TECHNOLOGIES FOR THE AUTONOMOUS RAIL OPERATION

D3.1 – Contribution to enhanced TCMS for automatic diagnostic functionality regarding autonomous train: ATO automatic functional test

Due date of deliverable: 31/03/2022

Actual submission date: 28/06/2022

Leader/Responsible of this Deliverable: Paolo Piccione

Reviewed: Y

Document status		
Revision	Date	Description
01	19/11/2021	First issue
02	14/12/2021	Document update for all chapters.
03	02/02/2022	Document update for all chapters based on reviews
04	22/04/2022	Document update for all chapters based on last contributions and reviews
05	14/06/2022	Document update for all chapters based on last contributions and riorganisation of document structure
06	28/06/2022	Final. Accepted by SC.

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: 42 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

Contr. ID	Resp.	Contrib.	Contribution	Chapter	Weight
D3.1_1	DB	BT	Fire Protection Test	4.1	4%
D3.1_2	BT	DB	Internal and External Lights Test	4.2	4%
D3.1_3	FTI	BT, SNCF-V	Passenger Alarm Test	4.3	7%
D3.1_4	FTI	KB	Passenger Door Test	4.4	7%
D3.1_5	DB	BT	Pantograph Test	4.5	4%
D3.1_6	BT	DB	Auxiliaries Power Supply Test	4.6	3%
D3.1_7	BT	DB	Low Voltage System Test	4.7	4%
D3.1_8	KB	FTI	Air Generation and Treatment Unit Test	4.8	7%
D3.1_9	DB	BT	Traction Test	4.9	4%
D3.1_10	KB	FT	Brake Test	4.10	9%
D3.1_11	BT	DB	Horn test	4.11	4%
D3.1_12	INDRA	MERMEC, CAF SIG	Communication between Train and Ground	4.12	4%
D3.1_13	CAF SIG	AZD, MERMEC	ATO Test	4.13	5%
D3.1_14	CAF SIG	MERMEC	ATP Test	4.14	5%
D3.1_15	CAF SIG	MERMEC	Positioning System Test	4.15	5%
D3.1_16	BT	CAF SIG, AZD	Perception System Test	4.16	4%
D3.1_17	DB	BT	TCMS	4.17	4%

D3.1_18	BT	DB	Degraded Scenario Management	4.18	4%
D3.1_19	INDRA	AZD, MERMEC, SNCF-V	On board Tests Results Automatic Management	4.19	4%
D3.1_20	INDRA	MERMEC	Non-Automatic Management (from ground station)	4.20	4%

Table 1 – Scope of work splitting among contributors

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 are actually **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 to.

The subject of this document is the Test of functions at the start of the mission

The main goal of the tests at the start of the mission is to guarantee the mission safety and reliability.

The definition of these tests is linked with

- the mission safety and reliability targets (THRs and mission failure rates),
- the train architecture (available redundancies),
- the technical solution (basic reliability of components),
- the permanent diagnosis during the mission (capability to detect failures during the train operation),
- periodical maintenance tests (periodical assessment of the functions availability).

A test needs to be performed at the start of the mission if permanent diagnosis and periodical maintenance test are not capable to guarantee the mission safety and reliability targets (for example due to functionalities that are not normally activated during train operation and therefore not permanently monitored or too high failure rate of the technical solution respect the target) .

This is the principle applied today on GoA1/2 trains to define the tests to be performed and which remain applicable also for the GoA3/4 trains

The transition from GoA1/2 to GoA3/4 trains can impact the existing solutions by:

- the change of the systems architecture, to be operated without the intervention of train operator
- the introduction of new functionalities replacing the actions performed by train operator, which need as well to be diagnosed.

In particular the replacement of manual operation done by train operators for the management of degraded modes following any failure is an interesting impacts considered

The present document D3.1 has the objective to analyse these impacts in order to make hypothesis about functional test to be performed on autonomous trains at the start of the mission and generate high level use cases which can be taken as reference by WP that are currently developing new generation of ATO and TCMS for autonomous trains

The **decision taking** process in case of faulty tests, by independent automatic routine or by ground operator remote intervention, is a transversal impact of the transition to autonomous train to be analyzed as well.

The definition of the new technologies necessary due to transition from GoA1/2 to GoA3/4 is instead out of the scope, which is limited to the functional level.

METHODOLOGY

A functional approach is adopted.

The standard EN15380-4 is taken as initial input for the analysis, providing all the train functionalities.

Functions impacting on mission safety and reliability are identified and, for each of them, the general systems concept implemented to achieve the mission safety and reliability targets is analysed with the goal to identify the rationale behind the choice of the tests to be performed at the start of the mission.

The possible modification of the actual general system concept due to transition to GoA3/4 is then identified and the rationale behind the choice of tests is adapted.

The updated rationale become the base to define the test at the starting of the mission for train GoA3/4.

In this way a standard methodology applicable to any systems is put in place to define the tests to be performed.

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

MAIN CONCLUSIONS

The work done gave an interesting contribution thanks to a structured and repeatable process, based on

- functional approach, strongly linked to existing applicable standards (EN15380-4, TSI),
- common analysis method for any train, autonomous or not, and for any function
- clear test identification criteria: the satisfaction of the safety condition and of the train mission reliability targets.
- State of art status analysis
- Permanent diagnosis and periodical maintenance test effectiveness analysis in guaranteeing the safety condition and of the train mission reliability targets

The analysis done evidenced that

- existing tests performed at the start of the mission of not autonomous trains are generally carried over also on autonomous train
- adaptation due to new condition given by the automatization of the testing process and new technologies is needed.
- new tests are needed

Use cases to manage the GoA3/4 trains are defined (see list of table) and new potential tests and new technologies necessary on GoA3/4 trains are identified.

The main contribution are:

- Analysis method and criteria defintion
- New functions, technologies and potential testing functions to be developed to replace the driver
- New functions necessary to take decisions if to start or to cancel the mission

The document contributes effectively to the next generation ATO and TCMS system development

Note: GoA4 Metro application existing technologies used for similar functions, where applicable, are indicated as possible starting point for the development of the same functions on main line and regional GoA3/4 trains

ABBREVIATIONS AND ACRONYMS

AC	Alternating Current
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
GoA	Grade of Autonomy
HVAC	Heating Ventilation Air Conditioning
LIM	Limiter Switch (train protection switch)
LV	Low Voltage
MCB	Main Circuit Breaker
N.A.	Not Applicable

PC	Personal Computer
SIL	Safety Integrity Level
SoA	State of the Art
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 identify the self-diagnostic process of the train *functions* at the start of the mission to be implemented on GoA3/4 trains.

The not autonomous main line and regional trains state of art is the reference regarding type of test executed.

The document investigate the rationale that is present behind the choice of tests to identify the standard driving rules to be followed in defining the tests, so that they become the reference for the analysis to be done on the train functions and on their test integration/modification required due to the transition from GoA1/2 not autonomous train to GoA3/4 autonomous trains

The identified test are then described by using the formal language of use cases, applying for each of them a standard formal definition table.

The document is organized as follow:

In chapter 2 the Context of the analysis is defined, making a critical analysis of rationale used for the definition of the test at the start of the mission, its impact on GoA3/4 trains, investigating also the effect of permanent diagnosis and corrective maintenance in the definition of the tests and the functions scenario is defined choosing, among the function list of EN15380-4, the functions which could require a test at the start of the mission on GoA3/4 trains (based on defined test rationale)

In chapter 3 the analysis method to be applied at every train function is described. The method consist of state of art rationale identification, critical analysis of impact due to GoA3/4 implementation on identified rationale, definition of GoA3/4 tests new rationale and proposal of functional requirements (use cases) to be taken in charge by new functions. Eventually new technologies in charge to resolve the impacts of GoA3/4 are identified.

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 test use case.

In chapter 5 the main results derived from the contribution are resumed and most innovative idea underlined.

2 CONTEXT

2.1 FUNCTIONS, SYSTEMS, ARCHITECTURE AND TECHNOLOGIES

Functions of the train are performed by technological system that are normally recognized as "systems".

The function is what is expected the train does.

The system is a group of devices, which border can be clearly defined, which communicate with the external part of the border by interfaces and which perform certain actions based on the status of the interfaces and its internal functional logics.

In EN15380-4 all passenger train functions are listed as per today state of art.

These functions can be performed by different system together communicating each other with the common goal to perform the function. For example the External Access function of EN15380-4 is composed not only by the door system supplied by the supplier of the door, but it include all the other system which participate to the door control (driver's desk, LV control circuit, TCMS, etc).

Same function can be done by different architectures, the chosen architecture of the train influence the definition of the train systems: a function can be done by more than one combination of train systems depending from the train architecture.

The analysis of this document remains at functional level, because has not the goal to define a standard architecture of the GoA3/4 train. New technologies are therefore not considered, because they are linked to the train architecture and technical solution to implement the functionalities.

On the other hand often functions are linked to the main system in charge of the function implementation, therefore in the document is still kept the reference to system to indicate the tests, but a relation between function and reference system is given.

2.2 TEST AT THE START OF THE MISSION SCOPE AND RATIONALE

The scope to perform a test is to assess if *functions* work as per nominal design condition or if any existing failures affects the mission of the train. The mission can be affected by failures degrading the safety or the availability level of the function.

- Function Safety

  The train safety related functions often have redundancies to guarantee the resistance to the single failure of components with failure rate not compatible with the expected THR for identified hazard.

  The THRs are guaranteed by proper design, permanent diagnosis and periodical maintenance tests

  Some of these safety related functions can be not fully used during normal operation; therefore some hidden failure on redundant component could be present during the normal operation which is not detected by the permanent diagnostic system because the component is not commanded during the mission.

Due to the missing diagnosis, any hidden failure to devices are not repaired during the corrective maintenance activity foreseen in the depot at the end of the service and the loss of redundancy for a long time reduce the safety margin of the function.

If the periodical maintenance test periodicity is not capable to guarantee the THRs for certain functions, then daily tests are performed to assess the safety of the function before the mission and reduce the time to risk.

The initial goal of the test at the start of the mission is therefore to guarantee that all the train safety related functions are working properly and all redundancies linked to safety are available.

On GoA1/2 train these tests can require manual operation by driver or operators, on GoA3/4 the tests **shall be automatic**.

- Function Availability

  Several functions of the train, safety and not safety related, have impact on mission reliability of the train because their failure impact the running capability or any other vital function for the mission (for example the passenger alarm).

  On GoA1/2 train this type of failures are mitigated by proper dimensioning of components or by redundant architecture single failure resistant which permit to continue the mission also in presence of one failure. Safety related function, which have already redundant architectures to guarantee the safety, in these cases could have a double redundant architecture to guarantee at the same time also the availability.

  The reaction to the failure in some case is automatically activated, in other cases it must be activated by the driver by manual operation (train **"degraded" mode** activation).

  Often the "degraded" mode impose limitation to the mission (for example limitation of the maximum speed). When a degraded mode is not compatible with the mission targets, the mission shall be cancelled.

  The redundancies necessary to guarantee the mission reliability and the degraded modes functionalities can be monitored by permanent diagnosis or can be "sleeping" system, which start to operate (and therefore monitored) only when a failure occur.

  If the permanent monitoring and the periodical maintenance test periodicity is not capable to guarantee the expected target for mission reliability of the train due to certain components with high failure rate, then daily tests are performed to reduce the time to risk of mission cancellation or degradation.

  The tests at the start of the mission have therefore also the goal to assess, when necessary, the availability of vital functions and the correct functionality of degraded modes when these are not verified by permanent diagnosis and if periodical maintenance checks are not sufficient to guarantee the expected reliability of the mission

  On GoA3/4 trains the running capability of the train shall be guaranteed by redundancies/degraded modes **automatic or remote enabling** when the failure happen.

  The management of the failures during the mission is the goal of the document D3.2, but the scope of GoA3/4 train tests at the start of the mission shall be extended also to the verification

of sufficient availability **of any new automatic systems** enabling the redundancies or degraded modes which guarantee the reliability of the mission

The execution of the test at the start of the mission is therefore strictly linked to the required **THRs** and **train mission reliability rates** and how the real system of the train can guarantee them, based on their architecture and device failure rates.

The analysis requires therefore an *high level* evaluation of the capability to diagnose wholly or only partially every *safety related and/or mission reliability related function* by permanent diagnostic routines in the control and command systems of the train.

Wherever the permanent diagnosis is not capable to detect failures a further critical analysis shall be done to evaluate if the periodical maintenance tests are capable to guarantee the required THR and train mission reliability rates.

Only in case this is not confirmed the test at the start of the mission is proposed.

As written before this document has not the goal to enter in detailed architectural and technical aspects, and therefore cannot define the specific THR and mission failure rates required for the trains, but can identify for each function a *rationale* to be taken in consideration during the development of GoA3/4 train.

The driving concept of this document is therefore the identification of the impacts that the transition to GoA3/4 train has on existing tests and the eventual definition of new test due to the automatization of certain operation of the GoA3/4 train, wherever permanent diagnosis and periodical maintenance tests cannot fully assess the THR compliance and mission reliability target.

2.3 SCENARIO

GoA3/4 train has interfaces with the following subsystems:

- Ground operation and control command
- Ground Radio
- Ground Signalling
- Catenary
- Track
- Platform

The following EN15380-4 functions are identified having a safety or mission reliability impact.

Note: in the table, a correspondence between the functions and the main system that traditionally take in charge the functions implementation is provided. The paragraph where the function is analysed is also reported.

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 emergency alarm from passengers	Passenger Alarm (4.3)
C F F a C	Provide passenger emergency 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 2 –Functions list

At train level most of the functions involve TCMS, which is a further subsystem which can be tested at the start of the mission.

EN15380-4 ID	FUNCTION	MAIN RELATED SYSTEMS
	Not applicable	TCMS (4.17)

In GoA3/4 train two additional functions are needed due to the missing train operator that could impact the mission reliability

EN15380-4 ID	FUNCTION	MAIN RELATED SYSTEMS
-	Degraded scenario management	Any of the above system (chapter 4.18)

The above group of functions need to be integrated with further **decision maker functions**, replacing the decision process by the driver. Critical analysis about necessary initial test shall be done as well:

EN15380-4 ID	FUNCTION	MAIN RELATED SYSTEMS
-	On board tests results automatic management	TCMS (chapter 4.19)
-	On board tests results non-automatic management (ground management)	Communication between train and ground and TCMS (chapter 4.20)

3 ANALYSIS METHOD

For every function the following analysis is done:

- State of art

  Critical analysis at the base of the execution or not execution of the function tests on GoA1/2 trains, identifying the rationale used.

  - Function general description: systems involved, actors
  - Sub-functions involved among the EN15380-4 sub-function list related to main function
  - Function high level safety requirement analysis:

    the safety requirements present on TSI or any other standard related to the function if necessary are reported and a brief description of the architectural solution adopted on GoA1/2 to satisfy the safety requirement is provided,
  - Function high level mission reliability impact analysis:

    the mission reliability impact of the function is analyzed and a brief description of the architectural solution / operative instruction to the driver or train operator adopted to mitigate the risk of loosing or reducing the running capability or vital functions of

GoA1/2 trains is provided. Particular attention is given to the manual operations, which on GoA3/4 shall become autonomous.

- Tests at the start of the mission rationale description:

  Based identified sub-functions, architecture implemented and solution adopted to maximize the function safety and reliability, on considerations about permanent diagnosis, periodical maintenance check and achievable sub-function safety and reliability targets, the **list of sub-functions test** generally performed at the start of the mission on GoA1/2 train is provided and the **rationale** justifying them is described

- Impact of transition to GoA3/4
  - Critical analysis is done to verify which are the main impact on the function given by the transition to GoA3/4:
    - new solution to perform test at the start of the mission which are normally performed by the driver
    - new redundancies or functionalities to comply with new safety requirements or to be able to comply to the existing ones, but without the driver,
    - new redundancies or functionalities to comply with mission reliability requirement, but without the driver
- GoA3/4 tests at the start of the mission rationale
  - A critical analysis is done based on output of former sections on following subjects:
    - GoA1/2 tests to be adapted for autonomous execution
    - New redundancies/functions critical analysis to understand if the operative condition, permanent diagnosis and periodical maintenance test are sufficient to guarantee their availability or a new functional test at the start of the mission shall be considered.
- Use case definition
  - GoA1/2 tests use cases are revised in order to be performed with the actor present on GoA3/4 train, which doesn't include operators, and at GoA3/4 applicable conditions. Any interaction between Train System and Ground control are also part of the descriptions
  - New use cases are defined for the new functionalities which need to be tested at the start of the mission

The last chapters of the document makes an evaluation about the method to analyse the test results, take decisions and perform actions in case of failures (e.g. redundancies or degraded mode activations).

Difficult scenarios are also evaluated, where for "difficult" scenarios are intended events where a computer cannot assess a decision to put the train in service operation, but the Ground control intervention, even remotely, is required.

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

4.1 FIRE PROTECTION SYSTEM TEST

4.1.1 State of Art

4.1.1.1 Architectural principles

The actors of the Fire Protection System are the following ones (for GoA1/2 application, i.e. with a driver):

- On-board staff
- Maintenance staff
- Driver

The Fire Protection System is mostly linked to the following subsystems:

- TCMS

4.1.1.2 Sub-Functions

The functions covered by the Fire Protection System in EN15380-4 are the following ones.

- BE Fire Protection
- HBEJ Provide diagnostic information

4.1.1.3 Safety requirement

The Fire Protection System depends on TSI Loc&Pas (4.2.10.2)

Regarding to TSI Loc&Pas(4.1.4.) categorisation of the rolling stock for fire safety:

(1) In respect of fire safety requirements, four categories of rolling stock are defined and specified in the TSI SRT. — Category A passenger rolling stock (including passenger locomotive), — Category B passenger rolling stock (including passenger locomotive), — Freight locomotive, and self-propelling unit designed to carry other payload than passengers (mail, freight, infrastructure inspection vehicle, etc.), — OTMs.

(2) The compatibility between the category of the unit and its operation in tunnels is set out in the TSI SRT.

(3) For units designed to carry passengers or haul passenger carriages, and subject to the application of this TSI, category A is the minimum category to be selected by the party asking for assessment; the criteria for selecting category B are given in the TSI SRT.

(4) This categorisation shall be used by the notified body in charge of the assessment, in order to assess the applicable requirements from the clause 4.2.10 of this TSI, and shall be stated in the certificate of 'EC' verification.

According to TSI, Fire containment and control systems for passenger rolling stock (clause 4.2.10.3.4):

In addition to requirements of the clause 4.2.10.3.4, units of category A and B passenger rolling stock shall be equipped with active Fire Containment and Control Systems.

Fire Containment and Control Systems shall be assessed according to the notified National Rules about fire automatic extinguishing systems. CEN/TR 17532:2020 – "Railway applications - Fire protection on railway vehicles - Assessment of fire containment and control systems for railway vehicles" shall be considered.

In addition to the requirements specified in clause 4.2.10.3.4, the units of category A and B passenger rolling stock shall be equipped with automatic fire extinguishing systems in all technical areas.

Freight locomotives and freight self-propelling units: fire spreading protection measures (clause 4.2.10.3.5) and running capability (clause 4.2.10.4.4)

In addition to the requirements specified in clause 4.2.10.3.5, freight locomotives and freight self-propelling units shall be equipped with fire automatic extinguishing systems in all technical areas.

In addition to the requirements specified in clause 4.2.10.4.4, freight locomotives and freight self-propelling units shall have a running capability equivalent to that of category B passenger rolling stock. For running capability, EN 50553 (REQUIREMENTS FOR RUNNING CAPABILITY IN CASE OF FIRE ON BOARD OF ROLLING STOCK) shall be applied in addition.

4.1.1.4 Mission reliability impacts

Special attention needs to be given to TCMS, brake and propulsion design that prevents stopping a train at a hazardous location not suitable for rescue, e. g. tunnels or bridges. Therefore EN 50553 (REQUIREMENTS FOR RUNNING CAPABILITY IN CASE OF FIRE ON BOARD OF ROLLING STOCK) shall be applied in addition.

4.1.1.5 Test at the start of the mission rationale

-Daily self-test on power on
-Permanently supervision of relays and trainlines by TCMS
Manual Maintenance of the whole system every 3 -6 month .

4.1.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 may still need to be performed in GoA3/4, However TCMS will in future take over the tasks which were formerly performed by the driver .

4.1.3 GoA3/4 Tests at the start of the mission rationale

All the tasks performed by the driver during service in GoA1/2 need to be done either by ATO or TCMS.

Additional safety functions associated with shifting driver responsibilities to machine may result in an upgrade and extension of the ETCS telegrams or a third radio channel beyond ETCS and ATO.

4.1.4 Use cases definition

The following tables summarize the tests of the Fire Protection System.

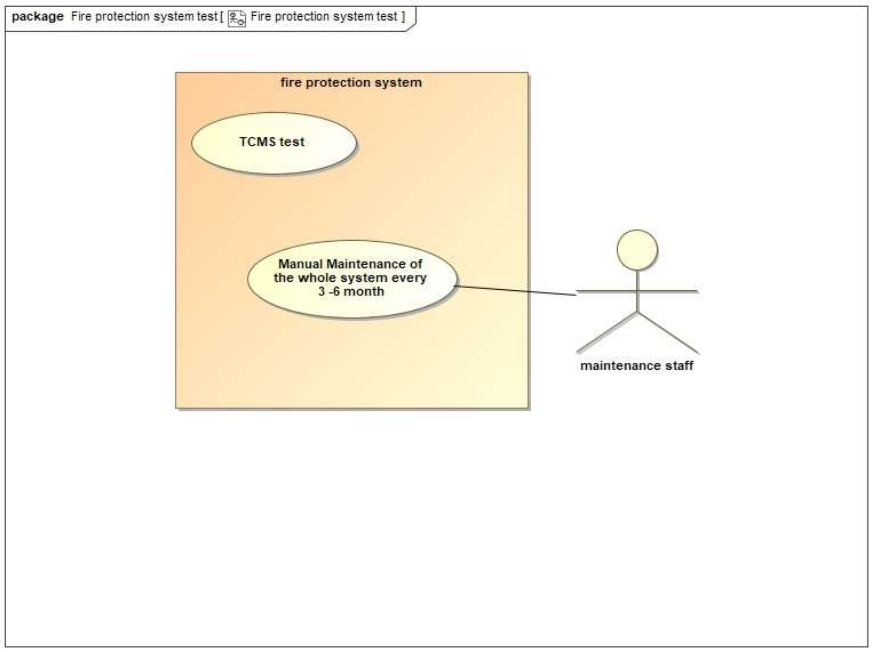

Figure 1: Fire Protection System Test

Use Case	Fire Protection System test
ID	
Actor	Fire protection system, maintenance staff, TCMS
Goal	Periodic test of the fire protection system
Safety relation	TSI Loc&Pas
Precondition	The train is at a standstill
Flow of events	-Daily self-test on power on -Permanently supervision of relays and trainlines by TCMS -Manual Maintenance of the whole system every 3 -6 month, if needed
Post condition	The train is at a standstill
Things that can go wrong	System failure
Already implemented risk reduction measures	Fire Materials implemented
Observations	

Table 3: Testing of Fire Protection

4.2 INTERNAL AND EXTERNAL LIGHTS TEST

This chapter describes internal and external lights test of the deliverable D3.1 of TAURO's WP3.

Actual implementation - state of the art Internal and External Lights Test for not autonomous trains - GoA1/2- is described as reference.

Reliable and safe train operation needs correct function of internal and external lights.

The responsibility for proper function of internal and external lights is assigned to the train driver.

As support to GoA2 systems already diagnosis and monitoring functions for locomotive lights are implemented, in automatic and manually way. To reach next step of autonomy of GoA3 and GoA4 systems will require additional innovative methods.

Succeeding chapter describes functional tests for up to GoA2 trains related to the lighting system. The use cases described are clustered according EN15380-4 (“Railway applications – Classification system for railway vehicles – Annex E: Function groups).

4.2.1 State of art

4.2.1.1 Architectural principles (Actors and systems involved)

The internal and external lights for GoA1/2is involving the following subsystems:

- TCMS,
- Head lamps, Marker lamps and tail lamps (this are on trains also head and marker lamps)
- Internal lighting
- Cab backwall placed rotary switch and switch on drivers’ desk.

The actors dealing with the light system for GoA1/2application are the following:

- Driver,
- Maintenance staff.

4.2.1.2 Sub-functions of “Internal and External Lights Test”

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

4.2.1.3 Safety requirements

Requirements are defined by TSI LOC&PAS referring for head, marker and tail lamps defining design mechanical position, concerning the spectral radiation distribution, colour and the luminous intensity of lamps to standard EN 15153-1:2013.

Note: where it is intended to use lights to inform of an emergency situation (operating rule, see TSI OPE), this should be done only by means of head lamps in flashing/blinking mode.

4.2.1.4 Service reliability aspects

Assuming positive tests of the internal and external lights, it can be assumed, that by illumination of the track and reflective signals by headlights is enough, and in proper way to operate the train safely.

