed to reboot the system.	YES
Ground communications with train crew.	In GoA1/2 the ACS system makes use of the best channel. If the ACS system has no channels, the driver may need to reboot the system. In GoA3/4 the same system is used to select the best communication service. Only in case of the ACS has no channels, as the driver is not present, an automatic reboot may be needed to reboot the system.	YES
Communications to passengers from the ground in case of need to inform on how to manage the emergency.	In GoA1/2 the ACS system makes use of the best channel. If the ACS system has no channels, the driver may need to reboot the system. In GoA3/4 the same system is used to select the best communication service. Only in case of the ACS has no channels, as the driver is not present, an automatic reboot may be needed to reboot the system.	YES
Provision of train / control centre communication failed	The recovery solution is to use a separate communication system between train and control centre.	NO

Table 64 – Train-ground communication system auto-recovery functions critical analysis

In all the cases the system try to select the best channel, or in case that there is at least a channel, the Virtual driver will be able to connect to the communication system and will be able to diagnose the system. Only in the case that the system is totally isolated and it is not getting any connectivity during a period of time, the system can require a reboot to verify that is not a failure in the on-board communication system. Also if the TCMS could receive a request using the other active channels (ATO or ETCS). It could trigger the reboot.

4.12.1 New/Updated auto-recovery function use cases

Use Case	No Channels available
ID	UC4.12.2
Actor	Communication system or TCMS
Goal	G_12X1: Recovery communication.
Safety relation	
Precondition	Communication system without connectivity in all the channels. KPI defines the minimum level of service. ACS always has a channel available with a minimum KPI, so if ACS has no available channel, it is due to a system failure and then a reboot is required.
Flow of events	1. Send status of each device to remote desk. 2. Measure KPIs of all the channels, in the case of ACS has no available channel, it is due to a system failure and a reboot is required.
Post condition	All GoA3/4 minimum required systems have their On-Board – On-Track segments connected.
Things that can go wrong	At least one essential GoA3/4 system has not On-Board – On-Track segments connected with the minimum required KPIs. 1. Test the alarms and communication crew. 2. Check KPIs for channels reserved for passengers. In case of the flow of events and this “Things that can go wrong” flow, then the safety resides in the affected subsystems.
Already implemented risk reduction measures	
Observations	

Table 65 – Train-ground Communication channel missing availability new auto-recovery use case

4.13 ATO (ATO-AV)

4.13.1 Functional failure impacting running capability

For the purpose of this study, the following logical system architecture is considered where ATO-TS is composed of TD, MD, OE and DM:

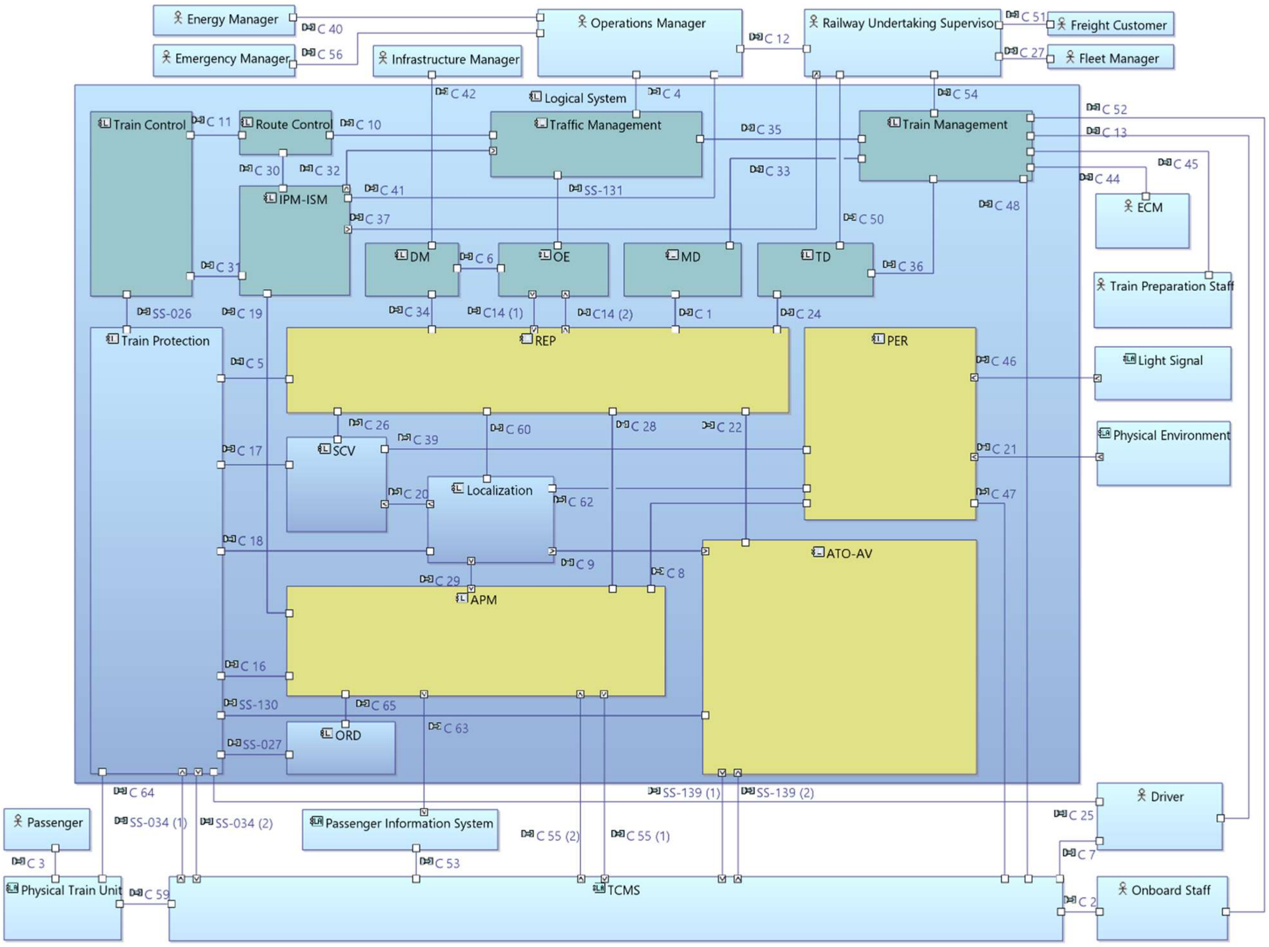


Figure 4 – GoA3/4 Logical Architecture Breakout

The main function of ATO-AV is to generate the signal for traction / brake control in order to follow a speed profile generated using information from ATO-TS (through REP), ATP and other subsystems. It is also responsible for sending door opening and closing commands as well as managing dwell.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
communication with REP failed	YES	no information from REP - ATO-AV cannot work	Mission
communication with ATP failed	YES	no information from ATP - ATO-AV can't work	Mission
communication with LOC failed	YES	no information from LOC - ATO-AV cannot work unless accurate enough key point data is received from SCV	Mission
Communication with TCMS failed	YES	No information from TCMS – ATO-AV cannot work	Mission
ATO-AV software / hardware failure	YES	ATO-AV cannot operate	Mission
ATO-AV runtime error	NO (unless unrecoverable and no redundancy available)	ATO-AV reset, then new start of mission and normal operation (stopping the train possibly necessary if redundancy does not step up or is not present)	Mission (if redundancy does not step up or is not present)

Table 66 – ATO system running capability impact critical analysis

4.13.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN	
communication with REP failed	NO	not implemented in GoA2	YES	New function
communication with ATP failed	YES		YES	In GoA2, ATO-AV goes to FA mode if any failure occurs. In GoA3/4, further actions will be necessary
communication with LOC failed	NO	not implemented in GoA2	YES	New function
ATO-AV software failure	YES		YES	In GoA2, ATO-AV goes to FA mode if any failure occurs. In GoA3/4, further actions will be necessary
ATO-AV hardware failure	YES		YES	In GoA2, the driver continues the mission with manual driving. In GoA3/4 remote driving will be necessary.