4.2.1.5 Test scheduling

From timing perspective, the tests of subsystem can be executed:

- At every start-up (powering up of the train) – before the mission on train,
- As continuous monitoring – the whole time during the mission on train.
- In fixed longer periods – in depo:
  - regularly – e.g. latest after 24 hours
  - during maintenance in depo – e.g. every 3 months,
- additionally, today trains are externally observed by other driver and at train stations

The tests during start-up, usually before a train is leaving the depot in the manual tests must be performed. Actual trains are already supporting the continuous monitoring with defined scope. The driver still must perform manual tests.

In case of failures that do not allow safe operation, the operator can timely decide to enable or not mission with this train. During operation with degraded functionality of external lights an reduced operation (speed and range of action limitation) is allowed.

Tail lamps are not special lamps on locomotive but covered by the functionality of the marker lights of locomotive. Especially the check of tail lamps of trains can be time consuming if the driver has no supporting stuff for this task.

4.2.2 Impacts of transition to GoA3/4

The TCMS will in future take over the tasks which were formerly performed today by the driver, to allow GoA3/4 mode operation for the train.

The way how the tests will be executed, and the reporting of the outcome will change. Today the lamps are checked visually or when the monitoring detects issues, an appropriate message on the HMI informs is shown to the driver, with the failure codes and possible remedy text. In GoA3/4 mode the driver will be not physically available (at least not locally), so visual information collected by driver should be replaced by e.g. on-board cameras, and the diagnostics information from the TCMS must be provided / accessible for remote monitoring/controlling center.

For external light tests in depo and special measurement wall and external camera(s) can be provided. To replace external observation and warning in failure case by other train drivers, the trains

should observe with their own cameras also the other approaching train for plausible external light functionality – and raise warning in case of assumed failure to ground control.

4.2.3 GoA3/4 Tests at the start of the mission rationale

4.2.4 Use cases definition

4.2.4.1

4.2.4.1 UC-XL2 Testing of head lamps HW part availability

Use Case	Testing of head lamps HW part availability
ID	XL1
Actor	Virtual Driver
Goal	G_XL1: Make sure head lamp HW is available within technical specifications.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available
Flow of events	1. Occupy train 2. Select light pattern with head lamp ON 3. Check power supply for lamps is provided 4. Check for possible detected HW failure (monitoring for lamp over/under current, voltage and temperature) 5. Repeat 2...5 on another end of train
Post condition	Inform the TCMS/Virtual Driver whether head light is power supplied and HW is working in defined current, voltage and temperature limits.
Things that can go wrong	HW failure, power supply not provided – e.g. MiCB switched unintentionally OFF.
Already implemented risk reduction measures	Monitoring of lamp power supply and intelligent LED lamps monitoring continuously working conditions (current, voltage and temperature) are available.
Observations	Test is done as continuous monitoring.

Table 4: Testing of Head lamps HW part availability

4.2.4.2 UC-XL2 Testing of head lamps function

Use Case	Testing of head lamps function
ID	XL2
Actor	Virtual Driver
Goal	G_XL2: Make sure head lamp is functioning according operational rules.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select light pattern with head lamp on 3. Check illumination availability
Post condition	Inform the TCMS/Virtual Driver whether head light is according EN 15153-1 norm.
Things that can go wrong	Head lights are not illuminating the track, because of got dirty lamps.
Already implemented risk reduction measures	
Observations	Test is done before start of each mission.

Table 5: Testing of Head lamps function

4.2.4.3 UC-XL3 Testing of head lamps illumination

Use Case	Testing of head lamps illumination
ID	XL3
Actor	Virtual Driver + maintenance staff
Goal	G_XL3: Make sure head lamp illumination is functioning according requirements.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select light pattern with head lamp on 3. Check illumination availability 4. Check color 5. Check spectral radiation distribution 6. Check luminous intensity
Post condition	Inform the TCMS/Virtual Driver whether head light is according EN 15153-1 norm.
Things that can go wrong	Color, spectral radiation distribution and luminous intensity is wrong.
Already implemented risk reduction measures	Specified test for the depo are defined, some specialised sensors are additionally needed.
Observations	Test is done regularly during periodic maintenance, typically every 3 months.

Table 6: Testing of Head lamps illumination

4.2.4.4 UC-XL4 Testing of marker lamps HW part availability

Use Case	Testing of marker lamps HW part availability
ID	XL4
Actor	Virtual Driver
Goal	G_XL4: Make sure marker lamps HW are available within technical specifications.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available
Flow of events	1. Occupy train 2. Select light pattern with marker lamp ON 3. Check power supply for lamps is provided 4. Check for possible detected HW failure (monitoring for lamp over/under current, voltage and temperature) 5. Repeat 2...5 on another end of train
Post condition	Inform the TCMS/Virtual Driver whether marker lights are power supplied and HW is working in defined current, voltage and temperature limits.
Things that can go wrong	HW failure, power supply not provided – e.g. MiCB switched unintentionally OFF.
Already implemented risk reduction measures	Monitoring of lamp power supply and intelligent LED lamps monitoring working conditions (current, voltage and temperature) are available.
Observations	Test is done as continuous monitoring.

Table 7: Testing of Marker lamps HW part availability

4.2.4.5 UC-XL5 Testing of marker lamps function

Use Case	Testing of marker lamps function
ID	XL5
Actor	Virtual Driver
Goal	G_XL5: Make sure marker lamp is functioning according operational rules.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select light pattern with marker lamp on 3. Check illumination availability
Post condition	Inform the TCMS/Virtual Driver whether marker light is according EN 15153-1 norm.
Things that can go wrong	Color, spectral radiation distribution or luminous intensity is wrong.
Already implemented risk reduction measures	
Observations	Test is done before start of each mission.

Table 8: Testing of Marker lamps function

4.2.4.6 UC-XL6 Testing of marker lamps illumination

Use Case	Testing of marker lamps illumination
ID	XL6
Actor	Virtual Driver
Goal	G_XL6: Make sure marker lamp illumination is functioning according requirements.
Safety relation	Illumination of the track and reflective signals is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select light pattern with marker lamp on 3. Check illumination availability 4. Check color 5. Check spectral radiation distribution 6. Check luminous intensity
Post condition	Inform the TCMS/Virtual Driver whether marker light is according EN 15153-1 norm.
Things that can go wrong	Color, spectral radiation distribution and luminous intensity is wrong.
Already implemented risk reduction measures	
Observations	Test is done regularly during periodic maintenance, typically every 3 months.

Table 9: Testing of Marker lamps illumination

4.2.4.7 UC-XL7 Testing of correct required lamp pattern

Use Case	Testing of correct required lamp pattern
ID	XL7
Actor	Virtual Driver
Goal	G_XL7: Make sure selected lamp pattern is according required operational rules.
Safety relation	Shown lamp pattern is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select required light pattern 3. Check shown light patter
Post condition	Inform the TCMS/Virtual Driver whether light pattern is according operational rules.
Things that can go wrong	Wrong light pattern is selected or shown.
Already implemented risk reduction measures	
Observations	Test is done before start of each mission.

Table 10: Testing of Correct required lamp pattern

4.2.4.8 UC-XL8 Testing of available lamp patterns

Use Case	Testing of available lamp patterns
ID	XL8
Actor	Virtual Driver
Goal	G_XL8: Make sure all lamp pattern needed in train operational area are available.
Safety relation	Shown lamp pattern is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Occupy train 2. Select each available light pattern provided by locomotive 3. Check shown light patter
Post condition	Inform the TCMS/Virtual Driver whether light pattern is according operational rules.
Things that can go wrong	Wrong light pattern is selected or shown.
Already implemented risk reduction measures	
Observations	Test is done regularly during periodic maintenance, typically every 3 months.

Table 11: Testing Available lamp pattern

4.2.4.9 UC-XL9 External observation during mission

Use Case	Check by external observer of lamps
ID	XL9
Actor	Virtual Driver – but external (not on train in focus)
Goal	G_XL9: Make sure all lamps needed by train in operational area are visibly working.
Safety relation	Shown lamp pattern is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Observe train in focus (from other passing train or station) 2. In case of deviation from expected inform ground control 3. Ground control informs train in focus
Post condition	Inform via ground control the affected train.
Things that can go wrong	During mission one or more lights fail or got dirty.
Already implemented risk reduction measures	Operational rules defined for driver, when, what deviation has to be reported.
Observations	This check should be done each train on mission “seeing” other trains.

Table 12: Checking of lamps by External observer

4.2.4.10 UC-IL10 Internal lighting - CAB

Use Case	Check by internal observer CAB lighting
ID	IL10
Actor	Virtual Driver – internal observer
Goal	G_IL10: Make sure all internal lamps needed in CAB are visibly working.
Safety relation	Internal lighting can be safety relevant. Supports the virtual driver functionality.
Precondition	Electric power supply available XL1 test done
Flow of events	1. Switch ON CAB internal lighting 2. Observe illumination function 3. Create diagnostic log entry
Post condition	Store result in diagnostics. Inform ground control in case of failure.
Things that can go wrong	CAB internal lighting not working.
Already implemented risk reduction measures	Currently only functional test by driver is used.
Observations	This check should be done at each mission start.

Table 13: Testing of Cab Internal light

4.2.4.11 UC-IL11 Internal lighting – passenger area

Use Case	Check by internal observer passenger area lighting
ID	IL11
Actor	Virtual Driver – observer at passenger area
Goal	G_IL11: Make sure all internal lamps needed in passenger area are visibly working.
Safety relation	Internal lighting in passenger area is safety relevant.
Precondition	Electric power supply available XL1 test done
Flow of events	4. Switch ON passenger area internal lighting 5. Observe illumination function 6. Create diagnostic log entry
Post condition	Store result in diagnostics. Inform ground control in case of failure.
Things that can go wrong	Internal passenger area lights are not working.
Already implemented risk reduction measures	Currently only functional test by driver/train staff is used.
Observations	This check should be done at each mission start.

Table 14: Testing of Passenger area internal light

4.3 PASSENGER ALARM SYSTEM TEST

4.3.1 State of art

4.3.1.1 Architectural principles

The systems and scenario actors for GoA1/2 train involved by the function “Passenger Alarm” can be:

Train systems:

- passenger alarm,
- vehicle electrical circuits,
- TCMS,
- Brake system,
- driver’s desk HMI,
- PIS

Actors

- Driver,
- Train operator,
- Maintenance people

4.3.1.2 Sub-functions of Passenger Alarm function

The passenger alarm function is realized in not autonomous train by the implementation of the here below sub-functions (reference is EN15380-4):

CFDaA – Manage alarm requests from passengers / CFDaB – Manage passenger emergency request

CFFaC – Provide passenger communication

The execution of the alarm request is done by Passenger Alarm Devices (PAD), accessible to the passengers and present on each vestibule and separated area, and transmission systems to the driver, normally done by vehicle control circuits and/or TCMS.

The alarm request and transmission system is often implemented by redundant system (for safety and reliability reason).

The presence of several PADs on the train is generally not considered a redundancy, because the alarm device shall be immediately accessible by passenger, but the standard allow that a PAD can be isolated (to guarantee the service availability in case of blocking failure), see EN16334 §6.2.8, §9.6. The safety conditions shall be of course still guaranteed to continue the service

The execution of the emergency request can be done by independent devices (eventually redundant for safety/reliability reasons), operating by proper interfaces on brake system, or by brake system itself (which is sometime, in this case, the owner of the passenger alarm management system).

The execution of the passenger communication is done generally by PIS or by dedicated system

4.3.1.3 Safety requirements

TSI §4.2.5.3.5 specifies the hazard to be mitigated for the passenger alarm function:

(1) For the scenario 'failure in the passenger alarm system leading to the impossibility for a passenger to initiate the activation of brake in order to stop the train when train departs from a platform', it shall be demonstrated that the risk is controlled to an acceptable level considering that the functional failure has typical credible potential to lead directly to 'single fatality and/or severe injury'.

(2) For the scenario 'failure in the passenger alarm system leading to no information given to the driver in case of activation of a passenger alarm', it shall be demonstrated that the risk is controlled to an acceptable level considering that the functional failure has typical credible potential to lead directly to 'single fatality and/or severe injury'.

TSI §4.2.5.3.2 (5) and §4.2.5.4 communication requirements are not part of the functionalities involved in the hazard scenario to be mitigated for safety reason and therefore they are not vital for the service reliability and safety

Above requirements by TSI and hazard scenario are fully taken into account by standard EN16334:2014, which is the reference for regional/intercity/high speed train passenger alarm system. EN16334:2014 §9 minimum safety requirements are aligned with TSI risk mitigation requirements.

The passenger alarm function involves directly the train driver or on board staff on safety related functions:

TSI Loc&Pas §4.2.5.3 and 4.2.5.4 specify clearly which are the requirements related to the passenger alarm functions and passenger communication with driver or staff in case of alarm.

- TSI §4.2.5.3.2 (3-5) §4.2.5.3.3 specify the role of the driver in the management of the passenger alarm. The driver has a safety related role in the moment that decide to override the emergency brake application for any reason (TSI §4.2.5.3.3 (2)).

  The GoA3/4 train shall take in charge this safety related role by remote controlled re-designed functionalities.

- TSI §4.2.5.3.2 (6) requires that train crew only is enabled to reset passenger alarm request

  GoA3/4 trains shall take in charge this function (impacting service reliability and safety) by remote controlled re-designed functionality.

- TSI §4.2.5.3.6 requires that train staff can isolate the passenger alarm system and also state that (3) "*A train with an isolated passenger alarm system does not meet the minimum requirements for safety and interoperability as defined in this TSI and shall therefore be regarded to as being in degraded mode".*

  GoA3/4 trains shall take in charge this function (impacting service reliability and safety) by remote controlled re-designed functionality or shall guarantee a sufficiently reliable/redundant passenger alarm system, capable to manage single failures situation without requiring isolations (failure safe state corresponding to degraded mode)

- EN16334 allow that single passenger alarm devices can be isolated, but only by train staff (§6.2.8, §9.6).

  This function can be necessary to guarantee the service availability.

GoA3/4 trains shall take in charge also this function or implement sufficiently reliable/single fault tolerant systems permitting to guarantee the required service availability (high PAD reliability, redundancies, etc).

- EN16334 §9 also defines the acceptable functional failure rates (TFFR) for the safety relevant function of the system (reachable also by implementation of proper monitoring functions)

4.3.1.4 Mission reliability impacts

To maintain low the above risk, the systems are normally designed following fails safe design solution, which can have relevant impact on the reliability of the train. To reduce as much as possible above impact, **redundancies** are often implemented to be resistant to single failures or **degraded condition** described in TSI §4.2.5.3.6 (see above) can be enabled by the train crew or driver to exit from the safe state. Degraded condition fully remove the driver safety role from the process and apply immediately the emergency brake

Degraded condition can be compatible with the service (for example on lines without restrictions in stopping the train in certain points of the line) or not compatible.

4.3.1.5 Test at the start of the service rationale

In not autonomous train several of the safety related functions are managed by ≥SIL2 assessed software. These functions don't need to be tested.

The functional test of passenger alarm is done before going into service operation to check that the functions involving physical components which can be affected by failure are fully efficient:

- the alarm request,
- the emergency override command by driver
- the emergency application functions.

This is mandatory, because the passenger alarm system is a "sleeping system", generally not activated during the train service, but need to be always efficient to guarantee the safety condition of the service. Even if "sleeping", part of the system could be frequently operated, for example during switch on configuration phase, therefore its element can be subjected to failures also during that operation.

As written above the passenger driver communication is not considered vital for the function, therefore specific test is not done and the general communication system test at the start of the service is sufficient to check the passenger alarm communication.

As written above the reliability of the safety relevant functions can be guaranteed by monitoring functions capable to detect the availability of the functions (EN16334 §9).

These monitoring functions are the ones used during the tests at the beginning of the service, during which a passenger alarm request is simulated. If the test is successful, the risk that a failure can happen during the service is limited due to the short time to risk (time to risk depending from the frequency of the test: every morning, at every cab change, at every new service).

The definition of the frequency of the test depends from the type of architecture and implementation of the function. For example, if the change of cab reconfigures the passenger alarm system, can be convenient for safety reason to check that the configuration is successful at every cab change.

The test at the start of the service is capable to check all the safety related functionalities except the functionality of all the PADs, which requires a manual operation of all the PADs.

This is generally considered acceptable because periodical maintenance checks verify the correct operation with time intervals compatible with a time to risk exposure acceptable for the expected service reliability level.

4.3.2 Impacts of transition to GoA3/4

The transition to GoA3/4 impact the system architecture in charge of the Passenger Alarm function by the remote command of actions normally done by driver/staff or by definition of new solutions which guarantee a sufficient reliability/fault reaction.

In 4.3.1.3 the impacts of GoA3/4 are already briefly described:

- Emergency 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 sufficiently reliability or any safety relevant failure shall move the system into a safe state corresponding to degraded condition compatible with the running capability or Passenger alarm isolation shall be remote controlled.
- Single PAD can be remotely isolated or shall be sufficiently reliable/single fault tolerant to guarantee the required service availability.

This document has not the goal to define the potential new passenger alarm system technical solutions for GoA3/4 train but can elaborate reasonable hypothesis about implementation principles.

The above impacts in principle can be managed by solution involving following actors:

- Ground Operator,
- Ground Operation Command and Control,

functions:

- Operational communication and Train/Ground data transmission function

Train systems:

- Passenger alarm
- Train -ground communication
- TCMS
- Brake system
- PIS
- VCC

and related interfaces.

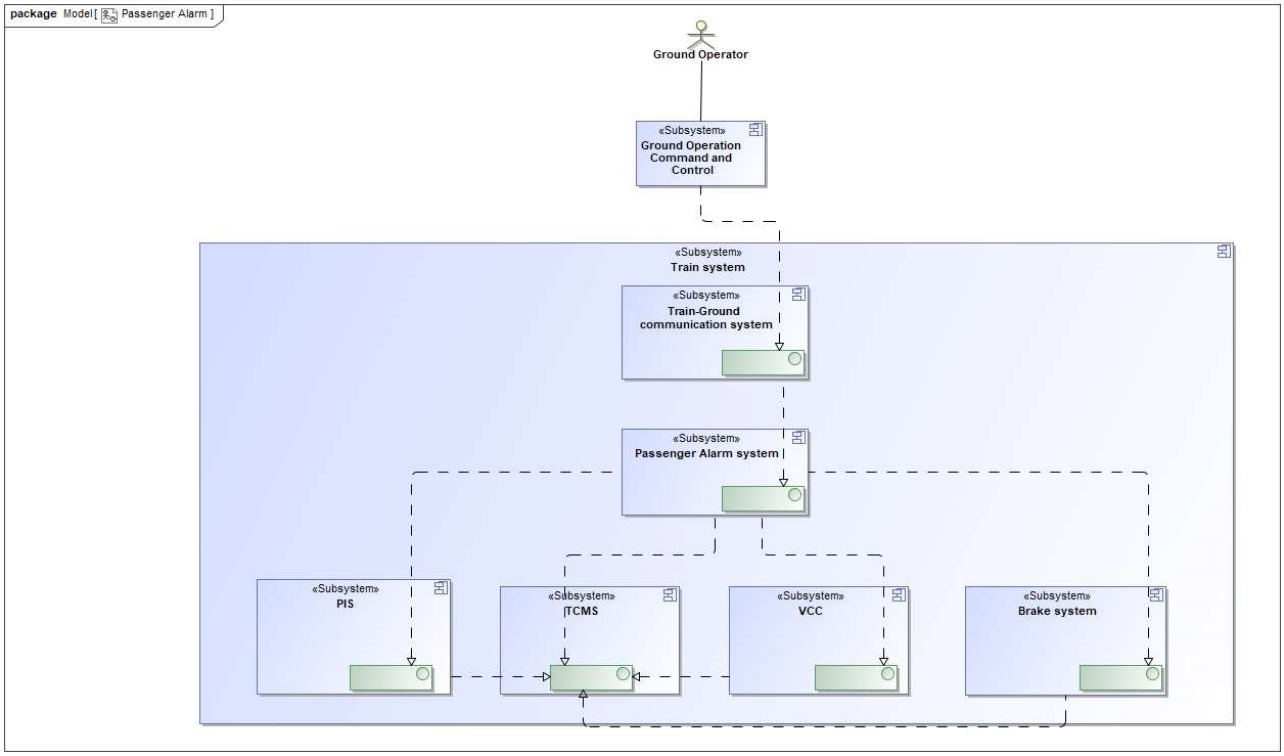

Figure 2 – GoA3/4 train Passenger Alarm management architecture

The solution will involve for sure mainly software routines (≥SIL2) and I/O of the involved systems controllers, which should be permanently monitored and tested at systems start-up or their generic test at the start of the service.

A comparison with GoA3/4 metro technical solution / technologies and reliability targets is suggested to verify if existing technologies are already capable to cover the requirements of GoA3/4 trains.

4.3.3 GoA3/4 Tests at the start of the mission rationale

The above analysis evidenced that Test of Passenger Alarm function shall be done on GoA3/4 trains as far as physical components (vehicle electrical circuits like train lines, switches, relays, or control units) are involved in the implementation of the function at train level and are not already tested by other system tests performed at power up or beginning of the service.

As per actual GoA1/2 train, the periodical checks of all PADs by maintenance people is considered sufficient to guarantee the expected reliability and safety.

As conservative hypothesis the same test performed on GoA1/2 train are therefore considered, but involving in the test the new actors and train function above mentioned

4.3.4 “Passenger alarm” testing use cases definition

The test of the “Passenger alarm” function at the start of the service includes the testing of

- the alarm request,

- the emergency override command by Ground Operator Emulator
- the emergency application functions.

as per above analysis.

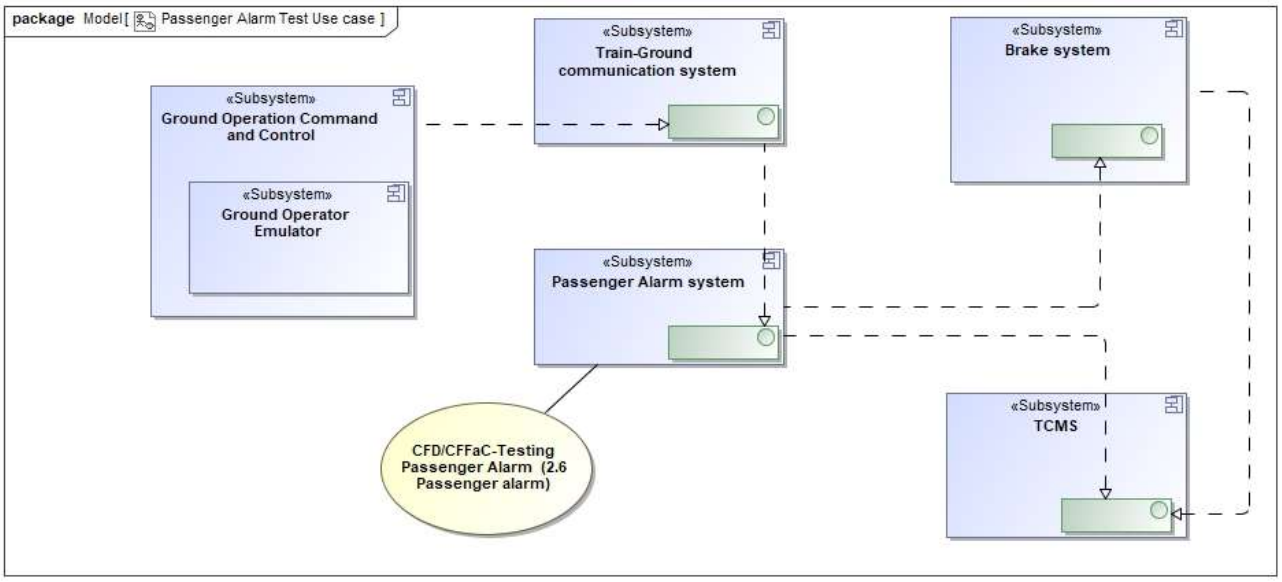

Figure 3: Use case of Function "Passenger Alarm Test"

Isolated PAD can be present at the start of the service (for example due to maintenance activities not finished or missing spare parts), if the type of train allow the service with some isolated PAD.

Therefore the test routine shall perform the tests allowing a certain number/location of isolated PAD, as per safety analysis.

The use cases condition is described in following table.

Use Case	Testing of Passenger Alarm
ID	DB1
Actor	Passenger Alarm System and Ground Operation Control Center
Goal	Check the functionality of the Passenger alarm request, emergency brake application and emergency brake override
Safety relation	The use case is safety relevant with relation to the hazards related to the immediate emergency brake application at station, delayed emergency brake application during the run and emergency brake override by ground operator
Precondition	Train in standstill and immobilized, not in emergency brake, brake system, TCMS, train-ground communication system, operative and tested
Flow of events	1. The Passenger Alarm system simulate the activation of any PAD 2. The Passenger Alarm system check that train-ground communication system received the passenger alarm request 3. The ground operation control center override the alarm request 4. The Passenger Alarm system check that the override command is received and, by TCMS interface, that emergency brake is not applied. 5. The Passenger Alarm system reset the simulation of activation of any pad 6. The Passenger Alarm system simulate again the activation of any PAD 7. The ground operation control center **doesn't** override the alarm request 8. The Passenger Alarm system check that the override command is not received and, by TCMS interface, that emergency brake is applied. 9. The Passenger Alarm system reset the simulation of activation of any pad and check that the emergency brake is released
Post condition	Train in standstill and immobilized, not in emergency brake,
Things that can go wrong	Train operation control center doesn't receive the alarm Passenger Alarm doesn't receive the override signal Brake system doesn't apply the emergency brake
Already implemented risk reduction measures	
Observations	Use case linked to Passenger Alarm architecture as described in Figure 3

Table 15: Testing of Passenger Alarm

4.4.1 State of art

4.4.1.1 Architectural principles

The systems and scenario actors for GoA1/2 train involved by the function “Provide passenger access and egress from rolling stock” can be:

Train systems:

- passenger door,
- PRM access ramps,
- vehicle electrical circuits,
- TCMS,
- On board Signalling system (ATC),
- driver’s desk HMI,
- PIS

Actors

- Driver,
- Train operator,
- Ground Operation Command and Control
- Ground Signalling System
- Platform screen doors system
- Maintenance people

4.4.1.2 Sub-functions of “Provide passenger access and egress from rolling stock” function

“Provide external access/egress” function is realized in not autonomous train by the implementation of the here below sub-functions :

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 unaccessible
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))

The execution is in charge of several similar equipment (doors), giving automatically a multiple redundancy in the execution of the function.

The architecture of not safety commands or executions depends from the general architecture of the train diagnostic.

4.4.1.3 Safety requirements

As written in the TSI §4.2.5.5.1 (3), the function is essential to safety.

The TSI defined in § 4.2.5.5.8-9 the following safety requirements for the functional failure

1. For the scenario one door is unlocked (with train crew not correctly informed of this door status) or released or opened in inappropriate areas (e.g. wrong side of train) or situations (e.g. train running), it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible potential to lead directly to:

   — ‘single fatality and/or severe injury’ for units in which passengers are not supposed to stay in standing position in the door area (long distance), or to

   — ‘single fatality and/or severe injury’ for units in which some passengers stay in standing position in the door area in normal operation.

2. For the scenario several doors are unlocked (with train crew not correctly informed of this door status) or released or opened in inappropriate areas (e.g. wrong side of the train) or situations (e.g. train running), it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible direct potential to lead to:

   — ‘fatality and/or severe injury’ for units in which passengers are not supposed to stay in standing position in the door area (long distance), or to

   — ‘fatalities and/or severe injuries’ for units in which some passengers stay in standing position in the door area in normal operation.

3. For the scenario ‘failure in the internal emergency opening system of two adjacent doors along a through route (as defined in clause 4.2.10.5 of TSI), the emergency opening system of other doors remaining available’, it shall be demonstrated that the risk is controlled to an acceptable level, considering that the functional failure has typical credible potential to lead directly to ‘single fatality and/or severe injury’.

The above failure scenario remain the reference also for GoA3/4.

To maintain low the above risk, the systems are normally designed following fail safe design solution, which can have relevant impact on the reliability of the train (safe state normally means train stopping or traction cut-off).

4.4.1.4 Mission reliability impacts

To reduce as much as possible impact of safety related failures, **redundancies** are often implemented to be resistant to single failures or **degraded condition** can be enabled by the train crew or driver to exit from the safe state:

- Isolation of the door
- Bypass of safe state by driver (traction cut-off bypass)

Degraded condition can be compatible with the service (isolation of the door) or not compatible (bypass of the traction cut-off to reach the next station and detrain the passenger or isolate the door).

The train crew, during isolation, makes also a visual check of the status of the door, which permit to assess that the isolation reach the goal to put again the door in a safe condition.

The train crew:

- *verify the situation* of the door not closing or in failure,
- *manually close* the door (which remained open due to a failure)
- *isolate mechanically* the door (safety relevant operation)

The mechanical isolation *bypass the door safety loop* via dedicated microswitch connected to the mechanical isolation device (safety relevant operation).

4.4.1.5 Test at the start of the service rationale

In not autonomous train there is not a functional tests of passenger doors before going into service operation, even if several failures could have impact on the service (as could be demonstrated by a functional FMECA)

The main reason is that most of the function are normally used during the service of the train because part of the normal process of opening/closing the passenger doors:

- Release external doors
- Open external doors
- Close external doors
- Lock external doors
- Unlock external doors
- Provide entrance lighting
- Signal all external door closed and locked state
- Signal external door status change/open/close by visual or audible signals
- Reduce the gap between vehicle and platform

Their permanent diagnosis permit to detect any failure at least at every opening/closing of the door

If a failure is detected, the degraded condition is activated and the train comes to the depo at the end of the service or after detrainment of the passenger. The maintenance people repair the failed

door, establishing again the nominal safety and availability condition and put the door system in service again.

The missing tests of remaining functions (sleeping or not regularly used functionalities) is acceptable for the following reasons

- Manage door system upon obstacle

  This function is only local and generally managed by software task using sensors signals inputs. Redundant system (sensible edge + current monitoring) generally guarantees an acceptable level of safety and availability of the function even in case of single failure.

  Periodical maintenance checks verify obstacle detection function. Maintenance intervals are compatible with time to risk exposure acceptable for the expected service reliability level.

- Enable selective external door opening in order to make certain vehicles of the train inaccessible

  Generally this functionality is managed by software tasks only, at train and local level, therefore once validated don't need to be tested any more.

- Isolate external doors

  The function is relevant only in case of presence of another failure to the same door requiring isolation (see above), therefore the impact on service availability is reduced because the probability to have a sleeping failure on isolation function of the failed door (two failure on the same door) is limited.

  Periodical maintenance checks verify the isolation function. Maintenance intervals are chosen based on an acceptable time to risk for the double fault on the same door.

- External door opening in emergency execution.

  Periodical maintenance checks verify emergency egress/access operation and in any case there is a multiple redundancies on this function (it is implemented at single door level), therefore a single failure has not a big impact.

- Ensure passenger access by external doors for people with reduced mobility.

  If the access is guaranteed by dedicated equipment operable only in case of necessity, generally the equipment operation is done by the train operator or people assisting the people with reduced mobility. In case of malfunction the people can be carried inside the train manually, causing a certain delay. This risk is generally considered acceptable considering the not frequent use of the equipment.

- Provide special emergency exits functions (emergency front doors and other emergency exits (i.e. windows))

  Generally, these emergency operations are guaranteed by pure mechanical equipment manually operated, which cannot be tested by automatic testing procedure.

  Periodical maintenance checks verify the correct operation with time intervals compatible with a time to risk exposure acceptable for the expected service reliability level.

Based on above considerations following principles are the main rationale of not performing the test at the start of the service:

1. Most of the sub-functions are permanently monitored due to the extensive use of the function
2. Not permanently monitored sub-functions have periodical checks with time interval compatible with not detected failures time to risk which guarantee a proper safety/service reliability level
3. Vital sub-functions resistant to the single failure
4. Multiple redundancy of the execution system (several doors)
5. Failed door can be isolated by *fully independent* isolation function bypassing totally the effect of the failure.
6. Redundancies on not enough reliable door sub-functions
7. Assistance at PRM people (if special equipment is used to guarantee their access to the train)

4.4.2 Impacts of transition to GoA3/4

4.4.2.1 Sub-functions normally used during the service of the train

These subfunctions implementation on GoA3/4 train is similar to the GoA1/2 train where operation and monitoring activities done by the driver in the cab are done by the new generation of automatic train operation.

Automatic train operation will check its capability to manage the functionalities during its own test at the beginning of the service, therefore these specific test are not considered in the scope of this document.

Specific technical solution which will be implemented to replace push button or lamps with devices controlled by ATO, will be permanently monitored during the use by standard diagnostic function and therefore not necessary to be tested at the start of the service.

4.4.2.2 Sleeping or not regularly used functionalities

The sleeping or nor regularly used functionalities which could be more impacted by the transition to GoA3/4 are the ones involving the train crew for their execution on GoA1/2 train.

1. **Manage door system upon obstacle**

This subfunction implementation on GoA3/4 train can be the same of GoA1/2 train, therefore the same rationale of the GoA1/2 train can be considered and no test required at the beginning of the service

2. **Enable selective external door opening in order to make certain vehicles of the train inaccessible**

This subfunction implementation on GoA3/4 train is similar to the GoA1/2 train, where operation and monitoring activities done by the driver in the cab are done by the automatic train operation. Automatic train operation will check its capability to manage this functionality during its own test at the beginning of the service.

The same rationale of the GoA1/2 train can be considered and no test required at the beginning of the service

3. **Isolate external doors**

The isolation of a failed door on GoA1/2 **is done by the train crew**, which:

- *verify the situation* of the door not closing,
- *manually close* the door (which remained open due to a failure)
- *isolate mechanically* the door (safety relevant operation)

Above operations *bypass the door safety loop* via dedicated microswitch connected to the mechanical isolation device (safety relevant operation).

On GoA3/4 train this operation can be possible only **by autonomous remote-controlled devices**, able to verify the situation (by videocameras connected with the Ground Operation Command and Control Center), close the door and isolate it.

These devices become relevant for the availability of the train because its functionality is mandatory to permit the train to continue the service after any major fault to single door. The devices shall be also able to manage the movable step, when present.

The devices could be complex and, being in charge of safety functions, shall be also safe.

This devices are not present on existing train and could be not present in the case the failure rate of the doors would be acceptable for the requested availability of the train.

To consider the worst case scenario, the implementation on the train of remote controlled **back-up door closing device** and remote controlled **door isolation device** is considered.

A comparison with GoA3/4 metro technical solution / technologies and reliability targets is suggested to verify if existing technologies are already capable to cover the requirements of GoA3/4 trains.

4. **External door opening in emergency execution.**

This subfunction implementation on GoA3/4 train can be the same of GoA1/2 train, therefore the same rationale of the GoA1/2 train can be considered and no test required at the beginning of the service

5. **Ensure passenger access by external doors for people with reduced mobility.**

This subfunction implementation on GoA3/4 train can be the same of GoA1/2 train, therefore the same rationale of the GoA1/2 train can be considered and no test required at the beginning of the service

6. **Provide special emergency exits functions (emergency front doors and other emergency exits (i.e. windows))**

This subfunction implementation on GoA3/4 train can be the same of GoA1/2 train, therefore the same rationale of the GoA1/2 train can be considered and no test required at the beginning of the service

4.4.3 GoA3/4 Tests at the start of the mission rationale

The above analysis evidenced that the only sub-functions impacted by transition to GoA3/4 is:

D B K Isolate external doors

Based on chapter 4.4.2 clause 3 described impacts, the reliability of the devices in charge of door back-up closing and isolation can be much lower than existing GoA1/2 solutions, therefore the periodical maintenance control put in place on GoA1/2 to guarantee the availability and safety of the functionality could have a much higher frequency on GoA3/4 trains, arriving till the daily test (this conclusion should be part of safety and availability analysis on the equipment).

Therefore, in the worst case, the test should become automatic test at the start of the service, with the goal to verify the capability of the equipment to perform the following functions, today in charge of the driver:

a. *Video-monitoring of the area around every door*
b. *transmitting the images of every door to the Ground Operation Control Center,*
c. *activating the Ground to train passenger communication*
d. *transmitting the back-up door closing and isolating command to every door by Ground Operation Control Center*
e. *back-up closing of every door*
f. *mechanically isolating with safety loop bypassing of every door*

Video-surveillance, Ground - Passenger, 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

The verification of the correct functionality of the sub-functions a. to c. can be therefore demanded to those functions tests

Remote command transmission by Ground Operation Control Center, back-up closing and mechanical isolation could be therefore tested locally on every door at the start of the service for the reason described above

4.4.4 Passenger Door tests use cases definition

The test of the "External access and external doors management" function at the start of the service could include the testing of remote controlled door back-up closing function and remote controlled door mechanical isolation function only, as per above analysis.

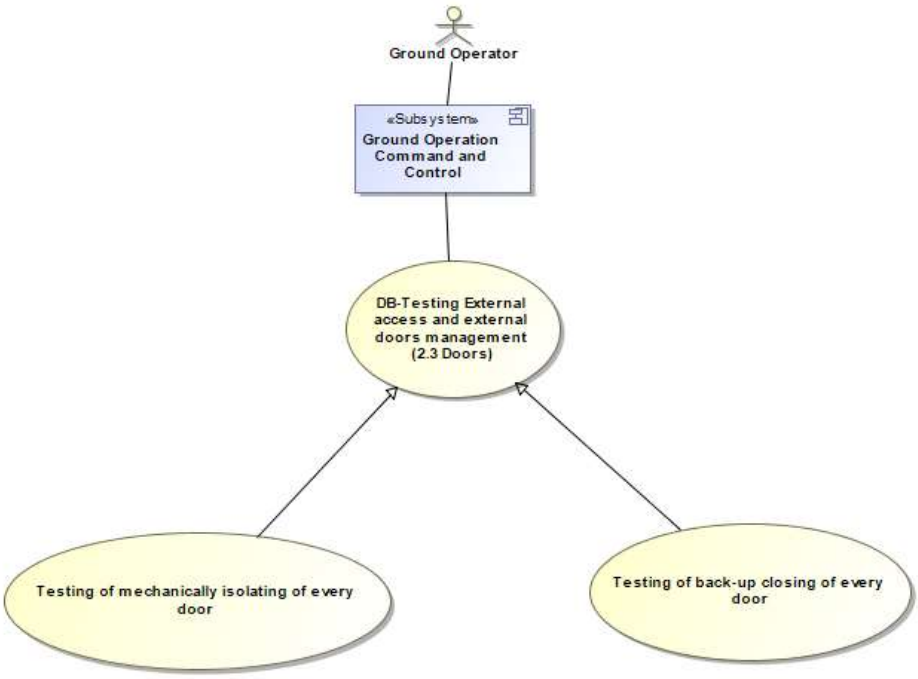

Figure 4: Use case of Function "Testing External Access and external doors Management"

Isolated doors can be present at the start of the service (for example due to maintenance activities not finished or missing spare parts), if the type of train allow the service with some isolated door.

Therefore the test routine shall perform the tests on not isolated doors only.

The use cases conditions are described in following tables.

Use Case	Testing of back-up door closing of every door
ID	PDT1
Actor	Ground Operation Control Center
Goal	G_PDT1: Check the functionality of the functionality of back up door closing of all the not isolated doors of the train
Safety relation	The use case is safety relevant with relation to the hazards related to the opening and closing of the door, which shall be mitigated by proper sub-function like visual and audible alert for people present in the area
Precondition	Train in standstill without any person inside, passenger doors closed, TCMS train-ground communication passenger information and video surveillance operative
Flow of events	1. The Ground Operation Control Center inform by passenger information system that door back-up closing test is starting and that any person shall stay far from doors 2. The Ground Operation Control Center launch the following actions in sequence a. Check that video surveillance is operative on every not isolated door (clear pictures of the vestibule) b. Check the communication with passenger is operative on every not isolated door c. Open all the door and simulate a major fault on every not isolated door d. Command the back-up closing of all the not isolated doors e. Check the closing of all the not isolated doors f. Remove the back-up closing command and doors major fault simulation on not isolated door g. Command the opening of the not isolated doors h. Check that all not isolated doors are opening and no faults are generated i. Command the closing of the not isolated doors j. Check that all not isolated doors are closing and no faults are generated
Post condition	Train in standstill, passenger doors closed,
Things that can go wrong	Any door doesn't open Any door doesn't close
Already implemented risk reduction measures	Test done in a moment when train has not maintenance activities Audible and visible alert activated before opening and closing the doors
Observations	The back-up door closing new device is supposed present on GoA3/4 trains, being in charge of the actions done by train crew on GoA1/2 train

Table 16: Testing of back-up door closing of every door

Use Case	Testing of mechanical isolation of every door
ID	PGT2
Actor	Ground Operation Control Center
Goal	G_PGT2: Check the functionality of the isolation function of all the not isolated doors of the train
Safety relation	The use case is safety relevant with relation to the hazards related to faulty isolation of the door (isolation command sent but isolation not executed) AND fault of safety loop bypass (safety loop bypassed with door not isolated
Precondition	Train in standstill, passenger doors closed, TCMS train-ground communication passenger information and video surveillance operative
Flow of events	1. The Ground Operation Control Center inform by passenger information system that door isolation test is starting, no one shall operate the door 2. The Ground Operation Control Center launch the following actions in sequence a. Check all door closed and locked (ADCL) information is active b. Simulate major fault on first not isolated door c. Check ADCL information is not active d. Command the isolation of the same door e. Check the isolation status of the doors f. Check the ADCL information is again activated g. Remove the major fault simulation on that door h. Command the de-isolation of that door i. Check the ADCL information is still active j. Repeat the same process on each not isolated door in sequence
Post condition	Train in standstill, passenger doors closed,
Things that can go wrong	Any door doesn't isolate Any door doesn't bypass the door safety loop: ADCL is not activated by isolation
Already implemented risk reduction measures	Double faults, diagnosis of isolation status independent from safety loop bypass
Observations	The remote controlled isolation new device is supposed present on GoA3/4 trains, being in charge of the actions done by train crew on GoA1/2 train

Table 17: Testing of mechanical isolation of every door

4.5.1 State of Art

4.5.1.1 Architectural principles

The actors of the Pantograph Test is the following ones (for GoA1/2 application, i.e. with a driver):

- Maintenance staff
- Driver

The Pantograph test is mostly linked to the following subsystems:

- TCMS

4.5.1.2 1.2 Sub-Functions

The functions covered by the Pantograph in EN15380-4 are the following ones.

- HBEJ Provide diagnostic information
- FB
- FDB

4.5.1.3 Safety requirements

The Pantograph depends on TSI Loc&Pas (5.3.10).

A pantograph shall be designed and assessed for an area of use defined by:
(1) The type of voltage system(s), as defined in clause 4.2.8.2.1. In case it is designed for different voltage systems, the various sets of requirements shall be taken into account.
(2) One of the 3 pantograph head geometries specified in clause 4.2.8.2.9.2.
(3) The current capacity, as defined in clause 4.2.8.2.4.
(4) The maximum current at standstill per contact wire of the overhead contact line for DC systems. Note: the maximum current at standstill, as defined in clause 4.2.8.2.5., shall be compatible with the value above, considering the characteristics of the overhead contact line (1 or 2 contact wires).
(5) The maximum operating speed: assessment of the maximum operating speed shall be performed as defined in clause 4.2.8.2.9.6.
(6) Range of height for dynamic behaviour: standard, and/or for 1 520 mm or 1 524 mm track gauge systems.
(7) The requirements listed above shall be assessed at IC level.
(8) The working range in height of pantograph specified in clause 4.2.8.2.9.1.2, the pantograph head geometry specified in clause 4.2.8.2.9.2, the pantograph current capacity specified in clause 4.2.8.2.9.3, the pantograph static contact force specified in clause 4.2.8.2.9.5 and the dynamic behaviour of the pantograph itself specified in clause 4.2.8.2.9.6 shall also be assessed at IC level.

4.5.1.4 Mission reliability impacts

Special attention needs to be given to TCMS, brake and propulsion design that prevents stopping a train at a hazardous location not suitable for rescue, e. g. tunnels or bridges. Therefore EN

50553 (REQUIREMENTS FOR RUNNING CAPABILITY IN CASE OF FIRE ON BOARD OF ROLLING STOCK) shall be applied in addition

4.5.1.5 Test at the start of the mission rationale

-TCMS test

-Function monitoring

-Manual Maintenance of the hole system every 3 -6 month .

4.5.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 still need to be performed in GoA3/4. TCMS will in future take over the tasks which were formerly performed by the driver.

4.5.3 GoA3/4 Tests at the start of the mission rationale

All the tasks performed by the driver during service in GoA1/2 need to be done either by ATO or TCMS.

Additional safety functions associated with shifting driver responsibilities to machine may result in an upgrade and extension of the ETCS telegrams or a third radio channel beyond ETCS and ATO

4.5.4 Use cases definition

-Powering up of the train, the Pantograph is systematically tested.

-Function monitoring, Checking position of pantograph (contact or auxiliary pressure feedback when Pantograph is down) when commanding up or down, by TCMS

-Pantograph Tests are periodically tested during train maintenance operations by the maintenance staff.

-Pantograph test is linked to a TCMS.

- Test of the Automatic Dropping Device (ADD) according to EN 50206-1

The following tables summarize the tests of the Pantograph Test.

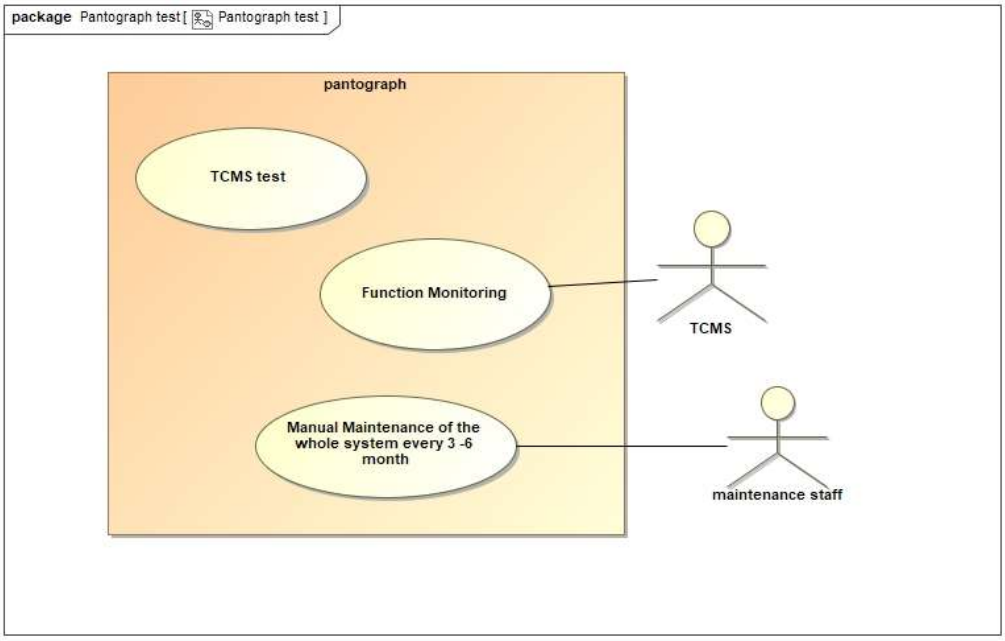

Figure 5: Pantograph Test

Use Case	Pantograph test
ID	
Actor	Pantograph, TCMS, maintenance stuff
Goal	Automated Pantograph
Safety relation	TSI lock§Pas 5.3.10
Precondition	The train is at a standstill
Flow of events	-TCMS test -Function monitoring -Manual Maintenance of the hole system every 3 -6 month, if needed
Post condition	The train is at a standstill
Things that can go wrong	System failure
Already implemented risk reduction measures	
Observations	

Table 18: Testing of Pantograph

4.6 AUXILIARIES POWER SUPPLY SYSTEM TEST

4.6.1 State of art

Main power supply can be realized based on 3 fundamental architectures:

1. Combustion engine – mechanical transmission – wheel
2. Combustion engine – hydraulic transmission – wheel
3. Some kind of electrical supply – power electronics – electric motor – wheel

Combined architectures are also possible with the combination of 1. and 2. having a significant market share in regional trains and hybrid solutions through combinations of 1./2. and 3. are becoming more an more popular.

Certainly the electric drive (3.) is the predominant architecture among the mentioned alternatives. Based on this setup the step towards hybrid systems featuring alternative power supplies is very small. So this architecture can be seen as generic and thus will be the basis for all considerations following below.