Table 67 – ATO system monitoring function critical analysis

4.13.3 New/Updated monitoring function use cases

In this chapter, actions performed by the driver in GoA1/2 are examined in order to detect cases requiring manual action which shall be automatically mitigated in GoA3/4.

Use Case	Testing for loss of operational conditions
ID	UC4.13.1
Actor	Virtual driver
Goal	Check the validity of operational conditions
Safety relation	Not safety relevant since safety is covered by ATP
Precondition	ATO-AV is in AV, RE, or EG mode
Flow of events	ATO-AV has operational conditions
Post condition	ATO-AV continues operation
Things that can go wrong	ATO-AV loses operational conditions, goes to NA mode and applies service brake if train is moving
Already implemented risk reduction measures	In GoA1/2 driver is responsible of proceeding with manual driving. In GoA3/4 train must at least be stopped and a request made to update faulty data until it returns to a consistent state to resume normal operation.
Observations	Possibly additional operational conditions would need to be added such as absence of obstacle detection.

Table 68: ATO Testing for loss of operational conditions new monitoring use case

Use Case	Testing for doors response to opening commands
ID	UC4.13.2
Actor	Virtual driver
Goal	Check that doors opening is working at ATO-AV level
Safety relation	Not safety relevant since doors remain closed.
Precondition	ATO-AV commands door opening
Flow of events	Doors open
Post condition	ATO-AV receives a doors open signal
Things that can go wrong	ATO-AV continues receiving doors closed signal
Already implemented risk reduction measures	It is expected from passenger doors subsystem to address door operation issues.
Observations	Maybe such an incident shall be reported for maintenance staff to check doors.

Table 69: ATO Testing for doors response to opening commands new monitoring use case

Use Case	Testing for doors response to closing commands
ID	UC4.13.3
Actor	Virtual driver
Goal	Check that doors closing is working at ATO-AV level
Safety relation	Not safety relevant since ATP shall prevent train movement if doors are open. Moreover ATO-AV would not try to move if doors are reported as open
Precondition	ATO-AV commands door closing
Flow of events	Doors close
Post condition	ATO-AV receives a doors closed signal
Things that can go wrong	ATO-AV continues receiving doors open signal
Already implemented risk reduction measures	It is expected from passenger doors subsystem to address door operation issues.
Observations	This error would cause failure of mission until ATO-AV receives a doors closed signal

Table 70: ATO Testing for doors response to closing commands new monitoring use case

4.13.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
communication with REP failed	Activation of function does not have immediate impact on train safety. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, ATO-AV changes to FA mode (and service brake shall be triggered)	new
communication with ATP failed	Activation of function does not have immediate impact on train safety. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, ATO-AV changes to FA mode (and service brake shall be triggered)	new
communication with LOC failed	Activation of function does not have immediate impact on train safety. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, ATO-AV changes to FA mode (and service brake shall be triggered)	new
ATO-AV unrecoverable software failure	Activation of function does not have immediate impact on train safety (train movement is supervised by ATP, other situations like starting the train without doors closed are covered by TCMS functions). Reset of ATO-AV software shall be executed. If this reset should not help, ATO-AV changes to FA mode (and service brake shall be triggered)	adaptation

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Loss of operational conditions	Activation of function does not have impact on safety since ATP in responsible for safety.	new
No doors response to opening commands	Activation of function does not have impact on safety since it is expected from other subsystems to not allow train movement in the case ATO-AV tries to depart while doors are actually open (ATO-AV receives doors closed signal).	new
No doors response to closing commands	Activation of function does not have impact on safety since ATO-AV would not try to move if doors are reported as open. However, mission would fail since the train would not be able to depart.	new

Table 71 – ATO system auto recovery functions critical analysis

4.13.5 New/Updated auto-recovery function use cases

Use Case	Communication reset
ID	ATO4
Actor	Virtual Driver
Goal	Reset a faulty communication channel to recover
Safety relation	Not safety relevant since ATO-AV is not considered a safety critical subsystem.
Precondition	Communication is faulty
Flow of events	The faulty communication channel is reset and required session establishment steps performed. ATO state is possibly changed to the state corresponding to the affected channel communication loss scenario.
Post condition	Communication is working again
Things that can go wrong	Communication remains faulty
Already implemented risk reduction measures	Transition to FA mode if the communication channel is mission critical. Otherwise, dispatcher is informed.
Observations	If transitioned to FA mode, remote control would be required.

Table 72: Communication reset

Use Case	ATO-AV reset
ID	ATO5
Actor	Virtual Driver
Goal	Reset ATO-AV to recover from software failure
Safety relation	Not safety relevant since ATO-AV is not considered a safety critical subsystem.
Precondition	ATO-AV software is faulty
Flow of events	ATO-AV is reset
Post condition	ATO-AV is working again
Things that can go wrong	ATO-AV remains faulty
Already implemented risk reduction measures	Transition to FA mode (and service brake activated if train is running).
Observations	Would require remote control in case of permanent failure

Table 73: ATO-AV reset new auto recovery use case

4.14 ATP

4.14.1 Functional failure impacting running capability

The main function of ATP is to protect the train from hazard by checking all operational parameters are consistent and within safe ranges. In case of a safety violation, ATP applies service or emergency brake in order to bring the train back to a safe state.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
communication with REP failed	YES	no information from REP - ATP cannot work	Safety
communication with Train Control failed	YES	no information from ATP - ATP cannot work	Safety
communication with LOC failed	YES	no information from LOC - ATP cannot work	Safety
communication with ORD failed	NO	ATP can fully operate, no technical reason to degrade the operational mode. Operational data are not stored in ORD - possibly legislative problem (for case of incident etc.)	Mission if local regulation authority does not allow running without data recording.
communication with SCV failed	YES	No information from SCV – ATP cannot work	Safety
communication with APM failed	YES	No information from APM – ATP cannot work	Safety
Communication with ATO-AV failed	YES	No information from ATO-AV – ATP can work but remote controlled	Mission
ATP software / hardware failure	YES	ATP cannot operate	Safety
ATP runtime error	NO (unless all required redundant units fail)	ATP reset, then new start of mission and normal operation, redundant units take care of mission continuity in the meantime. Stopping the train mandatory if all required redundant units fail (by another subsystem, possibly APM).	Safety

Table 74 – ATP system running capability impact critical analysis

4.14.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN	
communication with REP failed	NO	not implemented in GoA2 since REP is a concept of future specifications	YES	New function
Communication with Train Control failed	YES		NO	
communication with LOC failed	NO	not implemented in GoA2 since LOC is a concept of future specifications	YES	New function
Communication with ORD failed	YES		NO	
communication with SCV failed	NO	not implemented in GoA2 since SCV is a concept of future specifications	YES	New function
communication with APM failed	NO	not implemented in GoA2 since APM is a concept of future specifications	YES	New function
communication with ATO-AV failed	YES		NO	
ATP software failure	YES		YES	In GoA2, the driver would be responsible of moving the train to a safe place. In GoA3/4, remote control may not be safe enough without ATP

Table 75 – ATP system monitoring function critical analysis

4.14.3 New/Updated monitoring function use cases

In this chapter, actions performed by the driver in GoA1/2 are examined in order to detect cases requiring manual action which shall be automatically mitigated in GoA3/4.