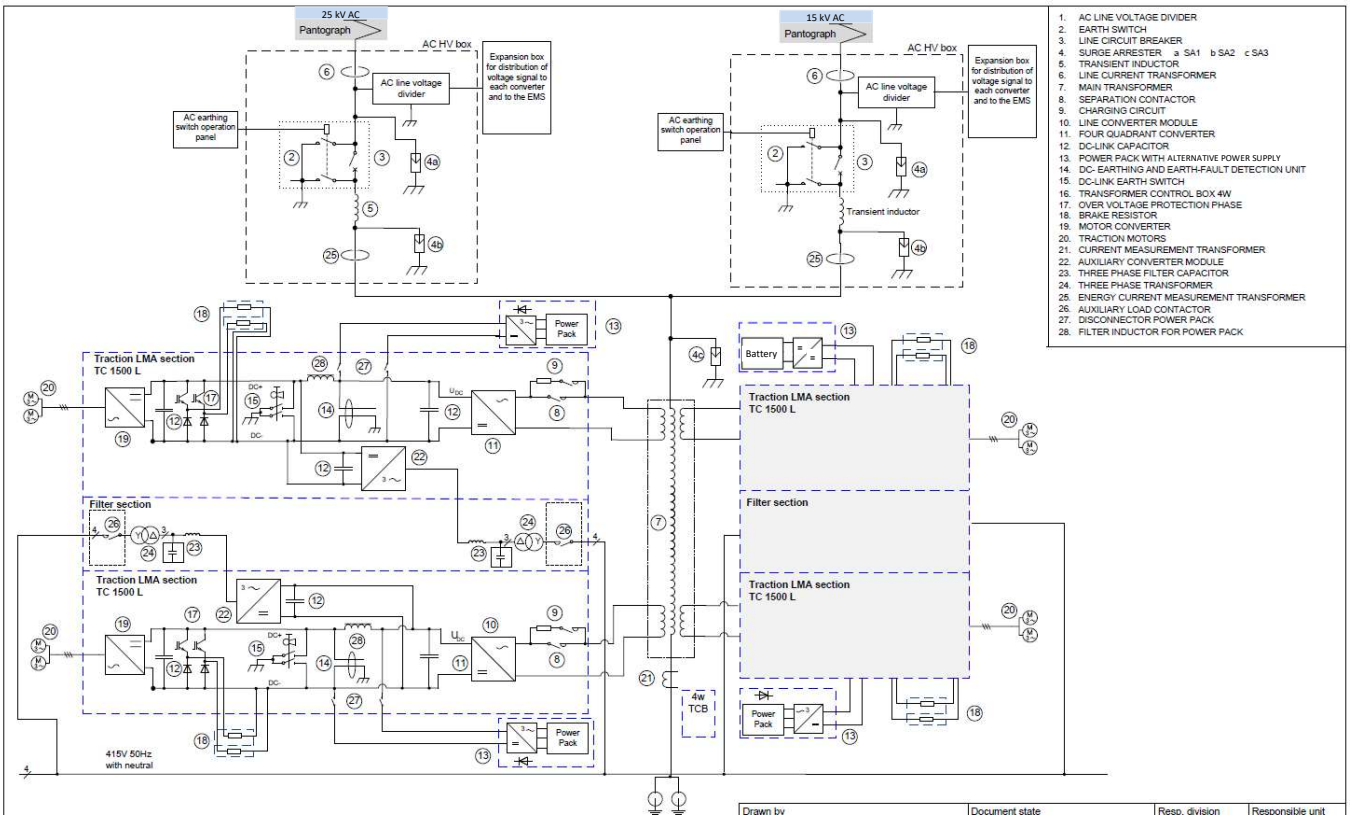

Figure 6 Power supply, generic system Architecture (example for multi mode/multi system setup)

4.6.1.1 Basic functional scope of the power supply system

F B Provide electrical energy for traction

F B B Manage electrical energy for traction, sense catenary voltage/current, configure input energy system

F B C Acquire energy demand for traction system

F B D Generate electrical energy for traction on board (generator set, fuel cell)

F B F Transform electrical energy for traction, manage transformation and conversion system, protect HV devices

F B G Protect distribution devices, Enable discharging, short circuiting and grounding

F B H Store electrical energy onboard for traction

F C Provide electrical energy for auxiliaries

F C B Manage electrical auxiliary energy provisioning/redundancies

This set of basic functions is reflected in the following vehicle functions:

- Manage country specific system configuration (semi automatic changeover in ETCS mode)
- Measure catenary voltage
- Switch/Interrupt voltage inputs
    - Transformer Main Out@15 kV
    - Transformer Main Out@ 25kV
    - Transformer THL Out
    - Choke Out @DC
    - Traction Battery Out
    - Generator/Rectifier Out
- Interlock inputs (Pantos, MCBs, line CB)
- LIM: Power Monitoring @ EmBr, monitor voltage, current, frequency
- LIM: Monitor interference current
- LIM: trigger protective actions (“MCB off “or “panto down”)
- Manage running through phase/system separation sections (RST level)
- Control DC-link voltage level (adapt to load + min/max supervision)
- Charge/discharge DC-link
- Control DC-link level during regenerative or dissipative el. braking

Main power supply diagnostic functions

- TCMS monitors all relevant values (voltages, currents)

- TCMS reads in the status of the main circuit switches and circuit breakers
- LIM device executes self-test on demand of the driver

4.6.1.2 Grade of automation in GoA 1/2

The main circuit and main power supply system have a high grade of auto monitoring, auto diagnostic and fail-safe design already today. From a safety point of view it is crucial that any manual action or inspection requiring to be near the high voltage components must be avoided. Indeed the driver's access to these component is locked and excluded by technical measures and a dedicated interlocking system.

The only manual actions required by the driver are:

- Acting on the pantograph switch
- Manually command MCB closing/opening
- Manually acknowledge re-activation of the energy supply the LIM has tripped
- Manually start self-test of the LIM device
- Communicate with shunting staff and manage the THL power supply during (un-)plugging of the THL connection according to the local safety rules.

4.6.2 Impacts of transition to GoA3/4

The driver actions required in GoA 1/2 are executed from the driver's desk and in GoA 3/4 operation will require a remote trigger instead of the local one. The rest of the power supply system will remain the same.

Certainly all status signals and diagnostic signals of the power supply system in GoA 3/4 operation shall be available in real time on the remote host.

When a shunter needs to plug/unplug the THL line the driver is responsible for deactivating the power supply before. Also a minimum staff-to-staff communication between shunter and driver is required.
This use case will require a corresponding semi-automatic function triggered by the shunter. The shunter himself shall be able trigger the safe deactivation of the THL. The vehicle must be able to indicate the safe state (unpowered and earthed) to the shunter.

4.6.3 GoA3/4 Tests at the start of the mission rationale

The built-in capabilities of the high voltage system (self-organizing and interlocking, fail-safe design) can be regarded as proven in use. As of today there are no special tests required at the start of mission each mission. Nevertheless, depending on future safety rules, some safety relevant subsystems should be capable of performing remotely triggered self-tests:

- Routine test of the LIM

- Routine test of the THL managing system when interacting with shunting staff
- Remote emergency shutdown
- Country selection and automatic system configuration.

4.6.4 Use cases definition

Use Case	Manage country specific system configuration
ID	PS1
Actor	Virtual driver
Goal	Receive and execute country selection and check plausibility.
Safety relation	Panto type and voltage must be correctly set
Precondition	TCMS and converter status ready for operation.
Flow of events	1. Country selection command received 2. System configuration automatically set 3. Correct panto is lifted and voltage monitoring starts 4. Check measured voltage/frequency level and GPS position data against commanded country. 5. Send check result to remote host. 6. Block execution of further commands in case of implausible result.
Post condition	When test passed, enable receiving MCB command after entering the normal operation mode.
Things that can go wrong	No suitable panto available, panto disfunction, implausible voltage detected
Already implemented risk reduction measures	MCB blockage in case of implausible voltage
Observations	The tests consists of the normal system routine and might not be required in daily operation.

Table 19: Manage country specific system configuration

Use Case	Check availability of the voltage inputs
ID	PS2
Actor	Virtual driver
Goal	Assure MCB commands can be executed when commanded.
Safety relation	Opening the MCB must be possible any time as a protective action.
Precondition	Country selected, panto lifted, plausibility check successful, line voltage available @ MCB entrance
Flow of events	1. Vehicle set into operating mode (unattended mode deactive) 2. Check preconditions for genset start. 3. Check preconditions for battery supply. 4. Check preconditions for fuel cell supply. 5. Send available supply options to stationary host. 6. When catenary supply voltage detected voltage plausibility check starts.
Post condition	When plausibility check successful, enable MCB closage.
Things that can go wrong	No suitable panto available, panto disfunction, implausible voltage detected
Already implemented risk reduction measures	MCB blockage in case of implausible voltage. MCB opened in case of overcurrent.
Observations	

Table 20: Testing of availability of the voltage inputs

Use Case	Trigger LIM selftest
ID	PS3
Actor	TCMS
Goal	When LIM faulty safely unlock MCB
Safety relation	LIM protects the vehicle from overvoltage and overcurrent. Staff safety and fire safety affected
Precondition	Battery power on, TCMS up, MCB off
Flow of events	1. Virtual driver to activate LIM self-test (every 24 h) 2. LIM test sequence starts 3. Send/save diagnostic report 4. Block execution of pantograph/MCB activation if test not passed 5. Save blockage until next successful LIM test
Post condition	LIM test successfully passed.
Things that can go wrong	LIM test failed, V/C/F sensor faults,
Already implemented risk reduction measures	MCB command blocked when LIM test failed.
Observations	

Table 21: Testing of Trigger LIM

Use Case	Acknowledge LIM Trips (LIM interface test)
ID	PS4
Actor	TCMS, virtual driver
Goal	Reset tripped LIM (today TBC acknowledgement)
Safety relation	LIM ensures SIL of the emergency brake, overcurrent/voltage detection.
Precondition	Panto up, MCB open, vehicle in test mode, LIM is active (no faults)
Flow of events	1. Virtual driver starts LIM interface test 2. TCMS-based test function forces LIM to trip 3. Virtual driver takes remote acknowledgement action 4. TCMS stops blocking the MCB command
Post condition	Test result is recorded, virtual driver is prompted for new test or leaving the test mode.
Things that can go wrong	Interface test not passed
Already implemented risk reduction measures	
Observations	This is non-daily preventive routine test

Table 22: Acknowledge LIM Trips (LIM interface test)

Use Case	Manage THL supply
ID	PS5
Actor	Virtual driver, shunting staff
Goal	Suspend THL supply whenever THL is (un-)plugged
Safety relation	Prevent risk of electrocution for shunting staff.
Precondition	Main power supply on, vehicle in unattended mode
Flow of events	1. Shunter commands THL deactivation 2. Vehicle performs THL deactivation sequence 3. Vehicle locks THL activation. 4. Vehicle indicates safe state to shunter and remote host. 5. Shunter acknowledges end of THL related task (could be automatically forced signal in test mode)
Post condition	Vehicle unlocks THL activation
Things that can go wrong	Malfunction of THL status indication,
Already implemented risk reduction measures	Operation rules
Observations	This is a routine test using the normal sequence (no test mode)

Table 23: Manage THL supply

4.7.1 State of art

Low Voltage (LV) Supply Architecture (Example)

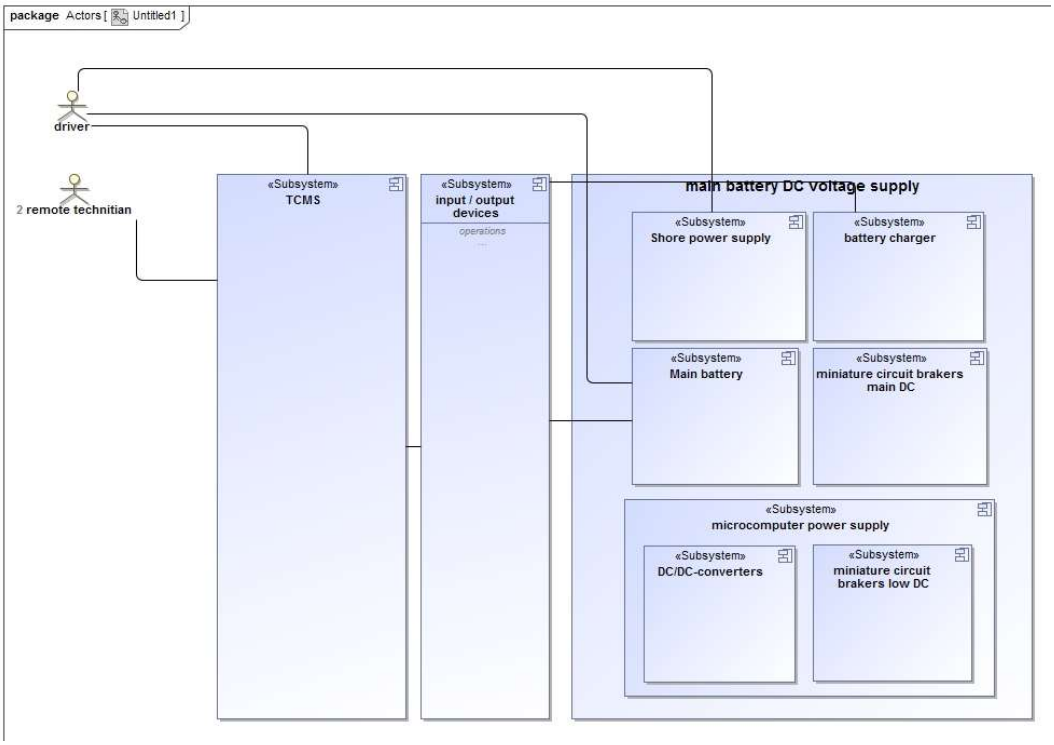

Figure 7 Low Voltage Supply Architecture

4.7.1.1 Functional Scope of low voltage supply

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

4.7.1.2 Technical features of a SoA System

In a typical state of art GoA1/2 application the low voltage system is monitored by the TCMS:

- TCMS monitors the status of relevant sub-systems such as the battery charger or the shore power plug status.

- DC/DC converters are equipped with simple health state indicators
- TCMS monitors the status of the miniature circuit breakers
- Optical feedback to driver and maintenance staff is possible using dedicated menus on the diagnostic screen or simply by looking at the circuit breaker boards.
- If required the complete actual monitoring state in the TCMS can be analysed using a PC-based tool.
- Remote service planning is possible based on programmable TCMS messages that are sent to stationary databases through a dedicated radio device. Quasi live monitoring of dedicated signals is possible.
- The communication vehicle to shore is “one-way”. No remote control capability

4.7.1.3 Low voltage supply system test rationale

In the light of the architecture and the functions described above having a stable LV-supply is obviously fundamental to safe and reliable operation of the vehicle. Hence the LV supply systems feature a high grade of automatic supervision and diagnostics already today. There are no regular routing tests to be performed by the staff in daily operation.

However regarding shore power supply there is a routine check required before the start of the mission in order to make sure that the all sockets are free and uncoupled. This routine status check requires the presence of technical staff in GoA1/2.

4.7.2 Impacts of transition to GoA3/4

The full TCMS based subsystem status must be permanently available in a remote virtual system without the need to physically connect to the vehicle’s TCMS. The corresponding signals must be available in real time. It can be expected that the number of transmitted signals will increase by one order of magnitude, which requires a high capacity connection to the wayside control.

The system architecture must be capable of bi-directional communication and control of the monitored subsystems according to a “digital twin” philosophy so that the remote technicians perform or trigger additional tests in case of failure.

The physical presence of external power supply plugs must me detected by a function that is independent from simply measuring the status of its supply voltage or current.

Degraded situations and remote tests would require circuit breakers that can be remotely set/reset. Today sealed circuit breakers activating certain safety relevant degraded modes must be replaced by an alternative solution including a digital “seal breaking procedure”.

The manual main battery switch must be replaced by an automated solution that can be controlled remotely.

A special unattended mode will be required in order to enable the vehicle to receive a “wake up - call.”

4.7.3 GoA3/4 Tests at the start of the mission rationale

4.7.3.1 Specification and rationale of routine checks

The high grade of monitoring and diagnostics already implemented in GoA1/2 vehicles naturally will be kept for GoA3/4 operation and will be amended by functions enabling remote monitoring and remote actions.

Automatic monitoring of the vital subsystems starts when the vehicle is powered up, hence when monitoring starts this can be considered as some kind of automatic routine test performed before the start of mission. Certainly this “test” continues permanently after the start of mission.

Safely detecting the status of the external supply plugs is a status check that must performed before being ready for the mission. However this automatic check is not a test in the sense of detecting the health status of a system.

4.7.3.2 Affected subsystems

Power Supply Devices

- Shore power 1 phase
- Shore power 3 phase
- Battery charger
- Battery state of charge

Miniature circuit breakers

- Read in and transmit status

DC/DC-Converters

- Read in and transmit health state

4.7.4 Use cases definition

Use Case	Test shore power 1 phase AC
ID	LVT1, F C E
Actor	TCMS
Goal	Detect if shore power is plugged in and make status available for remote actors.
Safety relation	Traction must be blocked when external power supply is plugged in.
Precondition	Vehicle TCMS is up and running.
Flow of events	1. TCMS running in unattended mode 2. 230 V shore power plugged in. 3. Plausibility check of voltage (level, frequency, current) 4. Block traction 5. Lock all 400 VAC auxiliaries 6. Check if all systems expected to be powered in unattended mode are running (e.g. battery charger)
Post condition	
Things that can go wrong	External supply plugged in, but not powered (failure on the shore side).
Already implemented risk reduction measures	Automatic traction interlock train when external voltage detected.
Observations	

Table 24: Testing shore power 1 phase AC

Use Case	Test shore power 3 phase AC
ID	LVT2, F C E
Actor	TCMS, local staff near vehicle
Goal	Detect if shore power is plugged in and make status available for remote actors.
Safety relation	Traction must be blocked when external power supply is plugged in.
Precondition	Vehicle TCMS is up and running.
Flow of events	1. TCMS running in unattended mode 2. 400 V shore power plugged in. 3. Plausibility check of voltage (level, frequency, current) 4. Block traction 5. Check if all systems expected to be powered in unattended mode are running (e.g. battery charger, HVAC, compressor)
Post condition	
Things that can go wrong	External supply plugged in, but not powered (failure on the shore side).
Already implemented risk reduction measures	Automatic traction interlock train when external voltage detected.
Observations	

Table 25: Testing shore power 3 phase AC

Use Case	Check battery charger
ID	LVT3, F C H
Actor	TCMS
Goal	Permanently check correct operation of the main battery charger (BC)
Safety relation	
Precondition	Vehicle TCMS is up and running.
Flow of events	1. TCMS running in unattended mode 2. Battery charger automatically start operation when supply voltage detected. 3. BC hardware performs self test 4. BC sends permanent health signals
Post condition	
Things that can go wrong	Battery charger power electronics broken. – Battery not charged.
Already implemented risk reduction measures	Automatic emergency stop when battery undervoltage detected.
Observations	

Table 26: Check battery charger

Use Case	Check battery voltage
ID	LVT4, F C H
Actor	TCMS
Goal	Permanently monitor battery voltage and detect state of charge. Send a warning message to the wayside in case voltage level drops below a defined threshold.
Safety relation	In case of low battery voltage the function shall trigger a safety function that stops the train.
Precondition	Vehicle TCMS is in unattended mode.
Flow of events	1. Battery switch activated 2. TCMS powered up to at least unattended mode 3. Measure and send state of charge 4. 4 trigger alarm event if required
Post condition	
Things that can go wrong	Battery charger disturbed. Battery cells failed.
Already implemented risk reduction measures	Automatic emergency stop when battery undervoltage detected.
Observations	

Table 27: Check battery voltage

Use Case	Control miniature circuit breakers
ID	LVT5, F C H
Actor	TCMS
Goal	Permanently monitor and transmit the status of each miniature circuit breaker (MCB) and manual switch. The set of activated LV-circuits must be checked against the desired state required for the mission. If required the MCB must be actively set to the position commanded by the remote staff.
Safety relation	There are safety relevant MCBs that control overrides for certain degraded situations. These require a safe remote acknowledgement procedure.
Precondition	Vehicle TCMS is in unattended mode.
Flow of events	1. Battery switch activated 2. TCMS powered up to at least unattended mode 3. Full set of position states of all MCBs and switches are transmitted to digital twin. 4. When system environment is set compare actual status against
Post condition	
Things that can go wrong	Activation of override switch does not work. Rescue train required.
Already implemented risk reduction measures	
Observations	

Table 28: Check miniature circuit breakers

Use Case	Monitor DC/DC-Supply
ID	LVT6, F C H
Actor	TCMS
Goal	Detect the power margin in the low voltage supply though evaluation of the status signals of the DC/DC-converters.
Safety relation	-none-
Precondition	Vehicle TCMS is active/attended mode.
Flow of events	1. Check the health signals of all DC/DC converters 2. Calculate the expected max. power demand during the current mission 3. Deactivate low priority functions in case of possible lack of power. 4. Send diagnostics on DC/DC converter status and available LV-subsystems.
Post condition	
Things that can go wrong	Important devices malfunction due to undervoltage if DC/DC is overloaded.
Already implemented risk reduction measures	Automatic deactivation of subsystems according to the actual performance of the DC/DC-supply
Observations	

Table 29: Monitor DC/DC-Supply

4.8 AIR GENERATION AND TREATMENT UNIT TEST

This document aims at contributing to the chapter 2.13 Air Generation and Treatment Unit Test of the deliverable D3.1 of TAURO's WP3.

The state of the art of Air Generation and Treatment Unit Test for not autonomous trains (GoA1/2) is described hereafter.

A reliable air supply system is essential for a reliable and safe train operation as it supplies safety critical functions as the brake system.

Today monitoring of the air supply system and the responsibility for this is mainly taken under the responsibility of the train driver.

Already today, for operation schemes up to GoA2 systems, intense diagnosis/ monitoring, partly done manually, are necessary for air supply systems. For later GoA3/4 systems different procedures, maybe done automatically, might be needed.

The document on hand describes functional tests for up to GoA2 trains related to the air supply system to be done before starting the service operation. The use cases described are based on existing documentation as EN15380-4 (“Railway applications – Classification system for railway vehicles – Part 4: Function groups).

There are also “indirect” availability tests of the air supply system done by other functions onboard the train, e.g. the brake system. Those can for example be found in EN16185-1 (2014+A1:2020 (E)) or EN15734-1 (2010 + AC:2013 (E)).

Today’s use cases will be the basis for the development of future functional tests for autonomous trains as their contents needs to be covered by automatic functions without presence of any assistance or driver.

Manual work related to maintenance use cases will still be necessary in future, whereas the work might relate to the maintenance itself (checking optically the air supply system, checking of the air dryer, …) and not to the performance of checks which might be automated.

In a next step, modifications to those tests will be done in order to integrate the tests into GoA3/4 trains.

4.8.1 State of art

4.8.1.1 Architectural principles (Actors and systems involved)

The Air Generation and Treatment Unit for GoA1/2 is mostly linked to the following subsystems:

- TCMS,
- Auxiliary systems, e.g. brake, air suspension,
- Driver’s desk HMI.

The actors dealing with the Air Generation and Treatment Unit for GoA1/2 application are the following:

- Driver,
- Maintenance staff.

4.8.1.2 Sub-functions of “Air Generation and Treatment Unit Test”

The following sub-functions of EN15380-4 are involved by Air generation and treatment unit test

- F E Provide fluid energy for auxiliaries fluid energy refers to hydraulic/pneumatic media
- F E B a Manage fluid energy for auxiliaries
- 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 work shop storage
- F E E Store fluid energy for auxiliaries pneumatic energy storage vessel for air suspension

4.8.1.3 Safety requirements

In fact, no direct safety requirements for Air Generation and Treatment Units could be found. Nevertheless, the air supply is important for the availability of safety relevant systems, as the brake system. Hence within standards related to those, as EN15734-1, there are requirements related to air supply as “the availability of the compressed air shall continuously be monitored, the compressed air shall be stored in a dedicated reservoir and its availability shall be continuously monitored” (chapter 5.5). Those can be considered when defining the use cases for the Air Generation and Treatment Units.

4.8.1.4 Mission reliability impacts

As a result of the air supply tests it can be assumed, that a train has enough compressed air under all circumstance to operate safely.

4.8.1.5 Test at the start of the mission rationale

Testing a subsystem can be performed with:

- Tests at start-up (powering up of the train),
- Periodical tests during maintenance (recurrence system-dependent),
- Continuous monitoring.

Focussing on the tests during start-up, usually before a train is leaving the depot in the morning automated and semi-automated tests must be performed. Since a certain time, trains are already able to perform the fully automated tests before the driver enters the driver's cab. Therefore, the driver just has to start the semi-automated and by hand performed tests.

In case of failures that do not allow safe operation of the overall train (fill up time of compressed air, tightness of the pressurised system), the operator can early decide whether this train can go into service or not.

4.8.2 Impacts of transition to GoA3/4

Thinking about having a train running in GoA3/4 mode, the TCMS will in future take over the tasks which were formerly performed by the driver.

Hence the execution of tests at startup and the reporting of their results might change. Currently an indicator lamp or a message on the HMI informs the driver about the train and test status/ result. With the driver not being available in GoA3/4, these messages need to be provided to and handled by the TCMS which then needs to select a measure based on the information (e.g. forwarding of the information to trackside units).

4.8.3 GoA3/4 Tests at the start of the mission rationale

To ensure safe train operation there are tests which need to be automated in future as no driver/ train attendant will be onboard of the train. An exact definition of the test to be automated and how that can be done is not in focus of the project yet and will be handled later on in the project.