Use Case	**Communication with REP failed**
ID	UC4.14.1
Actor	Virtual driver
Goal	Check communication with REP
Safety relation	Safety critical. If communication with REP fails, train safety cannot be guaranteed since operation data may be outdated or wrong.
Precondition	Communication with REP established
Flow of events	No issue
Post condition	ATP continues proper operation
Things that can go wrong	No data received from REP
Already implemented risk reduction measures	ATP interfaces redundancy. Worst case, stop the train.
Observations	The issue shall be reported and an interface restart can be performed while train is stopped.

Table 76: ATP communication with REP failed new monitoring use case

Use Case	Communication with LOC failed
ID	UC4.14.2
Actor	Virtual driver
Goal	Check communication with LOC
Safety relation	Safety critical. If communication with LOC fails, train safety cannot be guaranteed since location may be outdated or wrong.
Precondition	Communication with LOC established
Flow of events	No issue
Post condition	ATP continues proper operation
Things that can go wrong	No data received from LOC
Already implemented risk reduction measures	ATP interfaces redundancy. Worst case, stop the train.
Observations	The issue shall be reported and an interface restart can be performed while train is stopped.

Table 77: ATP communication with LOC failed new monitoring use case

Use Case	Communication with SCV failed
ID	UC4.14.3
Actor	Virtual driver
Goal	Check communication with SCV
Safety relation	Safety critical. If communication with SCV fails, train safety cannot be guaranteed since signal data may be outdated or wrong.
Precondition	Communication with SCV established
Flow of events	No issue
Post condition	ATP continues proper operation
Things that can go wrong	No data received from SCV
Already implemented risk reduction measures	ATP interfaces redundancy. Worst case, stop the train.
Observations	The issue shall be reported and an interface restart can be performed while train is stopped.

Table 78: ATP communication with SCV failed new monitoring use case

Use Case	Communication with APM failed
ID	UC4.14.4
Actor	Virtual driver
Goal	Check communication with APM
Safety relation	Safety critical. If communication with APM fails, train safety cannot be guaranteed since some critical input may be lost. NOTE: It is not yet defined if APM is safety related or not.
Precondition	Communication with APM established
Flow of events	No issue
Post condition	ATP continues proper operation
Things that can go wrong	No data received from APM
Already implemented risk reduction measures	ATP interfaces redundancy. Worst case, stop the train.
Observations	The issue shall be reported and an interface restart can be performed while train is stopped.

Table 79: ATP communication with APM failed new monitoring use case

Use Case	ATP software failure
ID	UC4.14.5
Actor	Virtual driver
Goal	Check ATP is working as expected
Safety relation	Safety critical. If an issue is detected during ATP runtime, train safety cannot be guaranteed.
Precondition	ATP is working properly
Flow of events	Self-tests pass
Post condition	ATP continues proper operation
Things that can go wrong	Some self-test fails
Already implemented risk reduction measures	ATP redundancy. Worst case, stop the train.
Observations	In GoA1/2 train can be manually driven. In GoA3/4 the issue shall be reported and a restart can be performed while train is stopped.

Table 80: ATP software failure new monitoring use case

4.14.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
communication with REP failed	Activation of function has immediate impact on train safety. Stop the train with emergency brake (after specified timeout has elapsed). Reset of communication shall be executed when train is stopped. If this reset should not help, ATP changes to SF mode.	new
communication with Train Control failed	Activation of function has immediate impact on train safety. Stop the train with emergency brake (after specified timeout has elapsed). Reset of communication shall be executed when train is stopped. If this reset should not help, ATP changes to SF mode.	new
communication with LOC failed	Activation of function has immediate impact on train safety. Stop the train with emergency brake (after specified timeout has elapsed). Reset of communication shall be executed when train is stopped. If this reset should not help, ATP changes to SF mode.	new
communication with ORD failed	Activation of function has no immediate impact on train safety. Reset of communication while train is running (after specified timeout has elapsed) shall be executed. If this reset should not help, ATP may continue operating if local regulations allow or otherwise changes to SF mode (and emergency brake shall be triggered)	adaptation
communication with SCV failed	Activation of function has immediate impact on train safety. Stop the train with emergency brake (after specified timeout has elapsed). Reset of communication shall be executed when train is stopped. If this reset should not help, ATP changes to SF mode.	new
communication with APM failed	Activation of function has immediate impact on train safety. Stop the train with emergency brake (after specified timeout has elapsed). Reset of communication shall be executed when train is stopped. If this reset should not help, ATP changes to SF mode.	new
communication with ATO-AV failed	Activation of function has no immediate impact on train safety. Reset of communication while train is running (after specified timeout has elapsed) shall be executed. If this reset should not help, ATP shall continue operating possibly using remote control driving.	new
ATP software failure	Activation of function has immediate impact on train safety. Train shall be stopped by applying emergency brake. Reset of ATP shall be executed after train has stopped. If this reset should not help, ATP changes to SF mode	adaptation

Table 81 – ATP system auto recovery functions critical analysis

4.14.5 New/Updated auto-recovery function use cases

Use Case	Communication reset
ID	UC4.14.6
Actor	Virtual driver
Goal	Reset a faulty communication channel to recover
Safety relation	Safety relevant since ATP is responsible of train safety and every auto-recovery function shall minimize impact on its operation.
Precondition	Communication is faulty
Flow of events	- Communication interface is reset - Communication is initialised - Data flow is resumed
Post condition	Communication is working again
Things that can go wrong	Communication remains faulty
Already implemented risk reduction measures	Transition to SF mode if the communication channel is mission critical. Otherwise, dispatcher is informed.
Observations	If transitioned to SF mode, there may be no enough safety guarantees to allow for remote control driving.

Table 82: ATP communication reset new auto recovery use case

Use Case	ATP reset
ID	UC4.14.7
Actor	Virtual Driver
Goal	Reset ATP to recover from software failure
Safety relation	Safety relevant since ATP is responsible of train safety and every auto-recovery function shall minimize impact on its operation.
Precondition	ATP software is faulty
Flow of events	- ATP is reset - Initialisation is performed - Operation is resumed
Post condition	ATP is working again
Things that can go wrong	ATP remains faulty
Already implemented risk reduction measures	Transition to SF mode (and emergency brake activated if train is running).
Observations	If transitioned to SF mode, there may be no enough safety guarantees to allow for remote control driving.