4.8.4 Use cases definition

Use Case	Testing of fill up time per compressor
ID	AT1
Actor	Virtual Driver
Goal	G_AT: Make sure compressor(s) can fill up the compressed air system within the designed time.
Safety relation	Availability of the air compressors is/are safety relevant
Precondition	Train has power for operating the compressors
Flow of events	10. Isolate all compressor(s) from electrical power, except the one under test 11. Cause a level of compressed air close to the lower limit 12. Monitor the time the compressor under test needs to fill up the system 13. Check whether the fill up time is within the limits 14. Repeat the above steps for all compressors in the system
Post condition	Inform the TCMS/Driver whether all compressors are able to fill up the system within the designed time.
Things that can go wrong	Too less performance of a compressor to fill up the system
Already implemented risk reduction measures	
Observations	

Table 30: Testing of fill up time per compressor

Use Case	Testing tightness of the system for compressed air
ID	AT2
Actor	Virtual Driver
Goal	G_AT2: Make sure the system with compressed air is sufficiently tight
Safety relation	Availability of compressed air is safety relevant
Precondition	Compressed air system is filled sufficiently
Flow of events	1. Check whether the system has enough compressed air for testing 2. Signal to all systems which are using compressed air, that they should not use compressed air (stay quiet). 3. Monitor the overall compressed air system 4. Check whether the decrease of compressed air level over a certain time is within the limits
Post condition	Decrease of compressed air level is within the designed bandwidth
Things that can go wrong	Loss of compressed air is higher than excepted.
Already implemented risk reduction measures	
Observations	

Table 31: Testing tightness of the system for compressed air

Use Case	Testing of automatic emergency brake in case of too low compressed air level
ID	AT3
Actor	Virtual Driver
Goal	G_AT3: Check, whether emergency brake is automatically applied if the level of compressed air is below the safety limit
Safety relation	Automatic triggering of emergency brake is safety relevant
Precondition	Compressed air system is filled sufficiently
Flow of events	1. Check whether the system has enough compressed air for testing 2. Isolate all compressor(s) from electrical power 3. Cause a level of compressed air below the safety limit (e.g. through brake application/release) 4. Check whether the emergency brake is automatically triggered
Post condition	Emergency brake has been triggered automatically at the moment, the level of compressed air went below the safety limit.
Things that can go wrong	No automatic triggering of the emergency brake.
Already implemented risk reduction measures	
Observations	

Table 32: Testing of automatic emergency brake in case of too low compressed air level

Use Case	Test of the air dryer changeover
ID	AT4
Actor	Virtual Driver
Goal	G_AT4: Error-free operation of the air dryer changeover is essential for the availability of the compressed air system. Therefore, it should (besides the monitoring during normal operation) be tested separately.
Safety relation	Availability of compressed air is safety relevant
Precondition	Train has power for operating the compressors
Flow of events	1. Keep the compressor running through permanent usage of compressed air (e.g. brake application/release) 2. Monitor the used air dryer 3. Check whether the used air dryer has been changed after the designed time 4. Monitor the used air dryer 5. Check whether the used air dryer has been changed again after the designed time Repeat the above steps for all compressors in the system.
Post condition	Air dryer switchover has been performed within the designed time.
Things that can go wrong	Switchover of the air-dryer is not performed within the designed time.
Already implemented risk reduction measures	
Observations	

Table 33: Testing of the air dryer changeover

Besides these requirements further ones could be generated by review of railway undertaking's operational rules. From those especially the frequencies of the tests could be found out. As no operational rules were available during the generation of the document on hand, no further use cases could be derived.

4.9 TRACTION TEST

4.9.1 State of Art

4.9.1.1 Architectural principles

The actors of the Traction are the following ones for GoA1/2 application:

- Maintenance staff
- Driver

The Traction is mostly linked to the following subsystems:

- TCMS

4.9.1.2 Sub-Functions

The functions covered by the Traction in EN15380-4 are the following ones.

- HBED Provide control command information
- GB Provide acceleration
- GC Provide deceleration

4.9.1.3 Safety requirement

The Traction system depends on TSI Loc&Pas (4.2.8.4).

Rolling stock and its electrically live components shall be designed such that direct or indirect contact with train staff and passenger is prevented, both in normal cases and in cases of equipment failure.

4.9.1.4 Mission reliability impacts

Special attention needs to be given to TCMS, brake and propulsion design that prevents stopping a train at a hazardous location not suitable for rescue, e. g. tunnels or bridges. Therefore EN 50553 (REQUIREMENTS FOR RUNNING CAPABILITY IN CASE OF FIRE ON BOARD OF ROLLING STOCK) shall be applied in addition.

4.9.1.5 Test at the start of the mission rationale

-TCMS test

-Function monitoring

-Manual Maintenance of the hole system every 3 -6 months

4.9.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 may still need to be performed in GoA3/4, However TCMS will in future take over the tasks which were formerly performed by the driver.

4.9.3 GoA3/4 Tests at the start of the mission rationale

All the tasks performed by the driver during service in GoA1/2 need to be done either by ATO or TCMS.

Additional safety functions associated with shifting driver responsibilities to machine may result in an upgrade and extension of the ETCS telegrams or a third radio channel beyond ETCS and ATO.

4.9.4 Use cases definition

- Powering up of the train, the Traction is systematically tested.
- Traction Tests are periodically tested during train maintenance operations by the maintenance staff.
- Traction test is linked to a TCMS.

The following tables summarize the tests of the Traction.

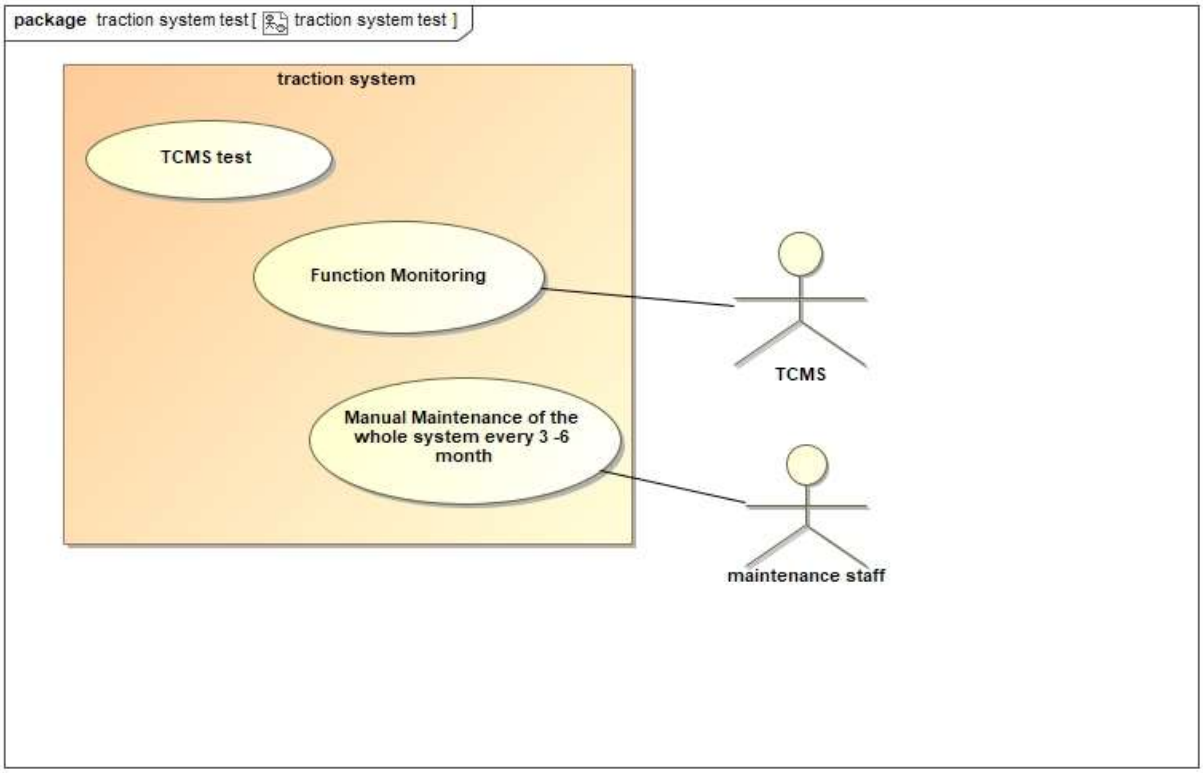

Figure 8: Traction Test

Use Case	Traction System test
ID	
Actor	Traction system, TCMS, maintenance staff
Goal	Automated traction system
Safety relation	TSI (Loc&Pas) 4.2.8.4
Precondition	The train is at a standstill
Flow of events	-TCMS test -Function monitoring -Manual Maintenance of the whole system every 3 -6 month, if needed
Post condition	The train is at a standstill
Things that can go wrong	System failure
Already implemented risk reduction measures	
Observations	

Table 34: Testing Traction

4.10 BRAKE TEST

Braking is safety critical in rail operation. As a supporting function adhesion management is also critical related to achievable braking distances in low adhesion situations. Nevertheless, today the responsibility for this is mainly taken by the train driver.

Already today, for operation schemes up to GoA2 systems, intense diagnosis/ monitoring, partly done manually, is necessary for braking and adhesion management systems. For later GoA3/4 systems different procedures, maybe done automatically, might be needed.

The document on hand describes functional tests for up to GoA2 trains related to brakes and adhesion management (represented by the sanding function) to be done before starting the service operation. The use cases described are based on existing documentation as:

- EN15380-4 (“Railway applications – Classification system for railway vehicles – Part 4: Function groups,
- High level use case list provided by CTA-1,
- Standards/ regulations as:
    - EN16185-1 (2014+A1:2020 (E)),
    - EN15734-1 (2010 + AC:2013 (E)),
    - CEN/TS 15427-1-3 (2021 (D)).

Today’s use cases will be the basis for the development of future functional tests for autonomous trains as their contents needs to be covered by automatic functions without presence of any assistance or driver.

Manual work related to maintenance use cases will still be necessary in future, whereas the work might relate to the maintenance itself (changing brake pads, refilling sand, etc.) and not to the performance of checks which might be automated.

In a next step, modifications to those tests will be done in order to integrate the tests into GoA3/4 trains.

4.10.1 State of art

4.10.1.1 Architectural principles (Actors and systems involved)

The brake system / adhesion management system for GoA1/2 is mostly linked to the following subsystems:

- TCMS,
- ATO onboard,
- ETCS onboard,
- Driver’s desk HMI,
- Brake system,
- Adhesion management system (e.g. sanding).

The actors of the brake system and the adhesion management system for GoA1/2 application are the following:

- Driver,
- Train operator,
- Ground Signalling System,
- Maintenance staff.

4.10.1.2 Sub-functions of “Brake and Adhesion Management”

4.10.1.2.1 Brake system sub functions based on EN15380-4

- 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

4.10.1.2.2 Adhesion management sub functions

In the document on hand adhesion wheel/rail management is represented by the sanding function. The maintenance and diagnosis measures derived from it, can later be generalised towards other adhesion management functions.

For the generation of sanding related sub functions and later use cases, multiple sources were considered.

The first basis was the EN15380-4 (“Railway applications – Classification system for railway vehicles – Part 4: Function groups). Therein several sub functions are defined for the sanding function but without any detailed specification. Hence, those can only be taken as a general hint for the later use case specification.

The second source for sub functions is the high-level list provided by CTA-1. Out of this list one use case could be generated.

Furthermore, existing normatives / standards were considered as:

- EN16185-1 (2014+A1:2020 (E)),

- EN15734-1 (2010 + AC:2013 (E)),
- CEN/TS 15427-1-3 (2021 (D)).

Out of those also diagnosis/ monitoring use cases can be deduced.

Beyond, operators might have their own internal operational rules. As none of those documents was available during generation of the document on hand, they have not been considered.

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

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

4.10.1.3 Safety requirements

The safety requirements for brake systems are described in the TSI Loc&Pas in chapter 4.2.4.2.2.

(1) The braking system is the means to stop a train, and therefore contributes to the safety level of the railway system. The functional requirements expressed in clause 4.2.4.2.1 (remark: clause in TSI Loc&Pas) contribute to ensure safe functioning of the braking system; nevertheless, a risk based analysis is necessary to evaluate the braking performance, as many components are involved.

(2) For the hazardous scenarios considered, the corresponding safety requirements shall be met, as defined in the Table 3 below (see Figure 9). Where a severity is specified within this table, it shall be demonstrated that the corresponding risk is controlled to an acceptable level, considering the functional failure with their typical credible potential to lead directly to that severity as defined within the table.

Table 3

Braking system — safety requirements

		Safety requirement to be met	
	Functional failure with its hazardous scenario	Associated severity/ Consequence to be prevented	Minimum allowable number of combinations of failures
No 1			
	Applies to units fitted with a cab (brake command)		
	After activation of an emergency brake command no deceleration of the train due to failure in the brake system (complete and permanent loss of the brake force). Note: activation by the driver or by the CCS system to be considered. Activation by passengers (alarm) not relevant for the present scenario.	Fatalities	2 (no single failure is accepted)

		Safety requirement to be met	
	Functional failure with its hazardous scenario	Associated severity/ Consequence to be prevented	Minimum allowable number of combinations of failures
No 2			
	Applies to units equipped with traction equipment		
	After activation of an emergency brake command, no deceleration of the train due to failure in the traction system (Traction force ≥ Brake force).	Fatalities	2 (no single failure is accepted)
No 3			
	Applies to all units		
	After activation of an emergency brake command, the stopping distance is longer than the one in normal mode due to failure(s) in the brake system. Note: the performance in the normal mode is defined in clause 4.2.4.5.2.	NA	single point(s) failure(s) leading to the longest calculated stopping distance shall be identified, and the increase of the stopping distance compared to the normal mode (no failure) shall be determined.
No 4			
	Applies to all units		
	After activation of a parking brake command, no parking brake force applied (complete and permanent loss of the parking brake force).	NA	2 (no single failure is accepted)

Figure 9: Braking system safety requirements based on TSI Loc&Pas

For adhesion management, especially the sanding function, no explicit safety requirement could be found. In general, the use of those systems is under responsibility of the driver for GoA1/2 systems. This might need to be updated for GoA3/4 systems, when those systems might need to be activated automatically.

4.10.1.4 Mission reliability impacts

As a result of the brake test, a brake weight percentage can be calculated. This way, already before operation the performance of the braking system can be checked and therewith the behaviour can reliably be determined (mission reliability).

4.10.1.5 Test at the start of the mission rationale

Testing a subsystem can be performed with:

- Tests at start-up (powering up of the train),
- Periodical tests during maintenance (recurrence system-dependent),
- Continuous monitoring.

Focussing on the tests during start-up, usually before a train is leaving the depot in the morning automated and semi-automated tests must be performed. Since a certain time, trains are already able to perform the fully automated tests before the driver enters the driver's cab. Therefore, the driver just has to start the semi-automated and by hand performed tests.

Using these tests, certain failures can already be detected before the train going into service. Calculation the train performance based on these tests a specific availability of the overall brake system is given. In case of failures, a performance value of the train can be defined, which allows operation with nominal or degraded performance. For example, if one brake controller has a failure, a certain bogie can be "locked" and does not contribute to the overall brake performance. In this case operation is possible in a degraded mode (reduced brake percentage, e.g. by 1 bogie out of 16).

In case of failures that do not allow safe operation of the brake system (build up time of Emergency Brake, fill up time of compressed air, tightness of the pressurised system), the operator can early decide whether this train can go into service or not.

4.10.2 Impacts of transition to GoA3/4

Thinking about having a train running in GoA3/4 mode, the TCMS will in future take over the tasks which were formerly performed by the driver.

Hence the execution of tests at startup and the reporting of their results might change. Currently an indicator lamp or a message on the HMI informs the driver about the train and test status/ result. With the driver not being available in GoA3/4, these messages need to be provided to and handled by the TCMS which then needs to select a measure based on the information.

Some measures, e.g. brake tests, can already be done automatically today, others as the sand flow determination which are today mostly done by the driver, need to be automated in future.

Other tests and maintenance activities which are usually performed in the depot today, might still not be changed for GoA3/4, e.g. the filling of sand into the sand boxes.

4.10.3 GoA3/4 Tests at the start of the mission rationale

To ensure safe train operation the tests that are currently done manually, for example commanded by the driver, need to be automated in future. These are for example the sand flow determination tests. How the automation can be done will be defined later in the project.

4.10.4 "Brake and Adhesion Management" use cases definition

4.10.4.1 Brakes Use Cases

Use Case	Testing of brake system is powered on
ID	BT1
Actor	Virtual Driver
Goal	G_BT1: Make sure brake receives electrical power
Safety relation	Availability of the brake system(s) is/are safety relevant
Precondition	Train has power / Battery power is available
Flow of events	3. The relay to power on brake system is closed 4. The presence of a signal indicating brake system is UP is received
Post condition	An indication (GoA1/2: DMI icon, GoA3/4: signal) is received indicating brake system is UP
Things that can go wrong	Any of the brake systems is not powered up
Already implemented risk reduction measures	
Observations	

Table 35 –Testing of brake system is powered on

Use Case	Testing of passed self-tests
ID	BT2
Actor	Virtual Driver
Goal	G_BT2: Make sure all supplier specific tests passed
Safety relation	Availability of the brake system(s) is/are safety relevant
Precondition	Brake system is powered on
Flow of events	Brake system self-tests after power on.
Post condition	Self-tests have shown no failure
Things that can go wrong	Self tests not passed
Already implemented risk reduction measures	
Observations	

Table 36 –Testing of passed self-tests

Use Case	Testing of connectivity to brake system(s)
ID	BT3
Actor	Virtual Driver
Goal	G_BT3: Check brake system is connected to the required networks and buses.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant
Precondition	Brake system is powered on and self-tests are finished
Flow of events	1.1.1.1 TCMS starts communication with brake system 1.1.1.2 TCMS is able to communicate without problems
Post condition	Communication is checked and shows no failures
Things that can go wrong	Communication is not working or free from failures
Already implemented risk reduction measures	
Observations	

Table 37 –Testing of connectivity to brake system(s)

Use Case	Test application and release of parking brake
ID	BT4
Actor	Virtual Driver
Goal	G_BT:.
Safety relation	Availability / Connectivity of the parking brake system(s) is/are safety relevant
Precondition	-Brake system is powered on and self-tests are finished -Air supply is showing enough air in the system
Flow of events	Systems with manual/controlled parking brake application and release: 1. TCMS commands application of parking brake 2. Waiting for a designed time for an applied parking brake 3. TCMS commands release of parking brake 4. Waiting for a designed time for released parking brake
Post condition	Application and release of parking brake has been performed within the designed time limits.
Things that can go wrong	-Parking brake has been not applied -Parking brake has been not released
Already implemented risk reduction measures	
Observations	

Table 38 –Testing application and release of parking brake

Use Case	Test application and release of emergency brake
ID	BT5
Actor	Virtual Driver
Goal	G_BT:.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant Application and release of the emergency brake is fundamental.
Precondition	-Brake system is powered on and self-tests are finished -Air supply is showing enough air in the system
Flow of events	-TCMS and/or Virtual Driver opens the emergency brake loop -brake system applies emergency brake pressure -TCMS and/or Virtual Driver closes the emergency brake loop -brake system releases emergency brake pressure
Post condition	Brake system applies holding brake pressure or released brake pressure
Things that can go wrong	-Brake system doesn't apply emergency brake pressure -Brake system responds with a diagnostic that the application of the emergency brake pressure was wrong or not in time
Already implemented risk reduction measures	
Observations	

Table 39 –Testing application and release of emergency brake

Use Case	Test application and release of service brake
ID	BT6
Actor	Virtual Driver
Goal	G_BT:.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant
Precondition	-Brake system is powered on and self-tests are finished -Air supply is showing enough air in the system
Flow of events	-Release the holding brake for a part of a train -Apply service brake with brake demand stepwise up to 100% for a part of a train -Check for each step whether the application level has been correctly applied -Release service brake stepwise via change in brake demand -Check for each step whether the application level has been correctly applied Repeat the above step for the other part(s) of the train
Post condition	No diagnostic state identified due to service brake application/release
Things that can go wrong	Application of the demanded service brake pressure is not performed within required deviation.
Already implemented risk reduction measures	
Observations	

Table 40 –Testing application and release of service brake

Use Case	Test application and release of holding brake
ID	BT7
Actor	Virtual Driver/TCMS
Goal	G_BT:.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant An automatic application of holding brake based on service brake function and necessary for holding trains at stations.
Precondition	-Brake system is powered on and self-tests are finished -Air supply is showing enough air in the system
Flow of events	-Release the holding brake for a part of a train -Check whether brake system has release for that part of the train the brake system -Reapply the holding brake for the whole train -Repeat the above steps for all parts of the train
Post condition	No diagnostic state identified due to holding brake application/release
Things that can go wrong	Application of the demanded holding brake pressure is not performed within required deviation and time limit.
Already implemented risk reduction measures	
Observations	

Table 41 –Testing application and release of holding brake

Use Case	Test the safety functions of wheel slide protection
ID	BT8
Actor	Virtual Driver/TCMS
Goal	G_BT:.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant
Precondition	Brake system is powered on and self-tests are finished
Flow of events	-Start the safety function self-test of the WSP subsystem for a part of the train. -Check the test response of the WSP subsystem for a successful test -Repeat the above tests for all other parts of the train
Post condition	Safety function of the WSP subsystem shows no error
Things that can go wrong	WSP subsystem has identified a problem with the safety function.
Already implemented risk reduction measures	
Observations	

Table 42 –Testing the safety functions of wheel slide protection

Use Case	Test the effect of WSP activity
ID	BT9
Actor	Virtual Driver
Goal	G_BT:.
Safety relation	Availability / Connectivity of the brake system(s) is/are safety relevant
Precondition	Brake system is powered on and self-tests are finished
Flow of events	-Ensure train has an applied brake system -Start the test run for WSP activity for a part of the train -Monitoring of WSP activity is ongoing and shows no problems -Repeat the above tests for all other parts of the train
Post condition	Monitoring function of the WSP subsystem shows no error in monitoring the anti-skid valve operation
Things that can go wrong	WSP subsystem has identified a problem with the anti-skid valve operation
Already implemented risk reduction measures	
Observations	

Table 43 –Testing the effect of WSP activity

4.10.4.2 Adhesion Management Use Cases

Based on EN16185-1 chapter 5.16,

> *5.16 Enhancement of wheel-rail adhesion*
>
> *A means shall be provided for testing the correct function of the wheel-rail adhesion compensation system during train maintenance, including a means for checking the individual rate and consistency of deposition of the substance used is within acceptable limits and that speed and other vehicle system interlocks (e.g. WSP) are active.*
>
> *It shall be possible to check the quantity of the substance required to ensure daily operation which is used for compensating low levels of wheel-rail adhesion. The driver should be provided with a warning in the event that the quantity falls below the minimum level prescribed for normal train operation.*

and EN15734-1 chapter 5.17,

> *5.17 Enhancement of wheel-rail adhesion*
>
> *A means shall be provided for testing the correct function of the wheel-rail adhesion compensation system during train maintenance, including a means for checking that the rate and consistency of deposition of the substance used is within acceptable limits and that speed and other vehicle system interlocks (e.g. WSP) are active.*
>
> *It shall be possible to check the quantity of the substance used for compensating low levels of wheel/rail adhesion both locally at all storage positions on the train and remotely from the active drivers cab. The driver should be provided with both an audible and visual warning in the event that the quantity falls below the minimum level prescribed for normal train operation*

requirements related to maintenance/diagnosis could be found:

- amount of sand deployed on the rail (can also be found in CTA-D1.2-UC-99)
- consistency of sand deposition
- quantity of sand available in the reservoir
- sand deployment interlocks (e.g. Speed, …)

Use Case	Check sanding rate and consistency
ID	AM-1
Actor	Virtual Driver
Goal	Assure correct functionality of the sanding system.
Safety relation	Safety relevance: - Failure in the sanding rate leads to too high output of sand affecting train safety (track circuits). - Failure in the sanding rate leads to too low output of sand affecting the wheel/rail adhesion improvement negatively and therewith leading to too low deceleration. - Failure in the consistency of deposition leading to too low amount of sand deployed on the rail and therewith to reduced wheel/rail adhesion improvement leading to too low deceleration.
Precondition	Train is at standstill
Flow of events	1) The train is powered up 2) The sander is activated 3) The sand amount deployed in the test scenario is checked ((simulated) speed dependent, if applicable). 4) The orientation of the sand tube is checked visually
Post condition	Train is at standstill
Things that can go wrong	Sand is deployed in wrong amount. Sand is deployed in wrong place. Based on the sanding rate also wet sand in the container can be detected (faulty heating,…).
Already implemented risk reduction measures	
Observations	

Table 44 – Testing sanding rate and consistency

Use Case	Check sand level
ID	AM-2
Actor	Virtual Driver
Goal	Assure sand is available if needed.
Safety relation	Safety relevance: - In case there is too less sand available the necessary wheel/rail adhesion improvement cannot be guaranteed leading to lower deceleration and prolonged stoppingdistances.
Precondition	Train is at standstill/ during operation
Flow of events	1) The train is powered up 2) Diagnosis means measure the sand level and check if there is sufficient material available (both locally and remotely, audible and visual warning). 3) Eventually the train's maximum speed is reduced.
Post condition	Train is at standstill/ during operation
Things that can go wrong	Too less material available.
Already implemented risk reduction measures	
Observations	

Table 45 –Check sand level

Use Case	Check interlocks
ID	AM-3
Actor	Driver
Goal	Assure available interlocks are working correctly.
Safety relation	Safety relevance: - In case interlocks are not working correctly dangerous situations can emerge. One example would be a faulty speed interlock leading to deployment of sand below 30kph which could interrupt track circuits.
Precondition	Train is at standstill
Flow of events	1) The train is powered up 2) Sanding is activated with an interlock being active. 3) Activation of sanding function is being monitored.
Post condition	Train is at standstill
Things that can go wrong	Faulty interlock not deactivating the deployment of sand.
Already implemented risk reduction measures	
Observations	

Table 46 –Testing Interlock

Besides these requirements further ones could be generated by review of railway undertaking's operational rules. From those especially the frequencies of the tests could be found out. As no operational rules were available during the generation of the document on hand, no further use cases could be derived.

4.11.1 State of art

4.11.1.1 Architectural principles (Actors and systems involved)

The Horn system for GoA1/2 are involving the following subsystems:

- TCMS,
- Horns high note and low note above cab on both ends of train
- Switch on drivers' desk.

The actors dealing with the horn system for GoA1/2application are the following:

- Driver,
- Maintenance staff.

In GoA3/4 application the today utilized driver and maintenance staff must be replaced with microphones.

4.11.1.2 Sub-functions of "Horn Test"

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

4.11.1.3 Safety requirements

Requirements are defined by LOC&PAS referring for high and low note horns (660 Hz and 370 Hz), the frequency of the separately sounded note and sound pressure levels according to the standard EN 15153-2:2013.

4.11.1.4 Service reliability aspects

Assuming positive tests of the horns, it can be assumed, that acoustic warning system is enough, and in proper way to operate the train safely.

From timing perspective, the tests of subsystem can be executed:

- At every start-up (powering up of the train) – before the mission,
- As continuous monitoring – the whole time during the mission.
- In fixed periods:
  - regularly – e.g. latest after 24 hours
  - during maintenance in depo – e.g. every 3 months,

4.11.1.5 Test scheduling

The tests during start-up, usually before a train is leaving the depot in the manual tests must be performed. Actual trains are already supporting the continuous monitoring of the horn power supply. The driver still must perform manual tests.

In case of failures that do not allow safe operation, the operator timely decide to enable or not mission with this locomotive.

4.11.2 Impacts of transition to GoA3/4

The TCMS will in future take over the tasks which were formerly performed today by the driver, to allow GoA3/4 mode operation for the train.

The way how the tests will be executed, and the reporting of the outcome will change. Today the horns are checked by hearing or when the HW monitoring detects issues, an appropriate message on the HMI informs is shown to the driver, with the failure codes and possible remedy text. In GoA3/4 mode the driver will be not physically available (at least not locally), so acoustic information collected by driver should be replaced by e.g. on-board microphones, and the diagnostics information from the TCMS must be provided / accessible for remote monitoring/controlling center.

4.11.3 GoA3/4 Tests at the start of the mission rationale

To allow GoA3/4 tests the train driver and external maintenance staff sensing must be replaced by additional sensors – at least with microphone which can placed inside the cab also. This supports detection of horn functionality thus the acoustic warning – either by TCMS and/or by virtual driver.

4.11.4 Use cases definition

4.11.4.1 UC-HN1 Testing of horns HW part availability

Use Case	Testing horns HW part availability
ID	HN1
Actor	Virtual Driver
Goal	G_HN1: Make sure horns HW are available within technical specifications.
Safety relation	Acoustic warning system is safety relevant.
Precondition	Electric power supply available
Flow of events	1. Occupy train 2. Activate horns 3. Check air and power supply for horns is provided 4. Check for possible detected HW failure (monitoring for horn magnet valve) 5. Repeat 2...5 on another end of train
Post condition	Inform the TCMS/Virtual Driver whether the horn is power supplied and HW is working in defined limits.
Things that can go wrong	HW failure, power supply not provided – e.g. MiCB switched unintentionally OFF.
Already implemented risk reduction measures	Monitoring of horn air and power supply is available.
Observations	Test is done as continuous monitoring.

Table 47 –Testing horns HW part availability

4.11.4.2 UC-HN2 Testing of horns function

Use Case	Testing horns function
ID	HN2
Actor	Virtual Driver
Goal	G_HN2: Make sure horns functions according requirements.
Safety relation	Acoustic warning system is safety relevant.
Precondition	Electric power supply available
Flow of events	1. Occupy train 2. Activate horns 3. Check air and power supply for horns is provided 4. Check for possible detected HW failure (monitoring for the horn air and electrical supply) 5. Repeat 2...5 on another end of train
Post condition	Inform the TCMS/Virtual Driver whether horns are air and electrically supplied and are functionally OK.
Things that can go wrong	Horn function degraded by mechanical impact from pollution like dust, collision with bird etc.
Already implemented risk reduction measures	Monitoring of horn air and electrical power supply is available.
Observations	Test is done before start of mission.

Table 48 –Testing horns function

4.12 COMMUNICATION BETWEEN TRAIN AND GROUND

4.12.1 State of art

4.12.1.1 Architectural principles

This section considers the Adaptable Communication System (ACS) as the Train-to-ground (T2G) communication system to link the On Board and the On Track infrastructure and services as a system that follows the Europe's Rail Innovation Programme 2 (IP2) developments for a unique T2G communication system. This system communicates the Train with the On-Track Infrastructure independently of the user requirements. Moreover, it selects and monitor the bearers of communications/configuration ensuring backward compatibility and resiliency.

The ACS, and its equivalent pair equipped into the On Track facilities, includes different communication technologies (3GPP and/or owner vehicle to infrastructure (V2I) solutions) that provide different performance following a security profile (IEC 62443-4). This performance is measures using KPIs that leads to their selection.

The following figure shows the overall scheme, aligned with the Task 3.1 architecture defined (GAR and MAR):

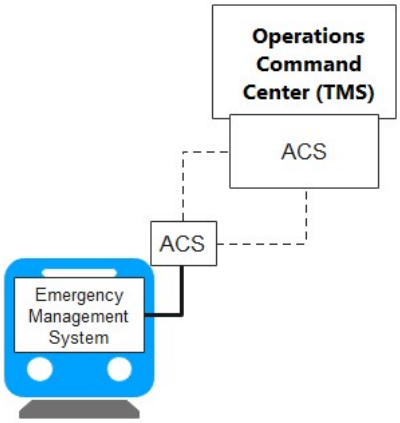

Figure 10: Comunications architecture

Aligned with the EN15380-2 that stablish the need (Group J subgroup E):

- Radio control equipment.
- Remote radio control equipment.
- Train to ground transmission equipment.

Train System

- ACS
- Operations Command Center (TMS)
- Maintenance Command Post (MMS) on board (see if it is from IM (Infrastructure Manager) or RU (Railway Undertaking))
- Emergency Management System (from the Infrastructure Manager (IM))

Actors

- Driver

4.12.1.2 Sub-Functions

The “Automatic Train Operation” function is realized in GoA2 train by the implementation of the here below sub-functions:

- Continuous or punctual communication, with session establishment or by packets.
- Communication of the status of all systems on a regular basis or only those with incidents. Alternatively, mixed, at long regular intervals and by events in case of system failure.
- Define the need or not of communication with safety requirements (guaranteed, with detection of communication failure and possible security reaction in case of non-recoverable failure) or security requirements (encrypted).
- Bandwidth requirements and transmission technology (e.g. radio for mobile communications, etc.).
- Point-to-point or point-to-multipoint.

4.12.1.3 Safety requirement

The communication train to ground currently follows the following points aligned with the CENELEC 50159:

- Cyclic communication of subsystem status (operation, maintenance)
- Subsystem failure communication (operation, maintenance)
- Decisions from the ground on how to continue with the mission in case of serious failure.

These points are aligned with the requirements extracted from the EN15380 – 4 group H, K that states the following points.

- Send diagnosis and condition data to ground.
- Ensure management of the communication train to ground and ground to train.
- Send voice, data to ground and to the train.
- Report information to the train personnel and passengers.

4.12.1.4 Mission reliability impacts

As it is mentioned in the architectural principles, 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 the On Board certified devices (CENELEC 50129) from the hardware perspective and regarding the software perspective it is mentioned above and those are required both for GoA2 to GoA4.

4.12.1.5 Test at the start of the mission rationale

The main failure that occur in the communication system at the begging of the mission is independent of the grade of automation. The key failure is the lack of coverage between both On Track and On Board sections; therefore, an initial test must be done to ensure the communication. Therefore, the

main objective of the tests is the monitoring of the communication bearers that the safety subsystems will required. It is remarked that these communication bearers are agnostics to the need of the safety subsystems as the ACS is a communication commodity.

4.12.2 Impacts of transition to GoA3/4

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).

4.12.3 GoA3/4 Tests at the start of the mission rationale

The following tests are defined:

- Test minimum bearers to provide communication services to every required GoA3/4 systems.
- Communication status to the On Board and On Track systems.
- Ground communications with train crew.
- Communications to passengers from the ground in case of need to inform on how to manage the emergency.
- Communication of safety alarm due to failure in any subsystem. Need for action (evacuation, rescue, etc.) (Operation, maintenance).
-

4.12.4 Use cases definition

A train-to-ground communication must be defined to communicate the status of the on-board equipment/subsystems. The status of such equipment is obtained from the tests defined in the previous chapters. This communication is independent of the communication between the track and train subsystems of each subsystem (e.g. ATP_TS and ATP_OB or ATO_TS and ATO_OB).

Use Case	Minimum bearers available
ID	12X1
Actor	GoA 1/2: Driver, GoA 3/4: Virtual driver
Goal	G_12X1: Ensure that the GoA3/4 systems will run with minimum communication capabilities available.
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	The use case is not safety related. The safety resides in the failed subsystem, which if not recoverable, will have its own fail-safe safeguards to prevent unsafe movement of the train with the failed system.
Flow of events	1. Ensure local communication between the GoA3/4 systems and their ACS and equivalents. 2. Measure KPIs and check channels selected by the OBU and equivalents.
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 subsystems affected.
Already implemented risk reduction measures	
Observations	

Table 49: Communication capabilities Train to Ground

4.13.1 State of art

4.13.1.1 Architectural principles (ATO over ETCS subset 125)

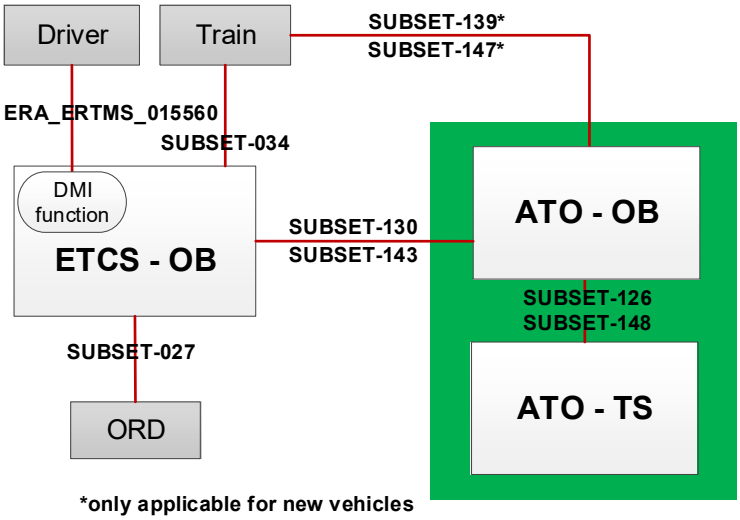

Figure 11: ATO architecture

This document takes into consideration ATO over ETCS as described in subset 125. The following architectural description is given as an illustrative indication. Refer to subset 125 for complete and up to date information.

The systems and scenario actors for GoA2 train involved by the function “Automatic Train Operation” can be:

Train systems:

- TCMS
- Radio communication modem,
- ETCS

Actors

- Driver,
- Train operator,
- ATO Trackside
- Maintenance people

4.13.1.2 Sub-functions of “Automatic Train Operation” function

“Automatic Train Operation” function is realized in GoA2 train by the implementation of the here below sub-functions:

Read odometry data

Read ETCS data

Read trackside data

Compute optimal speed profile

Manage dwell time

Apply traction and brake commands

Give feedback to the driver

The commands of the sub-functions may be implemented by redundant command path for reliability reason (the continuity of the transmission of the commands is guaranteed also in case of single failure)

4.13.1.3 Safety requirements

In GoA2 trains, “Automatic Train Operation” is not required to meet safety standards as it runs under the supervision of the “Automatic Train Protection” system. However, safety and integrity system design principles may be applied by suppliers in order to guarantee proper execution of system functions.

4.13.1.4 Mission reliability impacts

To maintain low the risk of service outage, the systems are normally designed following fails safe design solution, which can have relevant impact on the reliability of the train (safe state normally means train stopping or traction cut-off). To reduce as much as possible above impact, redundancies are often implemented to be resistant to single failures.

4.13.1.5 Test at the start of the service mission rationale

In not autonomous train there is already the possibility to introduce supplier specific tests before going into service operation.

Below the typical scenario of ATO test in GoA1/2 trains

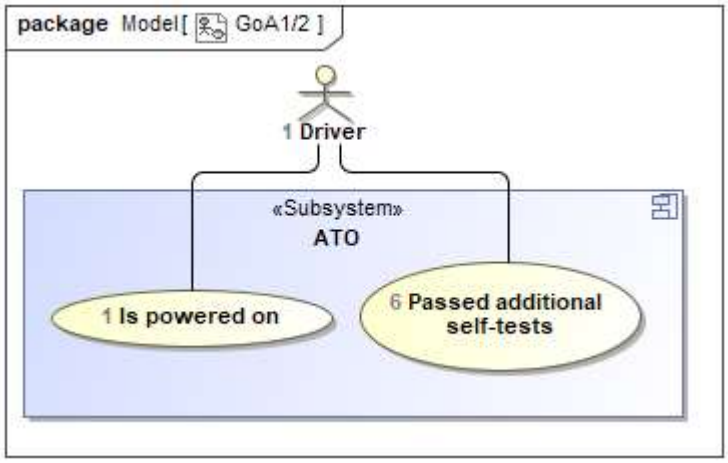

Figure 12: ATO test scenario

4.13.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 still need to be performed in GoA3/4. In addition, visual tests and actions performed by the driver during switch on must be automated in the case of the autonomous train. That is, has functional (correctly working) connectivity to all connected systems and is able e.g to read necessary information as well as actuate on the traction and braking system.

4.13.3 GoA3/4 Tests at the start of the mission rationale

In addition, all the tasks performed by the driver during service in GoA2 like making sure the track is clear of obstacles need to be done either by ATO or ATP. This implies new equipment connected to ATO which shall be tested before entering into service. In this analysis, it is assumed that ATP will remain responsible of operation safety. Thus, ATO is not to be considered safety critical but may nevertheless implement some new functions/interfaces based on new proposed GoA4 system architecture.

4.13.4 Testing "Automatic Train Operation (2.4 ATO)" Use cases

All the following use cases are related only to ATO system tests performed on a GoA3/4 train..

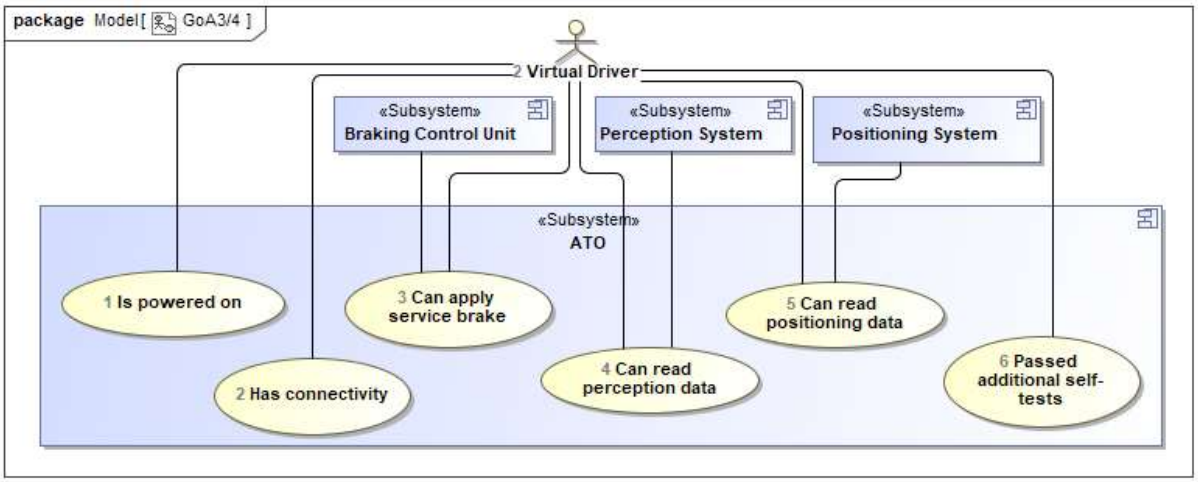

Figure 13: Use case of Function "Testing Automatic Train Operation"

Use Case	Testing of Is powered on
ID	ATO1
Actor	GoA 1/2: Driver, GoA 3/4: Virtual driver
Goal	G_ATO1: Make sure ATO receives electrical power
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	Train has power
Flow of events	1. ATO is powered on (electrically or by software execution) 2. The presence of a signal indicating ATO is in configuration mode is received
Post condition	An indication (GoA1/2: DMI icon, GoA3/4: signal) is received indicating ATO is in configuration mode
Things that can go wrong	ATO doesn't power on
Already implemented risk reduction measures	
Observations	

Table 50: Testing of Is powered on

Use Case	Testing of passed additional self-tests
ID	ATO6
Actor	GoA 1/2: Driver, GoA 3/4: Virtual driver
Goal	G_ATO6: Make sure all additional supplier specific tests passed
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	ATO is powered on
Flow of events	1. ATO self-tests are performed
Post condition	ATO is not in Failure mode
Things that can go wrong	Any test doesn't pass
Already implemented risk reduction measures	
Observations	

Table 51: Testing of passed additional self tests

Use Case	Testing of has connectivity
ID	ATO2
Actor	Virtual driver
Goal	G_ATO2: Check ATO is connected to the required networks and buses and receives data from the other systems.
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	ATO is powered on
Flow of events	1. ATO connects to the networks and busses 2. ATO receives data from the other systems
Post condition	A signal is received indicating ATO connectivity is up.
Things that can go wrong	Any connection is down
Already implemented risk reduction measures	
Observations	

Table 52: Testing of has connectivity

Use Case	Testing of can apply traction and service brake
ID	ATO3
Actor	Virtual driver
Goal	G_ATO3: Check ATO can command traction and service brake and get proper feedback.
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	ATO has connectivity
Flow of events	1. ATO receives braking capacity information 2. ATO receives traction capacity information
Post condition	Traction and service brake capacity is available
Things that can go wrong	No traction or service brake is available
Already implemented risk reduction measures	
Observations	

Table 53: Testing of can apply service brake

Use Case	Testing of can read data from other GoA4 specific systems
ID	ATO4
Actor	Virtual driver
Goal	G_ATO4: Check ATO is able to read data from other GoA4 specific systems.
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	ATO has connectivity
Flow of events	1. ATO reads data without error
Post condition	Some information is received
Things that can go wrong	No data is available from one of the required systems
Already implemented risk reduction measures	
Observations	

Table 54: Testing of can read data from other GoA4 specific systems

Use Case	Testing of can read positioning
ID	ATO5
Actor	Virtual driver
Goal	G_ATO5: Check ATO can read positioning data.
Safety relation	The use case is not safety relevant since automatic train operation is performed under ATP supervision
Precondition	ATO has connectivity
Flow of events	1. ATO reads positioning data without error
Post condition	ATO receives positioning information
Things that can go wrong	ATO is not able to locate in its journey and is not available.
Already implemented risk reduction measures	
Observations	

Table 55: Testing of can read positioning

4.14.1 State of art

4.14.1.1 Architectural principles (ETCS)

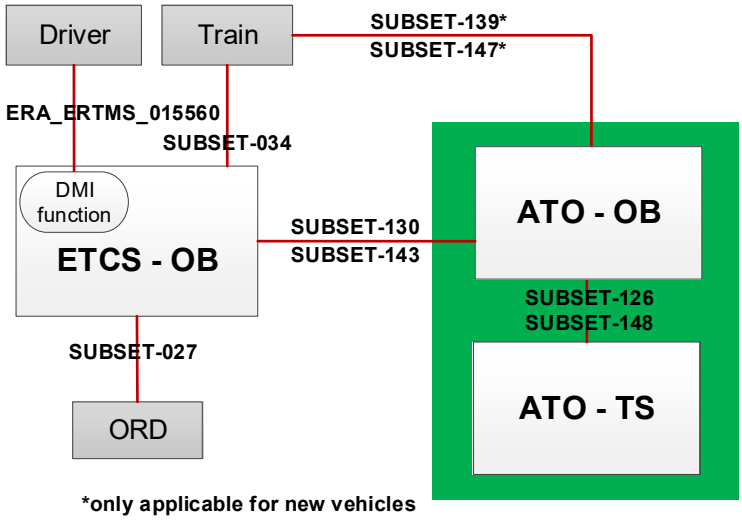

Figure 14: ATP architecture

This document takes into consideration the ETCS ATP as described in 026, 036, 040 and 041 subsets. The following architectural description is given as an illustrative indication. Refer to aforementioned subsets for complete and up to date information.

The systems and scenario actors for GoA1/2 train involved by the function “Automatic Train Protection” can be:

Train systems:

- Service brake,
- Emergency brake,
- Radio communication modem,
- Balise Transmission Module (BTM),
- Odometry source

Actors

- Driver,
- Train operator,
- Ground Signalling System
- Maintenance people

4.14.1.2 Sub-functions of “Automatic Train Protection” function

“Automatic Train Protection” function is realized in not autonomous train by the implementation of the here below sub-functions:

Read odometry data

Read balise data

Read trackside data

Compute most restrictive speed profile

Apply service brake

Apply emergency brake

The commands of the sub-functions are implemented by redundant command path for reliability reason (the continuity of the transmission of the commands is guaranteed also in case of single failure) or safety reason.

The architecture of ATP is fail safe, to guarantee that the risk are maintained at an acceptable level and redundant to guarantee the availability (single failure resistant).

4.14.1.3 Safety requirements

ATP function is essential to safety.

The following failure cases are considered:

1. Radio communication failure
2. Service brake application failure
3. Emergency brake application failure
4. Loss of information

The above failure scenario remains the reference also for GoA3/4.

4.14.1.4 Mission reliability impacts

To maintain low the above risk, the systems are normally designed following fails safe design solution, which can have relevant impact on the reliability of the train (safe state normally means train stopping or traction cut-off). To reduce as much as possible above impact, redundancies are often implemented to be resistant to single failures.

4.14.1.5 Test at the start of the mission rationale

In not autonomous train there is already the possibility to introduce supplier specific tests before going into service operation.

Below the typical scenario of ATP test in GoA1/2 trains

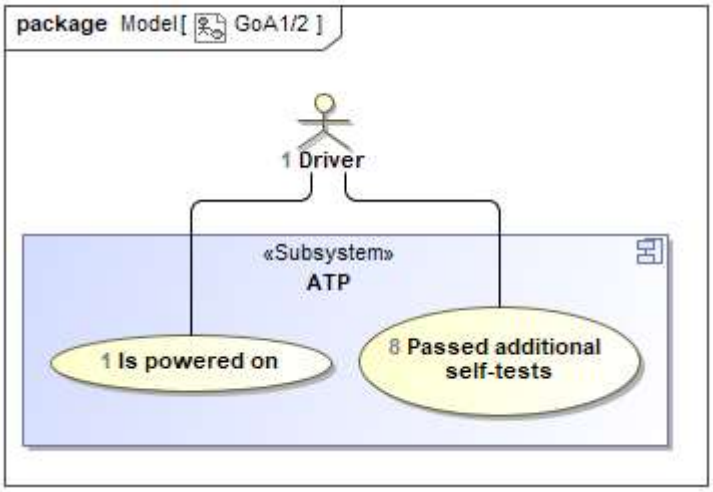

Figure 15: ATP test scenario

4.14.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 still need to be performed in GoA3/4. In addition, visual tests and actions performed by the driver during switch on must be automated in the case of the autonomous train.

4.14.3 GoA3/4 Tests at the start of the mission rationale

The actions to be automated in GoA3/4 start of mission include :

- Driver ID introduction which shall be removed in the absence of driver
- Train Running Number shall be received automatically from ground control
- Set/Remove virtual balise cover action
- ETCS Level management (especially a level allowing autonomous operation must be available)
- Radio network ID and RBC ID or phone number must be received automatically
- Shunting, Not Leading or Train Data Entry mode management must be automated
- Train data must be received from other subsystems such as braking system for braking capacity, …
- Correct supervision mode availability must be checked
- It must be checked that train is not rejected

In addition, it is assumed that ATP will remain responsible to supervise ATO operation. Thus, ATP is expected to read perception data and actuate for example in case of obstacle detection.