Table 83: ATP reset new auto recovery use case

4.15 Positioning System

4.15.1 Functional failure impacting running capability

The main function of Positioning system is to locate the train on a digital map as well as tracking train movement by providing position, train heading and speed signals to other subsystems.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
communication with REP failed	YES	no information from LOC - REP may not be able to retrieve further mission data	Mission
communication with ATP failed	YES	no information from LOC - ATP cannot work	Safety
communication with SCV failed	YES	No information from LOC - SCV environment information may not be accurate/available	Safety
communication with APM failed	YES	No information from LOC - APM may not allow proper operation/may not work	Mission
Communication with ATO-AV failed	YES	No information from LOC - ATO-AV cannot work	Mission
communication with PER failed	YES	At least inaccurate perception	No
LOC software / hardware failure	YES	No location data	Safety
LOC runtime error	NO (unless all redundant units fail)	LOC reset, then wait for an accurate enough location acquisition, redundant units may take care of mission continuity in the meantime.	Safety

Table 84 – Positioning system running capability impact critical analysis

4.15.2 Monitoring function critical analysis

In the communication interfaces considered below, data goes from the positioning subsystem to the other ones. Failure providing location data would affect other subsystems' behaviour.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN	
communication with REP failed	NO	not implemented in GoA2	YES	New function
communication with ATP failed	NO	not implemented in GoA2	YES	New function
communication with SCV failed	NO	not implemented in GoA2	YES	New function
communication with APM failed	NO	not implemented in GoA2	YES	New function
communication with ATO-AV failed	NO	not implemented in GoA2	YES	New function
communication with PER failed	NO	not implemented in GoA2	YES	New function
LOC software failure	NO	In GoA2 was part of ATP	YES	New function

Table 85 – Positioning system monitoring function critical analysis

4.15.3 New/Updated monitoring function use cases

In this chapter, actions performed by the driver in GoA1/2 are examined in order to detect cases requiring manual action which shall be automatically mitigated in GoA3/4.

Use Case	Communication with REP failed
ID	UC4.15.1
Actor	Virtual driver
Goal	Check connectivity with REP (if retained technology allows to do so)
Safety relation	Not safety critical. REP is not a safety critical subsystem hence failure to provide location data would not affect safety.
Precondition	Communication established with REP
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	

Table 86: Positioning system communication with REP failed new monitoring use case

Use Case	Communication with ATP failed
ID	UC4.15.2
Actor	Virtual driver
Goal	Check connectivity with ATP (if retained technology allows to do so)
Safety relation	Safety critical. ATP is a safety critical system and needs accurate and up to date location and speed data in order to operate properly.
Precondition	Communication established with ATP
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	

Table 87: Positioning system communication with ATP failed new monitoring use case

Use Case	Communication with SCV failed
ID	UC4.15.3
Actor	Virtual driver
Goal	Check connectivity with SCV (if retained technology allows to do so)
Safety relation	Safety critical. SCV is responsible for processing perception information which is fed to ATP. Proper obstacle detection and evaluation is required for safety.
Precondition	Communication established with SCV
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	

Table 88: Positioning system communication with SCV failed new monitoring use case

Use Case	Communication with APM failed
ID	UC4.15.4
Actor	Virtual driver
Goal	Check connectivity with APM (if retained technology allows to do so)
Safety relation	Not safety critical. APM is not a safety critical subsystem hence failure to provide location data would not affect safety.
Precondition	Communication established with APM
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	NOTE: It is not yet fully defined if APM is safety related or not.

Table 89: Positioning system communication with APM failed new monitoring use case

Use Case	Communication with ATO-AV failed
ID	UC4.15.5
Actor	Virtual driver
Goal	Check connectivity with ATO-AV (if retained technology allows to do so)
Safety relation	Not safety critical. ATO-AV is not a safety critical subsystem hence failure to provide location data would not affect safety.
Precondition	Communication established with ATO-AV
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	

Table 90: Positioning system communication with ATO-AV failed new monitoring use case

Use Case	Communication with PER failed
ID	UC4.15.6
Actor	Virtual driver
Goal	Check connectivity with PER (if retained technology allows to do so)
Safety relation	Not safety critical. PER is not a safety critical subsystem hence failure to provide location data would not affect safety.
Precondition	Communication established with PER
Flow of events	Positioning subsystem provides location
Post condition	Communication is alive
Things that can go wrong	Communication is lost
Already implemented risk reduction measures	
Observations	

Table 91: Positioning system communication with PER failed new monitoring use case

Use Case	Positioning software failure
ID	UC4.15.7
Actor	Virtual driver
Goal	Check positioning software is working as expected
Safety relation	Safety critical. If positioning functionality is missing, ATP which is safety critical will not be able to work properly.
Precondition	Positioning is working properly
Flow of events	Positioning subsystem provides location
Post condition	Positioning is working properly
Things that can go wrong	Positioning software failure
Already implemented risk reduction measures	Use of redundancy is possible.
Observations	A software failure may be logged in order to fix it.

Table 92: Positioning software failure new monitoring use case

4.15.4 Auto-recovery functions critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
communication with REP failed	Activation of function does not have immediate impact on train safety because it would affect digital map data and ATP can operate without that. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, remote control driving shall be used if possible.	new
communication with ATP failed	Activation of function has immediate impact on train safety because ATP's capacity to monitor train location and speed would be affected. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, ATP will change to SF mode as part of its failure management.	new
communication with SCV failed	Activation of function has immediate impact on train safety because obstacle detection capacity would be altered. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, remote control driving shall be used if possible.	new
communication with APM failed	Activation of function does not have immediate impact on train safety because APM not being able to work properly does not affect ATP operation. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, remote control driving shall be used if possible.	new
communication with ATO-AV failed	Activation of function does not have immediate impact on train safety because ATP would still cover train safety. Reset of communication (after specified timeout has elapsed) shall	new

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	be executed. If this reset should not help, remote control driving shall be used if possible.	
communication with PER failed	Activation of function does not have immediate impact on train safety because SCV would be able to detect a problem in PER data and notify ATP of obstacle detection issues. Reset of communication (after specified timeout has elapsed) shall be executed. If this reset should not help, remote control driving shall be used if possible.	new
LOC software failure	Activation of function has immediate impact on train safety because no location and speed data would be available to other subsystems. Reset of positioning system shall be executed. If this reset should not help, ATP will change to SF mode as part of its failure management.	adaptation

Table 93 – Positioning system auto recovery functions critical analysis

4.15.5 New/Updated auto-recovery function use cases

Use Case	Communication reset
ID	UC4.15.8
Actor	Virtual driver
Goal	Reset a faulty communication channel to recover
Safety relation	Safety relevant in case of ATP and SCV communication. Every auto-recovery function shall minimize impact on positioning information.
Precondition	Communication is faulty
Flow of events	- Communication interface is reset - Positioning information sending is resumed
Post condition	Communication is working again
Things that can go wrong	Communication remains faulty
Already implemented risk reduction measures	Mitigation measures implemented by consumer subsystems. Dispatcher is informed.
Observations	

Table 94: Positioning system communication reset new auto-recovery use case

Use Case	LOC reset
ID	UC4.15.9
Actor	Virtual Driver
Goal	Reset LOC to recover from software failure
Safety relation	Safety relevant since LOC is responsible of providing location information to ATP.