4.14.4 Testing "Automatic Train Protection (2.5 ATP)" Use cases

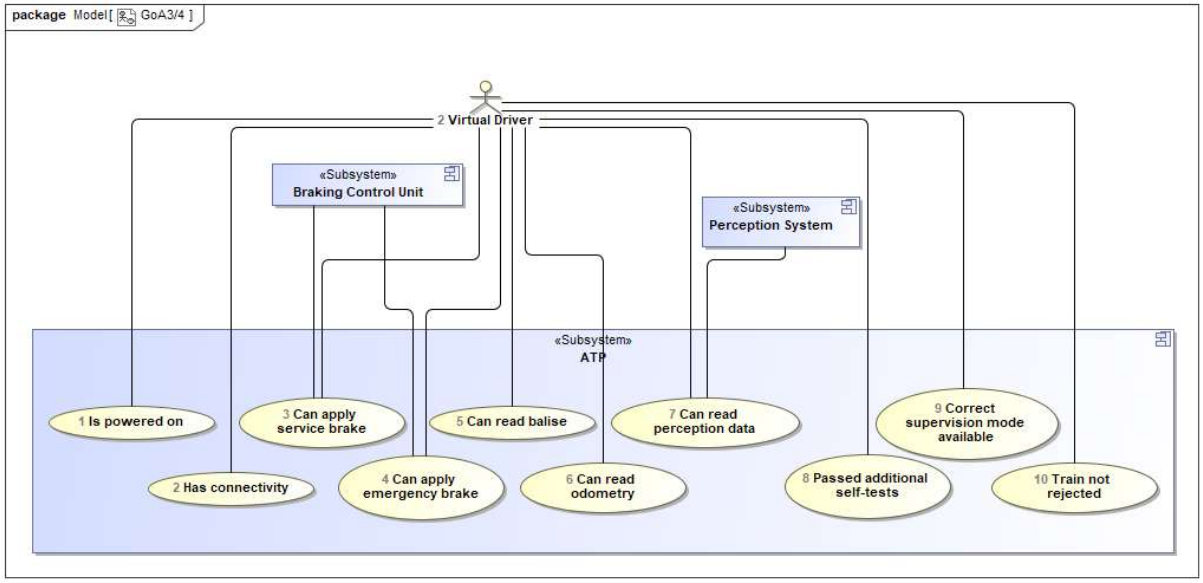

Figure 16: Use case of Function "Testing Automatic Train Protection"

Use Case	Testing of Is powered on
ID	ATP1
Actor	GoA 1/2: Driver, GoA 3/4: Virtual driver
Goal	G_ATP1: Make sure ATP receives electrical power
Safety relation	The use case is safety relevant with relation to the hazards related to automatic train protection, which shall be mitigated by proper sub-function like visual and audible alert for people present in the area
Precondition	Train has power
Flow of events	1. The relay to power on ATP is closed 1. The presence of a signal indicating ATP is UP is received
Post condition	An indication (GoA1/2: DMI icon, GoA3/4: signal) is received indicating ATP is UP
Things that can go wrong	ATP doesn't power on
Already implemented risk reduction measures	Test done in a moment when train has not maintenance activities
Observations	

Table 56: Testing of Is powered on

Use Case	Testing of has connectivity
ID	ATP2
Actor	Virtual driver
Goal	G_ATP2: Check ATP is connected to the required networks and buses.
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP is powered on
Flow of events	1. ATP connects to the networks and busses
Post condition	A signal is received indicating ATP connectivity is up.
Things that can go wrong	Any connection is down
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 57: Testing of has connectivity

Use Case	Testing of can apply service brake
ID	ATP3
Actor	Virtual driver
Goal	G_ATP3: Check ATP can command SB and get proper feedback.
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP has connectivity
Flow of events	1. ATP commands service brake 2. ATP receives a feedback of service brake application
Post condition	A signal indicating service brake application is received
Things that can go wrong	No service brake is applied
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 58: Testing of can apply service brake

Use Case	Testing of can apply emergency brake
ID	ATP4
Actor	Virtual driver
Goal	G_ATP4: Check ATP can command EB and get proper feedback.
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP has connectivity
Flow of events	1. ATP commands emergency brake 2. ATP receives a feedback of emergency brake application
Post condition	A signal indicating emergency brake application is received
Things that can go wrong	No emergency brake is applied
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 59: Testing of can apply emergency brake

Use Case	Testing of can read balise
ID	ATP5
Actor	Virtual driver
Goal	G_ATP5: Check ATP can read a balise.
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP is powered on
Flow of events	1. Antenna is in a working state
Post condition	Balise information is read
Things that can go wrong	No balise information is received
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 60: Testing of can read balise

Use Case	Testing of can read odometry
ID	ATP6
Actor	Virtual driver
Goal	G_ATP6: Check odometry sources are available.
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP is powered on
Flow of events	1. Tachometers are in a working state
Post condition	Odometry information changes
Things that can go wrong	No odometry information is available
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 61: Testing of can read odometry

Use Case	Testing of can read perception data
ID	ATP7
Actor	Virtual driver
Goal	G_ATP7: Make sure all additional supplier specific tests passed
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP is powered on
Flow of events	1. Perception data is read
Post condition	Perception data is available
Things that can go wrong	No perception data is available
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 62: Testing of can read perception data

Use Case	Testing of passed additional self-tests
ID	ATP8
Actor	GoA 1/2: Driver, GoA 3/4: Virtual driver
Goal	G_ATP8: Make sure all additional supplier specific tests passed
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	ATP is powered on
Flow of events	1. ATP self-tests are performed
Post condition	ATP is not in system failure mode
Things that can go wrong	Any test doesn't pass
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 63: Testing of passed additional self tests

Use Case	Testing of passed correct supervision mode available
ID	ATP9
Actor	Virtual driver
Goal	G_ATP9: Make sure autonomous operation is possible
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	No supervision mode information processed
Flow of events	1. Available supervision mode is processed
Post condition	A supervision mode allowing autonomous operation is available
Things that can go wrong	Available supervision modes don't allow autonomous driving
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 64: Testing of correct supervision mode available

Use Case	Testing of train not rejected
ID	ATP10
Actor	Virtual driver
Goal	G_ATP10: Check the received TRN is valid
Safety relation	The use case is safety relevant with relation proper automatic train protection
Precondition	No TRN is set
Flow of events	1. TRN is set
Post condition	Train is accepted on the network
Things that can go wrong	TRN is rejected
Already implemented risk reduction measures	Move ATP to a safe state
Observations	

Table 65: Testing of train not rejected

4.15.1 State of art

4.15.1.1 Architectural principles

In GoA1/2 specification, there is no subsystem dedicated to positioning. ETCS acquires positioning data from balises and tachometers and transmits the information to ATO as specified by subset 125 and subset 130. Existing systems and scenario actors which could be involved in an independent system dedicated to the function “Positioning” are:

Train systems:

- GPS,
- Radio communication modem,
- Balise Transmission Module (BTM),
- Odometry source
- RaDAR/LiDAR
- Computer vision system

Actors

- Driver,
- Train operator,
- Ground Signalling System
- Maintenance people

4.15.1.2 Sub-functions of “Positioning” function

Positioning function is realized in not autonomous train by the implementation of the here below sub-functions:

Read sensor data

Combine sensor data into a position

Publish position information

The sensors and processing units of the sub-functions may be implemented by redundant hardware for reliability reason (the continuity of the transmission of the position information is guaranteed also in case of single failure)

4.15.1.3 Safety requirements

Some of the sensors used for positioning may be used for safety related functions. Safety equipment implementing those functions generally have direct access to those sensors to guarantee the integrity of the information. Thus, an independent positioning system in its globality may not be considered as safety related.

4.15.1.4 Mission reliability impacts

To reduce as much as possible positioning information outage, **redundancies** are often implemented to be resistant to single failures or **degraded condition** can be implemented in sensor data processing to continue providing location information albeit with a lesser precision.

Degraded condition can be compatible with the service as long as the provided information meets the precision criteria for safe operation.

4.15.1.5 Test at the start of the service rationale

In not autonomous train, having no independent subsystem dedicated to positioning, there are no functional tests of positioning before going into service operation. The presence of a driver coupled to ETCS and possibly ATO are usually sufficient to allow proper operation of the train.

4.15.2 Impacts of transition to GoA3/4

In the absence of existing independent positioning system in GoA1/2 specification, the following is an attempt to describe what tests would be needed by such a system.

4.15.3 Tests at the start of the service rationale

While failing to read some sensor data may still allow for proper operation in GoA3/4, accurate enough positioning information is mandatory in the absence of a driver. Thus, positioning system shall estimate the position precision while processing available sensor data in order to be able to determine if proper train operation is still possible. Contrary to GoA1/2, in the absence of accurate enough position information, the train will not be able to enter or continue service.

The requirement to have position information to be able to give service mandates for positioning system tests at the start of the service.

4.15.4 “Testing Positioning " Use cases

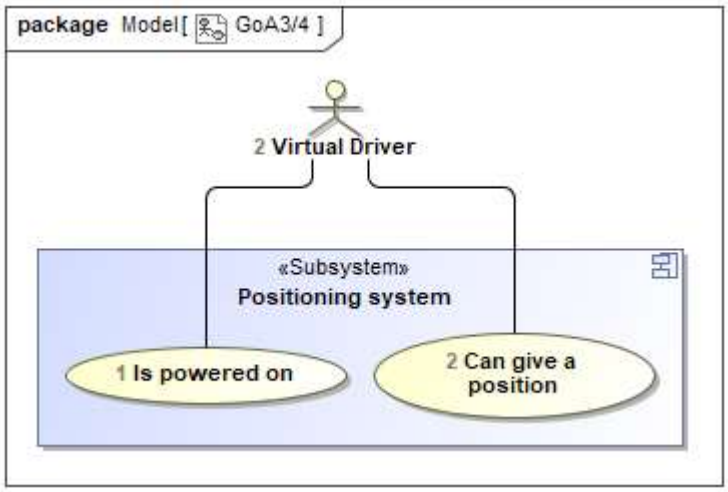

Figure 17: Use case of Function “Testing Positioning”

Use Case	Testing of Is powered on
ID	POS1
Actor	Virtual driver
Goal	G_POS1: Make sure positioning system receives electrical power
Safety relation	The use case is safety relevant with relation to the hazards related to positioning, which shall be mitigated by proper sub-function like visual and audible alert for people present in the area
Precondition	Train has power
Flow of events	15. The relay to power on the positioning system is closed 16. The presence of a signal indicating positioning system is UP is received
Post condition	An indication (GoA1/2: DMI icon, GoA3/4: signal) is received indicating positioning system is UP
Things that can go wrong	Positioning system doesn't power on
Already implemented risk reduction measures	Test done in a moment when train has not maintenance activities
Observations	

Table 66: Testing of Is powered on

Use Case	Testing of can give a position
ID	POS2
Actor	Virtual driver
Goal	G_POS2: Make sure the positioning system is able to give a position to other equipment
Safety relation	The use case is safety relevant with relation to the hazards related to positioning, which shall be mitigated by proper sub-function like visual and audible alert for people present in the area
Precondition	Positioning system is powered on
Flow of events	2. Positioning information is read
Post condition	Position information is available (and accurate)
Things that can go wrong	No position is available
Already implemented risk reduction measures	
Observations	The internal tests of the dedicated positioning system being black box and supplier specific, the virtual driver has no visibility on which sensors are used or other implementation details.

Table 67: Testing of can give position

4.16.1 State of art

Today the task of the perception system for the train and the corresponding implementation of the perception is mainly the responsibility of the driver.

4.16.1.1 Architectural principles (Actors and systems involved)

GoA 0: The train drives without an assistance systems in the driver-controlled operation. The driver controls the train at sight, stationary light signals controls the train operation.

The driver (corresponds actor) has different tasks during the mission, e. g. observe the track, read and implement the stationary light signals, read and implement the kilometer and information boards, detect obstacles on the track or inside the clearance profile. The observations of the driver result in measures that are carried out by the driver, e. g. adjustment of the train speed (e.g. slow speed section), emergency braking, appropriate reaction to obstacles, entry / exit to the station.

GoA 1/2: The driver drives and brakes manually the train. A train control system monitors continuously the speed of the train.

4.16.1.2 Sub-functions

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 center communication	
K	D	C	a	F	send train position to control center	
K	E				provide automatic train control (ATC)	

K	E	B			provide automatic train protection (ATP)	
K	E	C			provide automatic driving mode (ATO)	
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.					

4.16.1.3 Safety requirements

The detection distance and the reaction time of the driver has a relevant impact on the safety of the operation. The detection distance and the reaction time are dependent from the day time (light / dark), the environmental conditions (rain, fog, snow fall) and the healthy condition of the driver. The driver must note the light signals or must react on obstacles to prevent collisions with another train or the obstacle.

4.16.1.4 Service reliability aspects

The mission reliability is dependent from the driver, a failure of the driver is corresponding to the failure of the operation.

The driver noted information in the drivers log book, e. g. "button on control panel pressed and not working", which are used for the maintenance work after the mission.

4.16.1.5 Test at the start of the mission rationale

The driver tests the following already existing perception systems at the start of the mission:

- Passenger room monitoring
- Door cameras
- Rear view camera

4.16.2 Impacts of transition to GoA3/4

A perception system for the cab view of the driver will be implemented in the autonomous train for the transition to GoA 3/4.

The perception system consists of …

- radar, LiDAR and camera sensors,
- receiver for the Global Navigation Satellite System (GNSS),
- digital map.

The radar, LiDAR and camera sensors replaces the observations of the driver and 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 radar, LiDAR and camera sensors at the ends of the train detect the environment in short-, medium- and long-distance ranges. The detection by the sensors is working less dependent from the weather conditions. This relates to the comparison between the perception of the driver and the sensors which have advantages in specific weather conditions, e. g. specific LiDAR sensors can be detect mist itself and the objects behind it.

Furthermore the autonomous train has a connection to the Global Navigation Satellite System (GNSS). The sensor data will be synchronized with the data from the Global Navigation Satellite System (GNSS) and the digital map to orientate at the infrastructure (bridges, signal mast, etc.). Based on these data the position of the train is defined anytime. The digital map will be actualised permanently by the sensor data and so that the digital map will be to a digital twin of the track and the immediate surroundings.

At the start of the mission the digital map has the current state about the presence and the position of the railway infrastructure (catenary masts, signal masts, kilometer boards, bridges, buildings along the track, etc.). During the mission the perception system observes the track and the railway infrastructure and compares the observations with the digital map. When the perception system detects a deviation the deviation will be noted in the digital map, if necessary sent to the control center.

These information will be exchanged between the trains also on the track so that the perception systems of these trains can match the possible deviation. The deviation can be verified as true if further perception systems detects also the deviation. Otherwise the detection of the deviation is a single event and the sensors of the train concerned should be checked by a service technician after the mission.

The perception system is embedded into the train monitoring and diagnostic system.

A new solution is required to perform the test of the perception system. The test of the perception system for the autonomous train will be triggered via command by the control center (alternatively by the virtual driver). The test itself will be still performed on the autonomous train. If necessary the control center or the virtual driver can monitor the test to react early on diagnostic messages.

Alternatively the virtual driver in the control center can perform the tests of the perception system.

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

The safety requirement is that the components and the complete perception system will be tested at the start of the mission to guarantee the complete functionality. The operation of the autonomous train may not start if one or several of the components of the perception system has a failure. Neither the environment will capture completely nor the perception / observation can be implemented in an action.

4.16.3 GoA3/4 Tests at the start of the mission rationale

The perception system (for the cab view of the driver) must be checked at each start-up of the train and must be monitored continuously during the operation of the train because the perception system is the basic requirement for the autonomous operation and thus safety relevant. Also the periodic check in fixed maintenance intervals is required.

The following tests should be performed at the start-up of the train:

- Power supply of the sensor (radar, LiDAR, camera) available
- Signal of the sensor (radar, LiDAR, camera) available
- Plausibility check of the sensor signal (radar, LiDAR, camera)
- Plausibility check of the GNSS signal
- Real-time connection to the control center available

The tests for the autonomous execution must be defined completely new because the tasks of the driver at GoA 0/1/2 will transferred to the perception system at GoA 3/4.

Initially the availability and the function of each single component (radar, LiDAR, camera, receiver for GNSS, digital map) for the perception system should be checked automated for itself.

The functionality of the radar, LiDAR and camera sensors will be tested in which landmarks, stationary light signals, kilometer and information boards from the sensor. The plausibility of the received sensor signal will be checked based on the data from the digital map. A contamination or a misalignment of the sensor leads to a disturbed detection.

After the check of the single components the complete perception system (as fusion of all components) will be checked.

The control center / virtual driver should be informed about the result and the diagnostic messages of automated test if necessary to send out a service technician.

The operative condition, permanent diagnosis and periodical maintenance test are required for the mission. The autonomous train is without the perception system not compliant with the safety requirements and a real driver must take over the task.

4.16.4 Use cases definition

The use cases PST1 to PST7 describes the testing (before the start), the permanent monitoring (during the mission) and the periodic testing (during maintenance) for the radar, LiDAR and camera sensors. There will be not divided between the sensors of the respective systems radar, LiDAR and camera. For a better allocation in the train infrastructure the sensors are named with the addition RAD/LID/CAM-sensor.

The use cases PST2, PST4, PST6, PST11 and PST14 were listed to emphasize the importance of the monitoring and checks (sensor, GNSS signal, etc.) during the mission of the autonomous train.

compliant

Use Case	Testing of RAD/LID/CAM-sensors availability
ID	PST1
Actor	Virtual Driver
Goal	G_PST1: Make sure RAD/LID/CAM-sensors are available within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train by control center or virtual driver 2. Select RAD/LID/CAM-sensor ON 3. Check power supply for sensor is provided 4. Check for possible detected sensor failure 5. Repeat step 2. to 4. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor is power supplied and is working in defined current and voltage limits.
Things that can go wrong	Sensor faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 68: Testing of RAD/LID/CAM-sensors availability

Use Case	Monitoring of RAD/LID/CAM-sensors availability
ID	PST2
Actor	Virtual Driver
Goal	G_PST2: Make sure RAD/LID/CAM-sensors are available within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available (Test PST1 is done) - Train is in mission.
Flow of events	1. Check RAD/LID/CAM-sensor ON 2. Check power supply for sensor is provided 3. Check for possible detected sensor failure 4. Repeat step 1. to 3. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor is power supplied and is working in defined current and voltage limits.
Things that can go wrong	Sensor faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for sensor before start of each mission
Observations	Test is done as continuous monitoring.

Table 69: Monitoring of RAD/LID/CAM-sensors availability

Use Case	Testing of RAD/LID/CAM-sensors function
ID	PST3
Actor	Virtual Driver
Goal	G_PST3: Make sure RAD/LID/CAM-sensors are functioning
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available (Test PST1 is done) - Train is in standstill. Traction must be blocked.
Flow of events	1. Check RAD/LID/CAM-sensor ON 2. Check sensor signal is received 3. Check for possible detected sensor failure 4. Repeat step 1. to 3. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor signal is received.
Things that can go wrong	Sensor faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for sensor before start of each mission
Observations	Test is done before start of each mission.

Table 70: Testing of RAD/LID/CAM-sensors function

Use Case	Monitoring of RAD/LID/CAM-sensors function
ID	PST4
Actor	Virtual Driver
Goal	G_PST4: Make sure RAD/LID/CAM-sensors are functioning
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available (Test PST1 is done) - Train is in mission.
Flow of events	1. Check RAD/LID/CAM-sensor ON 2. Check sensor signal is received 3. Check for possible detected sensor failure 4. Repeat step 1. to 3. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor signal is received.
Things that can go wrong	Sensor faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for sensor before start of each mission - Testing of function for sensor before start of each mission
Observations	Test is done as continuous monitoring.

Table 71: monitoring of RAD/LID/CAM-sensors function

Use Case	Testing of RAD/LID/CAM-sensor signal plausibility
ID	PST5
Actor	Virtual Driver
Goal	G_PST5: Make sure RAD/LID/CAM-sensor signal is plausible within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available (Test PST1 is done) - RAD/LID/CAM-sensor signal is received (Test PST3 is done) - Train is in standstill. Traction must be blocked.
Flow of events	1. Check RAD/LID/CAM-sensor ON 2. Check power supply for sensor is provided 3. Check sensor signal is received 4. Focus sensor on a defined position (e. g. stationary light signal, kilometer board) 5. Adjust sensor detection with defined position 6. Check for possible detected sensor failure 7. Repeat step 1. to 6. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor is working in the specified range and the signal is 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 tests. - Testing of power supply for sensor before start of each mission - Testing of function for sensor before start of each mission
Observations	Test is done before start of each mission.

Table 72: Testing of RAD/LID/CAM-sensors signal plausibility

Use Case	Monitoring of RAD/LID/CAM-sensor signal plausibility
ID	PST6
Actor	Virtual Driver
Goal	G_PST6: Make sure sensor RAD/LID/CAM-signal is plausible within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available (Test PST1 is done) - RAD/LID/CAM-sensor signal is received (Test PST3 is done) - Train is in mission.
Flow of events	1. Check RAD/LID/CAM-sensor ON 2. Check power supply for sensor is provided 3. Check sensor signal is received 4. Focus sensor on a defined position (e. g. stationary light signal, kilometer board) 5. Adjust sensor detection with defined position 6. Check for possible detected sensor failure 7. Repeat step 1. to 6. for each RAD/LID/CAM-sensor
Post condition	Inform the TCMS / control center / virtual driver whether the RAD/LID/CAM-sensor is working in the specified range and the signal is 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 tests. - Testing of power supply for sensor before start of each mission - Testing of function for sensor before start of each mission
Observations	Test is done as continuous monitoring.

Table 73: Monitoring of RAD/LID/CAM-sensors signal plausibility

Use Case	Periodic testing of RAD/LID/CAM-sensors availability and function
ID	PST7
Actor	Maintenance staff
Goal	G_PST7: Make sure RAD/LID/CAM-sensors are available and functional within the technical specifications.
Safety relation	- Observation of the environment, track, clearance profile - RAD/LID/CAM-sensor signal is safety relevant
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train by control center or virtual driver 2. Select RAD/LID/CAM-sensor ON 3. Check power supply for sensor is provided 4. Check sensor signal is received 5. Check for possible detected sensor failure 6. Repeat step 2. to 5. for each RAD/LID/CAM-sensor
Post condition	Inform the service technician whether the RAD/LID/CAM-sensor is not working in defined current and voltage limits or the function is disturbed.
Things that can go wrong	Sensor faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done in fixed maintenance intervals.

Table 74: Periodic testing of RAD/LID/CAM-sensors availability and function

Use Case	Testing of digital map actuality
ID	PST8
Actor	Control center / Virtual Driver
Goal	G_PST8: Make sure digital map is actual (corresponds last status after end of last mission).
Safety relation	- Digital map is safety relevant (orientation at infrastructure)
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train by control center or virtual driver 2. Select vehicle control unit ON 3. Check power supply for vehicle control unit is provided 4. Check digital map is available 5. Check status of digital map and adjust with the last status
Post condition	Inform the TCMS / virtual driver whether the digital map is 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 tests.
Observations	Test is done before start of each mission.

Table 75: Testing of digital map actuality

Use Case	Testing of availability of GNSS receiver
ID	PST9
Actor	Virtual Driver
Goal	G_PST9: Make sure GNSS receiver is available
Safety relation	- Position of the train - Receiving of GNSS signal is safety relevant
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train by control center or virtual driver 2. Select GNSS receiver ON 3. Check power supply for GNSS receiver is provided 4. Check for possible detected receiver failure
Post condition	Inform the TCMS / control center / virtual driver whether the GNSS receiver is power supplied and is working in defined current and voltage limits.
Things that can go wrong	GNSS receiver faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 76: Testing of availability of GNSS receiver

Use Case	Testing of plausibility of GNSS signal
ID	PST10
Actor	Virtual Driver
Goal	G_PST10: Make sure GNSS signal is available and plausible with the last registered position of the train
Safety relation	- Position of the train - Receiving of GNSS signal is safety relevant
Precondition	- Electric power supply available (Test PST9 is done) - Train is in standstill. Traction must be blocked.
Flow of events	1. Check GNSS receiver ON 2. Check power supply for GNSS receiver is provided 3. Check for possible detected GNSS receiver failure 4. Adjust the current position of the train with the position of the received GNSS signal
Post condition	Inform the TCMS / control center / virtual driver whether the receiver is power supplied and the received GNSS signal is available.
Things that can go wrong	GNSS receiver faulty, GNSS signal not available, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for GNSS receiver before start of each mission
Observations	Test is done before start of each mission.

Table 77: Testing of plausibility of GNSS signal

Use Case	Monitoring of plausibility of GNSS signal
ID	PST11
Actor	Virtual Driver
Goal	G_PST11: Make sure GNSS signal is available and plausible with the current position of the train
Safety relation	- Position of the train - Receiving of GNSS signal is safety relevant
Precondition	- Electric power supply available (Test PST9 is done) - Train is in mission.
Flow of events	1. Check GNSS receiver ON 2. Check power supply for receiver is provided 3. Check for possible detected receiver failure 4. Adjust the current position of the train with the position of the received GNSS signal
Post condition	Inform the TCMS / control center / virtual driver whether the receiver is power supplied and the received GNSS signal is available.
Things that can go wrong	Receiver faulty, GNSS signal not available, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for receiver before start of each mission - Testing of plausibility of GNSS signal before start of each mission
Observations	Test is done as continuous monitoring.