Precondition	LOC software is faulty
Flow of events	- LOC is reset - full initialisation is performed - positioning information is acquired
Post condition	LOC is working again
Things that can go wrong	LOC remains faulty
Already implemented risk reduction measures	Mitigation measures implemented by consumer subsystems. Dispatcher is informed.
Observations	

Table 95: Positioning system communication reset new auto recovery use case

4.16 PERCEPTION SYSTEM

The perception system (consists of equipment such as radar, LiDAR, camera sensors, digital map and mission data) replaces the observations of the driver. The automatic activation of functions via vehicle control unit replaces the handling of the driver to carry out the observations to an action (e. g. accelerate or brake the train).

The perception system for the cab view of the driver is a new functionality and is safety relevant because the autonomous GoA 3/4 train (without a driver) can only operate with a complete functional perception system.

Main function “Provide perception system (for the cab view of the driver)” is realized in autonomous train by the implementation of the here below sub-functions, where new-n are the new function which D3.1 introduce as possible impact of the transition to GoA3/4.

The following sub-functions according to standard EN15380-4 are involved by the perception system:

Level					Function description	Example / Explanation
1[1]	**2**	**3**				
J	B				guide the train	
J	B	D	a[2]		observe obstacles on the track	observe possible presence of obstacles on track during the mission of vehicle
J	B	D	a	B	track obstacles inside the clearance profile	receive external sensors via sensors
J	B	D	a	C	signalize obstacles inside the clearance profile	report the obstacle to external monitoring system
K	D	C	a		provide train / control centre communication	
K	D	C	a	F	send train position to control centre	
K	E				provide automatic train control (ATC)	
K	E	B			provide automatic train protection (ATP)	
K	E	C			provide automatic driving mode (ATO)	
NEW-1					provide digital map for perception system	Digital map includes the static data of the track for train control
NEW-2					provide mission data for perception system	Mission data includes the dynamic track data for train control

[1] Level 1, Identifier ‘J’ ≙ Secure and guide the track of the train, Identifier ‘K’ ≙ Integrate vehicle into the overall system railway

[2] Identifier ‘a’ ≙ For this sub-function will be specified further sub-functions on a lower level in attachment A of the standard EN15380-4.

4.16.1 Functional failure impacting running capability

Based on the defined sub-functions the impact analysis on the running capability was carried out.

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
Observation of obstacles on the track failed	YES	- This is a function failure on train level. - The missing observation of obstacles can lead to serious consequences for the train and the passengers in the case of a crash with an obstacle. - The mission / train must be stopped immediately (e. g. at the current train station).	Safety
Tracking of obstacles inside the clearance profile failed	YES	- This is a function failure on train level. - The missing tracking of obstacles can lead to serious consequences for the train and passengers in the case of a crash with an obstacle. - The mission / train must be stopped immediately (e. g. at the current train station).	Safety
Signalizing of obstacles inside the clearance profile failed	YES	- This is a function failure on train level. - The missing signalizing of obstacles can lead to serious consequences for the train and passengers in the case of a crash with an obstacle. - The mission / train must be stopped immediately (e. g. at the current train station).	Safety
Provision of train / control centre communication failed	YES	The functioning communication between the train and the control centre is important / relevant for the perception system, as the control centre must have the possibility to occupy the train, drive the train or continue the mission (bring the train at a significant reduced speed into a safe position) at any time, with the data of the perception system being transmitted via the communication. (Three different communication channels between train and ground are identified, details see chapter 2.3. The management and the assurance of the communication between train and ground handled in chapter 4.12.)	Mission

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		- This is a function failure on train level or control centre. - The communication to the control centre is safety relevant in relation to the perception system, because in GoA3/4 no driver is on the train and the perception system replaces the observations of the driver. - The virtual driver / control centre can't take over the train / mission when the communication is missing. - If one of the three different communication channels (between train and ground) fails, the virtual driver / control centre can occupy the train (with one of the two remaining communication channels) and continue the mission. Otherwise, the mission / train would have to be stopped (e. g. at the current train station or at a safe position).	
Sending of train position to control centre failed	YES	The functioning position sending of the train to the control centre is important / relevant for the perception system, as the control centre needs to know the position of the train at any time to bring the train at a significant reduced speed into a safe position in case of danger (in combination with the data from the digital map and the mission data). - This is a function failure on train level. - The sending of the position to the control centre is mission relevant in relation to the perception system, because in GoA3/4 no driver is on the train and thus the position of the train must be submitted. - If the position transmission to the control centre fails, the position of the train can alternatively be determined using the current data of the digital map and the mission data (as an autonomous on-board positioning system). This redundancy enables the virtual driver to bring the train at a	Mission

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
		significant reduced speed into a safe position. Otherwise, the mission / train would have to be stopped (e. g. at the current train station).	
Communication with automatic train protection (ATP) failed	YES	- This is a safety-related function failure on train level. - The communication with ATP is relevant for the conversion of the balise signal and the adherence of the permitted train speed. - The driver monitors manually the permitted train speed and if necessary reduces manually the train speed to the specified speed.	Safety
Communication with automatic driving mode (ATO) failed	YES	- This is a function failure on train level. - The mission can be continued, the driver performs manually the functions of the ATO (e. g. accelerate or brake the train).	Mission
Provision of digital map failed	YES	- This is a function failure on train level. - The provision of the digital map is relevant because the digital map includes the static data about the track (segment profiles, position of signal masts or tunnel, gradient of track, etc.). - The mission can be continued with significantly reduced train speed.	Mission
Provision of mission data failed	YES	- This is a function failure on train level. - The provision of the mission data is relevant because the mission data includes the dynamic track data (journey profiles, speed limits, friction value of track, weather, etc.) - The mission can be continued with significantly reduced train speed.	Mission

Table 96 – Perception system running capability impact critical analysis

4.16.2 Monitoring function critical analysis

The monitoring function analysis is summarised in the following table.

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Observation of obstacles on the track failed	NO	- In GoA1/2 train, the observation is the task of the driver. - The observation of obstacles by a perception system is not implemented in GoA1/2 train. ⇒ No monitoring available	YES
Tracking of obstacles inside the clearance profile failed	NO	- In GoA1/2 train, the tracking is the task of the driver. - The tracking of obstacles by a perception system is not implemented in GoA1/2 train. ⇒ No monitoring available	YES
Signalizing of obstacles inside the clearance profile failed	NO	- In GoA1/2 train, the signalizing (≙ the reaction on the obstacle) is the task of the driver. - The signalizing of obstacles by a perception system is not implemented in GoA1/2 train. ⇒ No monitoring available	YES
Provision of train / control centre communication failed	YES	- The communication between the train and the control centre already exists in GoA1/2 train. ⇒ Monitoring available	NO
Sending of train position to control centre failed	NO	- In GoA1/2 train this data is sent at lower frequency for traffic management purposes. ⇒ No monitoring available	YES
Provision of automatic train protection (ATP) failed	YES	- The ATP system is already implemented in GoA1/2 train. ⇒ Monitoring available	NO
Provision of automatic driving mode (ATO) failed	YES	- The ATO system is already implemented in GoA1/2 train. - ⇒ Monitoring available	NO
Provision of digital map failed	YES	- In GoA2 train, the transmission of the segment profiles and the journey profiles are implemented via subset 126 (interface between ATO track side and ATO onboard) and via subset 130 (interface between ATO onboard and ETCS onboard). ⇒ Monitoring available	NO
Provision of mission data failed	YES	- In GoA2 train, the transmission of the segment profiles and the journey profiles are implemented via subset 126 (interface between ATO track side and ATO onboard) and via subset 130 (interface between ATO onboard and ETCS onboard). ⇒ Monitoring available	NO

Table 97 – Perception system monitoring function critical analysis

4.16.3 New/Updated monitoring function use cases

In this chapter, actions performed by the driver in GoA1/2 are examined in order to detect cases requiring manual action which shall be automatically mitigated in GoA3/4.

Use Case	Monitoring of observation function
ID	UC4.16.1
Actor	Virtual driver
Goal	G_PerSys1: Make sure the observation function of the perception system is available and functioning within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal for observation is safety relevant
Precondition	- Electric power supply available - Testing of RAD/LID/CAM-sensors availability
Flow of events	1. Monitoring RAD/LID/CAM-sensors (for observation function) ON 2. Monitoring power supply for sensors (for observation function) is provided 3. Monitoring each signal of RAD/LID/CAM-sensors (for observation function) and check for possible detected sensor failure. 4. TCMS sends diagnostic message of perception system to control centre. 5. The virtual driver analyses the fault situation. 6. The virtual driver decides the further steps such as - the restart of the perception system - taking over the train to continue the mission - stopping the mission and bringing the train into a safe position
Post condition	Inform the TCMS / control centre / virtual driver whether the observation function of the perception system is working in the specified range and the sensor signals are plausible.
Things that can go wrong	Sensor dirty, sensor faulty, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the observation function is continuously done.

Table 98 – Perception observation function new monitoring use case

Use Case	Monitoring of tracking function
ID	UC4.16.2
Actor	Virtual driver
Goal	G_PerSys2: Make sure the tracking function of the perception system is available and functioning within the technical specifications.
Safety relation	- Tracking of the obstacles inside the clearance profile - RAD/LID/CAM-sensor signal for tracking is safety relevant
Precondition	- Electric power supply available - Testing of RAD/LID/CAM-sensors availability
Flow of events	1. Monitoring RAD/LID/CAM-sensors (for tracking function) ON 2. Monitoring power supply for sensors (for tracking function) is provided 3. Monitoring each signal of RAD/LID/CAM-sensors (for tracking function) and check for possible detected sensor failure. 4. TCMS sends diagnostic message of perception system to control centre. 5. The virtual driver analyses the fault situation. 6. The virtual driver decides the further steps such as - the restart of the perception system - taking over the train to continue the mission - stopping the mission and bringing the train into a safe position
Post condition	Inform the TCMS / control centre / virtual driver whether the tracking function of the perception system is working in the specified range and the sensor signals are plausible.
Things that can go wrong	Sensor dirty, sensor faulty, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the tracking function is continuously done.

Table 99 – Perception tracking function new monitoring use case

Use Case	Monitoring of signalizing function
ID	UC4.16.3
Actor	Virtual driver
Goal	G_PerSys3: Make sure the signalizing function of the perception system is available within the technical specifications.
Safety relation	- Signalizing of the obstacles inside the clearance profile - Signalizing of obstacles to vehicle control unit and ATP is safety relevant
Precondition	- Electric power supply available
Flow of events	1. Monitoring vehicle control unit and ATP ON 2. Monitoring power supply for vehicle control unit and ATP is provided 3. TCMS sends diagnostic message of perception system to control centre. 4. The virtual driver analyses the fault situation. 5. The virtual driver decides the further steps such as - the restart of the perception system - taking over the train to continue the mission - stopping the mission and bringing the train into a safe position
Post condition	Inform the TCMS / control centre / virtual driver whether the signalizing function of the perception system is working.
Things that can go wrong	Communication to vehicle control unit and ATP failed, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the signalizing function is continuously done.

Table 100 – Perception signalizing function new monitoring use case

Use Case	Monitoring of position transmit function
ID	UC4.16.4
Actor	Control centre / Virtual driver
Goal	G_PerSys4: Make sure the receiver for positioning system (for transmitting the train position) and its signal is available within the technical specifications.
Safety relation	- Position of the train - Receiving of positioning system signal is safety relevant
Precondition	- Electric power supply available
Flow of events	1. Monitoring receiver of positioning system ON 2. Monitoring power supply for receiver of positioning system is provided 3. TCMS sends diagnostic message of positioning system receiver to control centre. 4. The control centre / virtual driver analyses the fault situation. 5. The control centre / virtual driver decides the further steps such as - the restart of the receiver - taking over the train to continue the mission using the current data of the digital map and the mission data (as an autonomous on-board positioning system) - bringing the train into a safe position (using the current data of the digital map and the mission data) and stopping the mission
Post condition	Inform the TCMS / control centre / virtual driver whether the receiver of positioning system is power supplied, is working in defined current and voltage limits and the received positioning system signal is available.
Things that can go wrong	Receiver faulty, positioning system signal not available, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the receiver for the positioning system is continuously done.

Table 101 – Perception position transmit function new monitoring use case

Use Case	Monitoring of digital map availability and relevance
ID	UC4.16.5
Actor	Control centre / Virtual driver
Goal	G_PerSys5: Make sure the digital map of the perception system is available and actual.
Safety relation	- Digital map is safety relevant (orientation at infrastructure and influencing the train driving behaviour)
Precondition	- Electric power supply available - Testing of digital map actuality
Flow of events	1. Monitoring vehicle control unit ON 2. Monitoring power supply for vehicle control unit is provided 3. TCMS sends diagnostic message of digital map to control centre. 4. The control centre / virtual driver analyses the fault situation. 5. The control centre / virtual driver decides the further steps such as - the restart of the vehicle control unit - taking over the train to continue the mission - stopping the mission and bringing the train into a safe position
Post condition	Inform the TCMS / control centre / virtual driver whether the digital map of the perception system is available and actual.
Things that can go wrong	Vehicle control unit not available, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the digital map availability is continuously done.

Table 102 – Perception digital map availability new monitoring use case

Use Case	Monitoring of mission data availability and relevance
ID	UC4.16.6
Actor	Control centre / Virtual driver
Goal	G_PerSys6: Make sure the mission data of the perception system is available and actual.
Safety relation	- Mission data is safety relevant (orientation at infrastructure and influencing the train driving behaviour)
Precondition	- Electric power supply available - Testing of mission data actuality
Flow of events	1. Monitoring vehicle control unit ON 2. Monitoring power supply for vehicle control unit is provided 3. TCMS sends diagnostic message of mission data to control centre. 4. The control centre / virtual driver analyses the fault situation. 5. The control centre / virtual driver decides the further steps such as - the restart of the vehicle control unit - taking over the train to continue the mission - stopping the mission and bringing the train into a safe position
Post condition	Inform the TCMS / control centre / virtual driver whether the mission data of the perception system is available and actual.
Things that can go wrong	Vehicle control unit not available, power supply not provided
Already implemented risk reduction measures	The train is fully equipped to perform the monitoring.
Observations	The monitoring of the mission data availability is continuously done.

Table 103 – Perception mission data availability new monitoring use case

4.16.4 Auto-recovery functions critical analysis

The analysis of the auto-recovery functions is resumed in the following table.

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
Observation of obstacles on the track failed	- In GoA1/2 train, the observation of the track and the clearance profile is the task of the driver. - The "recovery solution" is, that another driver takes over the mission, if the planned driver for the mission is absent. - If one of the components for the track observation of the perception system (such as radar, LiDAR or camera sensors) for the GoA3/4 train failed, the remote driving takes over the mission and thus the task of the perception system (with the still working components). - If the perception system completely "absent" (e. g. due to CAN-bus communication failure), the remote driving should bring the train at a significant reduced speed into a safe position.	YES
Tracking of obstacles inside the clearance profile failed	- In GoA1/2 train, the observation of the track and the clearance profile is the task of the driver. - The recovery solution is, that another driver takes over the mission, if the planned driver for the mission is absent. - If one of the components for the obstacles tracking of the perception system (such as radar, LiDAR or camera sensors) for the GoA3/4 train failed, the remote driving takes over the mission and thus the task of the perception system (with the still working components). - If the perception system completely "absent" (e. g. due to CAN-bus communication failure), the remote driving should bring the train at a significant reduced speed into a safe position.	YES
Signalizing of obstacles inside the clearance profile failed	- In GoA1/2 train, the observation of the track and the clearance profile and the processing of the observation ("signalizing") are the tasks of the driver. - The recovery solution is, that another driver takes over the mission, if the planned driver for the mission is absent.	YES
Provision of train / control centre communication failed	- The recovery solution is to use one of the three different communication channels between train and ground (details see also chapter 2.3). - In GoA3/4 trains, the digital train radio GSM-R will be used.	NO
Sending of train position to control centre failed	- In GoA1/2 train, the observation of the kilometer boards and the transmission of the position to the control centre are the tasks of the driver. - The recovery solution is, that another (real) driver (in GoA1/2 trains), if the planned driver for the mission is	YES

FUNCTIONAL FAILURE	GoA1/2 TRAIN AUTO-RECOVERY SOLUTION CRITICAL EVALUATION	ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
	absent or the virtual driver (in GoA3/4 trains) takes over the mission. - If the position transmission to the control centre fails in GoA3/4 trains, the position of the train can alternatively be determined using the current data of the digital map and the mission data (as an autonomous on-board positioning system). This redundancy enables the virtual driver to bring the train at a significant reduced speed into a safe position.	
Provision of digital map failed	- In GoA1/2 train, the segment profiles and the journey profiles are transmitted to the driver via subset 126 (interface between ATO track side and ATO onboard) and via subset 130 (interface between ATO onboard and ETCS onboard).	NO
Provision of mission data failed	- In GoA1/2 train, the segment profiles and the journey profiles are transmitted to the driver via subset 126 (interface between ATO track side and ATO onboard) and via subset 130 (interface between ATO onboard and ETCS onboard).	NO

Table 104 – Perception system auto-recovery functions critical analysis

4.16.5 New/Updated auto-recovery function use cases

Use Case	Auto-recovery of observation function
ID	UC4.16.7
Actor	TCMS / Control centre / Virtual driver
Goal	G_PerSys-Rec1: Make sure the observation function of the perception system is automatically recovered and available again within the technical specifications.
Safety relation	Yes
Precondition	The observation of the obstacles on the track failed.
Flow of events	1. Failure of one of the components (such as radar, LiDAR or camera sensors) for the observation function of perception system 2. The train reduces significantly the speed. 3. Control centre will be informed (diagnostic message) and checks the affected component via remote control. 4. If the function of the affected component cannot auto-recovered (e. g. by a reset), the virtual driver takes over the mission (supported by the still working components of the perception system) and leads the train into a safe position or to the next railway station. 5. The control centre / virtual driver decides depending on the degradation of the perception system whether the mission can be continued at a significant reduced speed or whether the mission ends at the safe position.
Post condition	The perception system needs to be inspected, the affected component for the observation function must be repaired / replaced and tested.
Things that can go wrong	
Already implemented risk reduction measures	The train is fully equipped to perform the auto-recovery.
Observations	

Table 105 – Perception observation function new auto-recovery use case

Use Case	Auto-recovery of tracking function
ID	UC4.16.8
Actor	TCMS / Control centre / Virtual driver
Goal	G_PerSys-Rec2: Make sure the tracking function of the perception system is automatically recovered and available again within the technical specifications.
Safety relation	Yes
Precondition	The tracking of the obstacles inside the clearance profile failed.
Flow of events	1. Failure of one of the components (such as radar, LiDAR or camera sensors) for the tracking function of perception system 2. The train reduces significantly the speed. 3. Control centre will be informed (diagnostic message) and checks the affected component via remote control. 4. If the function of the affected component cannot auto-recovered (e. g. by a reset), the virtual driver takes over the mission (supported by the still working components of the perception system) and leads the train into a safe position or to the next railway station. 5. The control centre / virtual driver decides depending on the degradation of the perception system whether the mission can be continued at a significant reduced speed or whether the mission ends at the safe position.
Post condition	The perception system needs to be inspected, the affected component for the tracking function must be repaired / replaced and tested.
Things that can go wrong	
Already implemented risk reduction measures	The train is fully equipped to perform the auto-recovery.
Observations	

Table 106 – Perception tracking function new auto-recovery use case

Use Case	Auto-recovery of signalizing function
ID	UC4.16.9
Actor	TCMS / Control centre / Virtual driver
Goal	G_PerSys-Rec3: Make sure the signalizing function of the perception system is automatically recovered and available again within the technical specifications.
Safety relation	Yes
Precondition	The signalizing of the obstacles inside the clearance profile failed.
Flow of events	1. Failure of signalizing function of perception system 2. The train reduces significantly the speed. 3. Control centre will be informed (diagnostic message) and checks the signalizing function via remote control. 4. The virtual driver takes over the mission and leads the train to the next railway station. 5. The mission ends.
Post condition	The perception system needs to be inspected, the affected component for the signalizing function must be repaired / replaced and tested.
Things that can go wrong	
Already implemented risk reduction measures	The train is fully equipped to perform the auto-recovery.
Observations	

Table 107 – Perception signalization function new auto-recovery use case

Use Case	Auto-recovery of position transmit function
ID	UC4.16.10
Actor	TCMS / Control centre / Virtual driver
Goal	G_PerSys-Rec4: Make sure the function for transmission of the train position is automatically recovered and available again within the technical specifications.
Safety relation	Yes
Precondition	The transmission of the train position failed.
Flow of events	1. Failure of position transmit function of perception system 2. The train reduces significantly the speed. 3. Control centre will be informed (diagnostic message) and checks the position transmit function via remote control. 4. The virtual driver takes over the mission and can continue the mission at a significant reduced speed using the current data of digital map and mission data (as an autonomous on-board positioning system) or can lead the train into a safe position or to the next railway station. 5.
Post condition	The perception system needs to be inspected, the components for the positioning system must be repaired / replaced and tested.
Things that can go wrong	
Already implemented risk reduction measures	The train is fully equipped to perform the auto-recovery.
Observations	

Table 108 – Perception position transmit function new auto-recovery use case

4.17 TCMS

4.17.1 Functional failure impacting running capability

The running capability impact analysis is resumed in the following table.

FUNCTIONAL FAILURE	RUNNING CAPABILITY IMPACT		MISSION/SAFETY FAILURE
TCMS	no	TCMS has redundancies making the system single fault resistant. Therefore, TCMS does not impact on running capability	

Table 109 – TCMS running capability impact critical analysis

4.17.2 Monitoring function critical analysis

FUNCTIONAL FAILURE MONITORING	GoA1/2 TRAIN MONITORING CAPABILITY PRESENCE/EVALUATION		ADAPTATION/ NEW USE CASE FOR GoA3/4 TRAIN
TCMS	yes	TCMS monitoring is done by control Unit. If any failure is detected, the control unit take appropriate action to rectify the situation. This may include adjusting the train's speed, applying emergency brakes, or even shutting down the train in extreme cases. Operating a train without the TCMS is not ideal and can be more challenging and potentially less safe than operating with a fully functional TCMS. Therefore, it is essential to have backup systems and procedures in place to ensure safe and reliable train operation in the event of a TCMS failure. This should be control by control center in GoA3/4	yes

Table 110 – TCMS monitoring function critical analysis

4.17.3 New/Upated monitoring function use cases

Use Case	Failure of TCMS
ID	UC4.17.1
Actors	TCMS, operation center
Goal	Enable remote actions when TCMS is down
Safety relation	yes
Precondition	Failure of TCMS system
Flow of events	-Connect to the backup system of TCMS -Move train to the closest safe area -Let trains on the same track be aware that TCMS connection of this specific train is lost
Post condition	Control center should be informed to take action.
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 111 – TCMS failure new monitoring use case

4.17.4 Auto-recovery functions critical analysis

In case of Failure of TCMS a reset of the system might be necessary. In GoA1/2 systems this might be done by the driver, the train attendant for GoA3 or via remote connection to trackside for GoA3/4. For other failures, like hardware failures, no recovery will be possible.

4.17.5 New/Upated auto-recovery function use cases

Use Case	Failure of TCMS autorecovery
ID	UC4.17.1
Actors	TCMS, operation center
Goal	Enable remote actions when TCMS is down
Safety relation	yes
Precondition	Failure of TCMS system
Flow of events	-Remote driver switch battery supply off and on -all systems start in low voltage mode
Post condition	Control center should be informed to take action.
Things that can go wrong	
Already implemented risk reduction measures	
Observations	

Table 112 – TCMS autorecovery use case

5 CONCLUSIONS

The functional failures impacting the running capability have the biggest effect among all the ones impacting the mission reliability because they interrupt traffic on the line

The transition from GoA1/2 to GoA3/4 trains introduces an element of complexity in managing such a type of failures, due to the absence of train driver and crew, instructed to put in place the necessary actions to exit from any condition blocking indefinitely the train.

GoA3/4 trains, due to the absence of the driver, shall have therefore new functionalities, that introduce additional failures elements impacting the running capability.

The method used for the critical analysis of all the functional failures impacting the running capability and their diagnosis (described in chapter 3) is the initial achievement of the working group, because gave a common way of working to all contributors, introducing uniformity in the definition of the analysis outputs, which are:

- New monitoring functions use cases.
- New auto-recovery functions use cases.

The impact on running capability is linked to failures of functions permitting the train to run (traction, …) or failures of safety relevant functions that in case of failure enter in a safe state stopping the train.

GoA1/2 monitoring and auto-recovery solutions are in most of the cases applicable, with the difference that any action performed by the driver shall be performed by a train *automatic* reaction or by the *ground* staff, via remote control, or that adaptation of the existing functions are required.

The remote-controlled trouble shooting or reset has been chosen several times as auto-recovery solution (see for example Table 5, Table 29, Table 43, Table 51)

This solution could overload the control centre, therefore a possible development for the future could be the study of possible replacement of remote-controlled solutions with automatic reaction by the train wherever it is possible.

Single failure resistant solutions are of course also used to manage the auto-recovery use cases (see for example chapters 4.2.2, 4.4.2, 4.4.4, 4.11.4, 4.12.4), as well as automatic reset or isolations (see for example Table 20, Table 38, Table 72, Table 73, Table 82, Table 94).

The analysis identified of course that train ground communication becomes in GoA3/4 a crucial function, because it permits the ground to take the control of the train in case of failures that the train is not capable to solve autonomously by proper auto-recovery functionalities. Therefore, the loss of this functionality must be limited as much as possible by redundant and reliable system, as described in initial chapter 2.3.

Any loss of communication can impact the running capability due to the presence of interfaces between the systems permitting to replace the driver (which normally collect, in these cases, information and act accordingly). Refer to chapters about ATP, ATO, Positioning, Perception.

In some cases additional tests at the start of the mission, scope of former task 3.1, are identified (see for example Table 15).

As a conclusion the outcome can be resumed as follow:

- ❖ Monitoring solution for GoA3/4 train
  - On board existing GoA1/2 monitoring functions
  - Trouble shooting by virtual driver
  - New tests to be performed at the start of the mission
  - Monitoring of new functionalities necessary due to transition to GoA3/4

4) Auto-recovery solutions for GoA3/4 trains
   - Redundant/single fault tolerance systems
   - Automatic reset or isolations or other autonomous auto-recovery actions
   - Remote controlled reset or isolations or auto-recovery actions

Examples of new monitoring and auto-recovery solutions which could be used:

- Broadcasting warning (for example in case of train with external light failed)
- Back-up door closing
- Remote controlled doors isolation system
- Passenger Emergency Egress device auto-reset or remote controlled, to close the doors and move the empty train from the line to the depo in case of passenger emergency detrainment
- Remote controlled mechanical isolations (pneumatic cocks)
- On board digital maps, used as an autonomous on-board positioning system to continue the mission or lead the train into a safe position or to the next railway station.

REFERENCES

[1] EN15380-4 - Railway applications – Classification system for railway vehicles – Part 4: Function groups

[2] EN16334 - Railway applications — Passenger Alarm System — System requirements

[3] EN16185-1 (2014+A1:2020 (E)) - Railway applications - Braking systems of multiple unit trains - Part 1: Requirements and definitions

[4] EN15734-1 (2010 + AC:2013 (E)) - Railway applications - Braking systems of high speed trains - Part 1: Requirements and definitions

[5] CEN/TS 15427-1-3 (2021 (D)) - - Railway applications - Wheel/Rail friction management - Part 1-3: Equipment and Application - Adhesion materials

[6] EN50553 – Railway applications – Requirements for running capability in case of fire on board of rolling stocks