Table 78: Monitoring of plausibility of GNSS signal

Use Case	Testing of real-time connection to control center
ID	PST12
Actor	Virtual Driver
Goal	G_PST12: Make sure real-time connection to control center is available
Safety relation	- Real-time connection to control center is safety relevant to take over the mission by virtual driver (redundancy)
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train by control center or virtual driver 2. Select transmitter-receiver module ON 3. Check power supply for transmitter-receiver module is provided 4. Check for possible detected failure of transmitter-receiver module 5. Check real-time connection to control center is available
Post condition	Inform the TCMS / control center / virtual driver whether transmitter-receiver module is available.
Things that can go wrong	Transmitter-receiver module faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 79: Testing of real-time connection to control center

Use Case	Monitoring of real-time connection to control center
ID	PST13
Actor	Virtual Driver
Goal	G_PST13: Make sure real-time connection to control center is available
Safety relation	- Real-time connection to control center is safety relevant to take over the mission by virtual driver (redundancy)
Precondition	- Electric power supply available (Test PST12 is done) - Train is in mission.
Flow of events	1. Check transmitter-receiver module ON 2. Check power supply for transmitter-receiver module is provided 3. Check real-time connection to control center is available 4. Check for possible detected failure of real-time connection
Post condition	Inform the TCMS / control center / virtual driver whether real-time connection to control center is available.
Things that can go wrong	Transmitter-receiver module faulty, real-time connection to control center disturbed, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of transmitter-receiver module and real-time connection to control center before start of each mission
Observations	Test is done as continuous monitoring.

Table 80: Monitoring of real-time connection to control center

Use Case	Check of head lamps of oncoming train
ID	PST14
Actor	Virtual Driver
Goal	G_PST14: Make sure all head lamps needed of oncoming train in operational area are visibly working.
Safety relation	Shown lamp pattern is safety relevant.
Precondition	- Electric power supply available (Tests PST1 to PST6 are done) - Train is in mission or in station.
Flow of events	1. Observe oncoming train in focus (from other passing train or station) 2. In case of deviation from expected inform control center 3. Control center informs train in focus
Post condition	Inform via control center the affected train.
Things that can go wrong	During mission one or more lights fail or got dirty.
Already implemented risk reduction measures	Operational rules defined for virtual driver, when, what deviation has to be reported.
Observations	This check should be done by each train on mission “seeing” other trains.

Table 81: Check of head lamps of oncoming train

4.17.1 State of Art

4.17.1.1 Architectural principles

The actors of the TCMS are the following ones (for GoA1/2 application, i.e. with a driver):

- CPU
- Remote Control Center
- Driver

The TCMS is mostly linked to the following subsystems:

- Brake,Door, ATO, ATP, Passenger Alarm, Fire Protection, Pantograph, Traction, Positioning, Air generation, internal and external lights, perception system, power supply and all auxiliaries that are needed to support the main functions of the locomotive or the train, such as fans, pumps, compressors, chargers, converters, radio and further communication means and automation technology and devices to support or enable automation of functions and also automation of mitigation actions like isolating drives, bogies, resetting fuses, etc.

4.17.1.2 Sub-Functions

The functions covered by the TCMS in EN15380-4 are the following ones:

- All control functions covered by function group H.

4.17.1.3 Safety requirement

TCMS tests are depending on EU interoperability requirements and CSM design targets for catastrophic or critical consequences..
It is recommended to develop the TCMS tests matching with Connecta`s safety target for the bus system in line with the targets above.

4.17.1.4 Mission reliability impacts

Special attention needs to be given to TCMS, brake and propulsion design that prevents stopping a train at a hazardous location not suitable for rescue, e. g. tunnels or bridges. Therefore EN 50553 (REQUIREMENTS FOR RUNNING CAPABILITY IN CASE OF FIRE ON BOARD OF ROLLING STOCK) shall be applied in addition.

4.17.1.5 Test at the start of the mission rationale

-Daily self test on power on (memory check)
-Permanent supervision of parameters (voltage, current, temperature, pressure...) and states (position of relays, valves)
-Permanent supervision of IP and MVB connection and I/O modules
-Sensors and microcontroller supervision.

4.17.2 Impacts of transition to GoA3/4

Tests performed in GoA1/2 may still need to be performed in GoA3/4, However TCMS will in future take over the tasks which were formerly performed by the driver.

4.17.3 GoA3/4 Tests at the start of the mission rationale

All the tasks performed by the driver during service in GoA1/2 need to be done either by ATO or TCMS.

Additional safety functions associated with shifting driver responsibilities to machine may result in an upgrade and extension of the ETCS telegrams or a third radio channel beyond ETCS and ATO

4.17.4 Use cases definition

- Powering up of the train, the TCMS is systematically tested.
- TCMS is periodically or continuously tested by the diagnostic functions implemented in TCMS. Technical diagnostics therefore can compensate nearly all dedicated tests, so additional testing effort in operation will approach 0.

The following tables summarize the test of the TCMS.

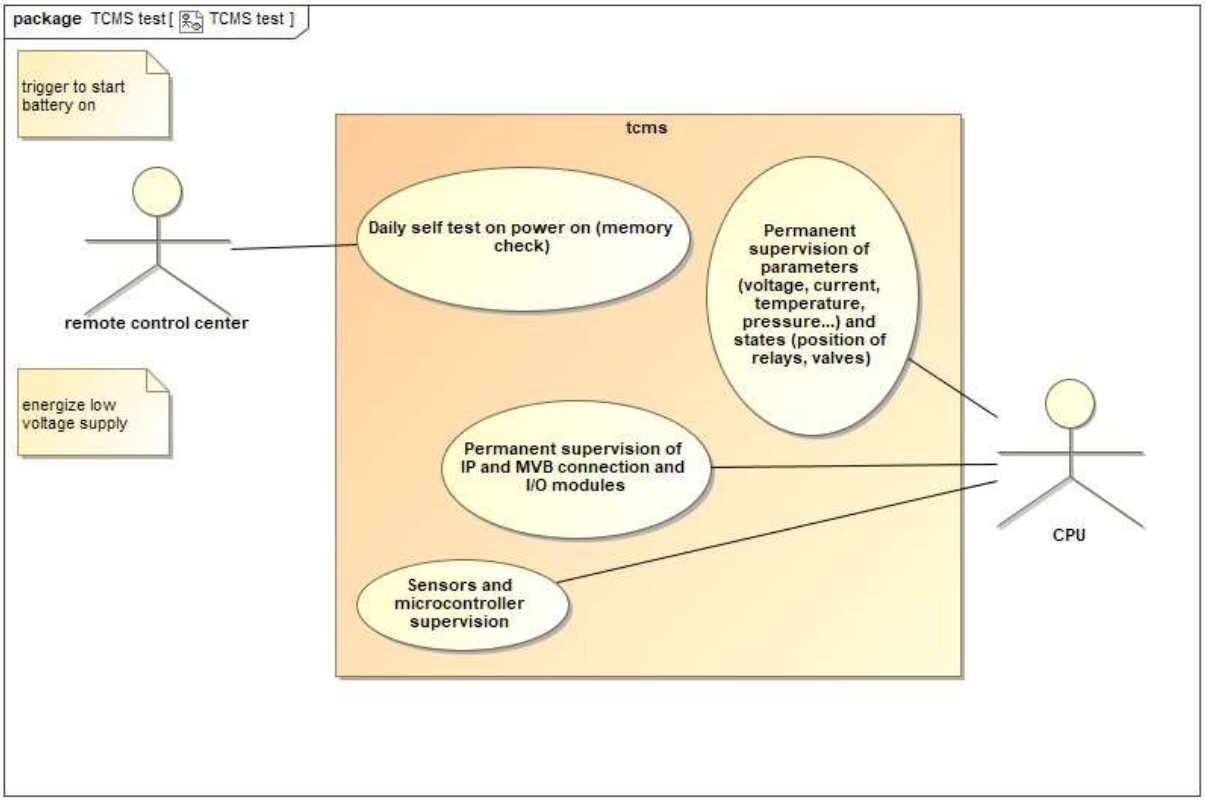

Figure 18: TCMS Test

Use Case	TCMS test
ID	
Actor	TCMS, CPU, ATO
Goal	Automated TCMS
Safety relation	EU Safety Directive, Common Safety Methods (CSM Design Targets)
Precondition	The train is in switched on configuration
Flow of events	-Daily self test on power on (memory check) -Permanent supervision of parameters (voltage, current, temperature, pressure...) and states (position of relays, valves) -Permanent supervision of IP and MVB connection and I/O modules -Sensors and microcontroller supervision
Post condition	The train is in switched on configuration
Things that can go wrong	System failure
Already implemented risk reduction measures	
Observations	

Table 82: Testing TCMS

4.18 DEGRADED SCENARIO MANAGEMENT

4.18.1 State of art

'Degraded' means a restriction or a malfunction of a system or a function. The restriction or malfunction can be caused e. g. by a fault, a contamination or environmental impacts.

The driver or train conductor can currently check the functionality of the system or the component based on a defined procedure if the restriction or malfunction indicated by the diagnostic system or visible during the check at the train start-up. The driver sets the train due to the restriction or malfunction in the ‘degraded mode’.

TSI LOC&PAS specified in clause 4.4. 'Operating rules' that the technical operating documentation gives the rolling stock characteristics to be considered in order to define the operating rules in degraded mode.

4.18.1.1 Architectural principles (Actors and systems involved)

GoA 1/2: The driver detects if a system or a function in the degraded mode and the degraded scenario management describes what the driver has to do in this case. The driver execute the respective remedy action for the system which is in degraded mode.

The driver records the failed system, the status ‘degraded mode’ (start / end time) and the measures in the drivers log book.

The actors are the driver, the train operator and service technicians.

The involved systems are among others power supply, traction, pantograph, fire protection, brakes, passenger doors, passenger alarm, automatic train protection (ATP) and automatic driving mode (ATO).

4.18.1.2 Sub-functions

The following sub-functions according to standard EN15380-4 are involved in the degraded scenario management:

Level					Function description	Example / Explanation
1[1)]	2	3				
H	B				keep train crew informed	all functions to inform the train crew about the current status of the train and its systems
H	B	E	a[2)]		Provide operationally relevant information	
H	B	E	a	B	provide state information of train to train crew	

H	B	E	a	J	provide diagnostic information	
H	E	E	a		handle suitable and safe conditions	central functions to control comfort and safety functionality
H	E	E	a	J	handle monitoring system	
K	D	C	a		provide train / control center communication	
K	D	C	a	D	send diagnostic data to control center	
K	D	C	a	E	send operation data to control center	
K	D	C	a	G	send train state to control center	

1) Level 1, Identifier 'H' ≙ Provide communication, monitoring and controlling in the train formation, 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.

4.18.1.3 Safety requirements

Precise safety criteria and limits are specified for all systems of the train to ensure the safe function of the respective system. When a safe operation of the system in 'degraded mode' is not possible the train does not start or interrupt the mission. When the train is in the degraded mode, the system with the restriction or malfunction will be isolated to set the train and the system in a safe condition. The continuation of the mission carried out with measures respectively constraints.

Example:

A train with an isolated passenger alarm system does not meet the minimum requirements for safety and interoperability as defined in the TSI and shall therefore be regarded to as being in degraded mode (TSI LOC&PAS 4.2.5.3.6.).

4.18.1.4 Service reliability aspects

Periodic and frequent tests at the start of the mission enable an early detection of the failure (and if necessary troubleshooting) and reduce the failure rate respectively increase the reliability during the mission.

4.18.1.5 Test at the start of the mission rationale

The systems (described in this document) will be tested manually by the driver at the start of mission. The driver detects the degraded mode of a system, activates the degraded mode of the failed system and carries out the required measures.

The driver decides based on the severity of the degradation and the safety relevance if the operation of the train can start (if necessary with restrictions) or the operation will not be started or must be stopped / interrupted.

4.18.2 Impacts of transition to GoA3/4

The implementation of the degraded scenario management into GoA3/4 requires first the automatic detection and transmission (to the control center / virtual driver) of malfunctions which are not available today.

The new functionality is that the manual handling of the driver at GoA 1/2 will be transferred to an automatic testing and monitoring of the systems and an automatic procedure for systems in the degraded mode. This procedure is assumed to take place after “battery on” command with a certain periodicity. During the test the vehicle is in a special test mode and will not receive any driving commands. At the end of the test the vehicle shuts down and waits for a new start trigger by the virtual driver.

The degraded mode will be activated automatically by the vehicle control unit or by the virtual driver. The data of the degraded mode (start / end time, measures, etc.) will be logged automatically.

The systems (among others power supply, traction, pantograph, fire protection, brakes, passenger doors, passenger alarm) of the autonomous train should be tested at the start and monitored permanently so that the control center / virtual driver can intervene at an early stage and if necessary shuts down the train.

The scenario management defines the procedure to guarantee the safety and reliability of the autonomous operation when a systems, a function or a component of the autonomous train is in the degraded mode.

The autonomous train has a permanent real-time connection to the control center to provide operation and diagnostic data and the position of the train.

The virtual driver is the redundancy in case of a failed automatic testing at the start and he can carry out the testing via the real-time connection from the control center.

4.18.3 GoA3/4 Tests at the start of the mission rationale

At each start all safety relevant systems of the train must be checked to detect a system or a function in the degraded mode.

- Safety relevant systems available and functional (without any restriction or malfunction)
- Real-time connection to the control center available
- Monitoring system available
- Train state available
- Operation data and diagnostic data available
- Simulation of management for safety relevant systems in degraded mode

When a degraded system or function will be detected by the tests, the diagnostic system sends a message to the control center and stops in the first step the release of the train. The vehicle control unit activates automatically the degraded mode for the system respectively for the train.

The control center or the virtual driver confirms manually the degraded mode for the failed system respectively for the train.

In some cases the system or function is limited (e. g. one of the passenger doors does not open, the speed of train is reduced), in other cases the system or function is failed and the failure of the function is very critical so that the operation must be interrupted or stopped.

Additionally, the virtual driver can check the system, activates the degraded mode and defines the required measures (if necessary the use of a service technician for troubleshooting).

The permanent diagnosis and periodical maintenance test are required to guarantee the availability and reliability of the autonomous train.

4.18.4 Use cases definition

Use Case	Testing of safety relevant systems
ID	DSM1
Actor	Virtual driver
Goal	G_DSM1: Make sure safety relevant system is available within the technical specifications.
Safety relation	Monitoring of safety relevant subsystems is precondition for safe reaction towards degraded situations.
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train 2. Select safety relevant system ON 3. Check power supply for system is provided 4. Trigger automatic testing of system (e. g. door control to open and close the doors) 5. Check if a fault indicated by the monitoring system 6. Check if possible visible (e. g. by cameras the opening and closing of the doors) if the function guaranteed. 7. Repeat step 2. to 6. for each safety relevant system
Post condition	Inform the TCMS / control center / virtual driver whether the safety relevant system is power supplied and is ready for operation.
Things that can go wrong	Component or function of safety relevant system faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 83: Testing of safety relevant systems

Use Case	Testing of real-time connection to control center
ID	DSM2
Actor	Virtual Driver
Goal	G_DSM2: Make sure real-time connection to control center is available
Safety relation	- Real-time connection to control center is safety relevant to send train state, operation and diagnostic data to control center and handle the degraded mode by virtual driver (redundancy).
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train 2. Select transmitter-receiver module ON 3. Check power supply for transmitter-receiver module is provided 4. Check for possible detected failure of transmitter-receiver module 5. Check real-time connection to control center is available
Post condition	Inform the TCMS / control center / virtual driver whether transmitter-receiver module and real-time connection to control center is available.
Things that can go wrong	Transmitter-receiver module faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 84: Testing of real-time connection to control center

Use Case	Testing of monitoring system availability
ID	DSM3
Actor	Virtual driver
Goal	G_DSM3: Make sure monitoring system of train is available
Safety relation	- Monitoring system is safety relevant to provide train state, operation and diagnostic data for sending to control center and virtual driver (detection of degraded mode)
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked.
Flow of events	1. Occupy train 2. Select monitoring system ON 3. Check power supply for monitoring system is provided 4. Check for possible detected failure of monitoring system 5. Perform perception test by (if applicable) 6. Save and transmit result of perception test.
Post condition	Inform the control center / virtual driver whether the monitoring system is power supplied and is ready for operation.
Things that can go wrong	Monitoring system faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests.
Observations	Test is done before start of each mission.

Table 85: Testing of monitoring system availability

Use Case	Testing of train state, operation and diagnostic data availability
ID	DSM4
Actor	Virtual driver
Goal	G_DSM4: Make sure train state, operation data and diagnostic data are available for control center and virtual driver
Safety relation	- Permanent provision of train state, operation data and diagnostic data is safety relevant to detect the degraded mode of train / system by control center or virtual driver
Precondition	- Electric power supply available (Test DSM3 is done) - Real-time connection to control center available (Test DSM2 is done) - Train is in standstill. Traction must be blocked.
Flow of events	1. Check transmitter-receiver module ON 2. Check power supply for transmitter-receiver module is provided 3. Check real-time connection to control center is available 4. Check monitoring system ON 5. Check power supply for monitoring system is provided 6. Check train state, operation data, diagnostic data from monitoring system 7. Save and transmit self-test result to remote host.
Post condition	Inform the control center / virtual driver whether the train state, operation data and diagnostic data are available.
Things that can go wrong	Real-time connection to control center not available, monitoring system faulty, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for monitoring system before start of each mission - Testing of real-time connection before start of each mission
Observations	Test is done before start of each mission.

Table 86: Testing of train state, operation and diagnostic data availability

Use Case	Simulation of management for system in degraded mode
ID	DSM5
Actor	TCMS, Virtual driver
Goal	G_DSM5: - Make sure degraded mode of failed system is detected and degraded mode is activated automatically. - Degraded mode of failed system is logged automatically.
Safety relation	Detection of failure and activation of degraded mode
Precondition	- Electric power supply available - Train is in standstill. Traction must be blocked. - Train is in dedicated test mode
Flow of events	1. Occupy train 2. Select safety relevant system ON 3. Check power supply for system is provided 4. Check monitoring system ON 5. Check power supply for monitoring system is provided 6. Simulate failure of system (e. g. door control does not open the doors) 7. Check if a failure indicated by the monitoring system 8. Check if the degraded mode detected and activated for the failed system 9. Check if the degraded mode logged for the failed system 10. Check if control center or virtual driver informed about failed system in degraded mode 11. Control center or virtual driver confirms manually the degraded mode for the failed system 12. Repeat step 2. to 11. for each safety relevant system
Post condition	Inform the control center / virtual driver whether the detection and activation of degraded mode for failed safety relevant system are happened automatically. Shut down / restart TCMS in normal operation mode.
Things that can go wrong	Monitoring system faulty, simulated failure not indicated, power supply not provided
Already implemented risk reduction measures	- The train is fully equipped to perform the tests. - Testing of power supply for monitoring system before start of each mission
Observations	Test is done before start of each mission (every 24 h)

Table 87: Simulation of management for system in degraded mode

4.19 ON BOARD TEST RESULTS AUTOMATIC MANAGEMENT

4.19.1 State of art

4.19.1.1 Architectural principles

N.A.

4.19.1.2 Sub-Functions

The core of the functionality is testing the capacity of the Autonomous Train Recovery System (ATRS) to report and restore failures. However, the actions to be handled are different depending on the situation and must be carried though different procedures.

The activation trigger is common and it is the detection of a failure defined by the ***Failure Detection*** sub function. The possible outputs are the ***Restart the Mission*** and ***the Cancel the mission*** sub functions that carry the situations that are naming. Moreover, a report of the failure information, which is common for both situations, is carried by the ***Communication to the ground of the tests results and of the decisions taken*** sub-function.

4.19.1.3 Safety requirement

It is not consider a safety system neither in GoA1/2 not in GoA3/4. The safety capabilities are relied on the safety subsystems, as this is only a detection and reporting issue. In case of, at least, one issue may occurs in one of the safety subsystems, these subsystems will protects themselves.

4.19.1.4 Mission reliability impacts

The impact is considered low as, in case of a failure in the ARTS, the systems may be functional also. It is not possible a degraded mode for the ARTS.

4.19.1.5 Test at the start of the mission rationale

A set of failures are prepare in order to confirm that the ARTS is able to handle the necessary actions such as:

- Failure detection.
- Stop the mission.
- Restart the mission.
- Notify to personnel and passengers about a failure.

4.19.2 Impacts of transition to GoA3/4

As it was defined before, the impact is minimum as the functionalities are not critical to the automatic functionality. However, the GoA1/2, based on the EN18530-2 groups G and E and EN18530 – 4 groups H,K and transversals, already had the functionalities that are defined in the below use case, it is changed the way they are automated. Such as:

- Provide trials results and manage properly those results in a data base (dates, space in data base,…).

- Start diagnosis data acquisition, processing and analysis.
- Register of failures and incidents.
- Provide diagnosis information.
- Manage maintenance mode.
- Manage emergency modes.

4.19.3 GoA3/4 Tests at the start of the mission rationale

The main drawback is the report of the failures in an automatic manner without human intervention. Therefore, the impact is high to move to GoA3/4, the safety conditions depend on the safety subsystems. However, the automatic view that the ATRS introduces is impactful.

4.19.4 Use cases definition

The use case define how to prepare the On-board section to certain subsystem/equipment failures before the mission starts. Prepare the system on how it is recovered or and can circulate in a compatible way with each failure to at least the next station or to the depot.

The core context for the Use case is performing relevant actions to restore the system in failure, which can range from switching to a backup system, restarting the system, continuation in degraded mode, etc.

Use Case	Restore Subsystem in failure
ID	19X1
Actor	Autonomous Train Recovery System (ATRS) | Subsystem in failure
Goal	G_19X1: The ATRS is prepared to perform actions to succeed in recovering the failed subsystem before the mission is started.
Safety relation	The use case is not safety related. The safety resides in the failed subsystem, which if not recoverable, will have its own fail-safe safeguards to prevent unsafe movement of the train with the failed system.
Precondition	The faulted subsystem has reported to the ATRS the type and magnitude of the failure.
Flow of events	1. A set of programmed failures are scheduled to be executed sequentially. 2. The sub-system failure detection detect each of these failures independently and by groups planned. 3. Different actions are carried depending on the failure.
Post condition	The On Board subsystem that was in failure and on which actions have been taken to recover it is ready to operate.
Things that can go wrong	If the actions performed by ATRS to recover the failed subsystem do not succeed in recovering it, the subsystem is in failure or degraded mode, pending evaluation of whether or not the train can continue with the mission under these conditions.
Already implemented risk reduction measures	
Observations	

Table 88: Restore Subsystem in failure

In order to proceed with the Use Case, the following input triggers it to get different outputs depending on the ATRS actuation.

- **Input Sub-Functions:**
  - **Failure Detection**

This sub-function is in charge of detecting that a subsystem of the train is in degraded or failure mode, and all relevant information is collected to determine what actions to take. The sub-function receives the required information from a failed on-board subsystem to be able to assess the type and magnitude of the failure and, then, the following actions are triggered:

1. A communication link must be established between the on-board subsystem that is monitored by the ATRS, with the appropriate communication protocol to receive relevant subsystem status information.
2. The failed subsystem shall report to the ATRS the type and magnitude of the failure.

Result: The ATRS is able to evaluate possible actions to recover the failed subsystem.

- **Output Sun-Functions:**

After the detection of the cases and their corresponding report for the failing tests. The following outputs may occur depending on the failure detected and how these failures are handled. Each sub function serves as a conclusion for the test:

  - **Restart the Mission**

If it is considered that the mission can be continued, even if it is in degraded mode, it is proceeded to continue. The ATRS has evaluated the status of the required subsystem and considered that the train is able to continue the ongoing mission:

1. ATRS checks that all subsystems required for the mission are active, and if not, activates them.
2. ATRS sends the appropriate command to the safety subsystems in order to prepare them to restart the mission.
3. ATRS sends the ATO subsystem the commands to engage and continue the mission.

Result: The train would continue the ongoing mission

  - **Cancel the mission**

If it is considered that it is not possible to continue with the mission, it is cancelled. The train will be kept in security conditions until it is decided from ground how to rescue the train.

As a context, the ATRS has attempted to recover the failed subsystem, but after revaluating, the status of the train's subsystems has decided that the train is not fit to continue with the mission:

1. ATRS performs an activation protocol of the emergency systems configured to put the train in safe conditions while waiting to be rescued by external means.
2. ATRS communicates the status of the train to the ground and awaits instructions.

Result: Train would be waiting to be rescued or running in degraded conditions to the next station.

  - **Communication to the ground of the tests results and of the decisions taken**

The status of the train after the restoration actions is communicated to the track, as well as if the train continues with the mission or it is cancelled, needing in this last case, actions from ground to remove the train and the passengers.

As a context, the ATRS has performed the configured actions and has to communicate the status of the train to the ground to wait for confirmation to continue the mission or instructions after its cancellation:

1. ATRS initiates communications session with ground if not already established.
2. ATRS communicates to ground the status of all subsystems as well as the overall status of the train, and whether it considers that it is ready to restart the mission or if it is cancelled.
3. ATRS is awaiting feedback from the ground on how to proceed in the event of mission cancellation.

Result: Train would be waiting for instructions in safety mode

4.20 NON-AUTOMATIC MANAGEMENT (FROM GROUND STATION)

4.20.1 State of art

4.20.1.1 Architectural principles

N.A.

4.20.1.2 Sub-Functions

This case is similar to the previous, but the authority to decide how the mission must proceed is relegated to the ground. The flux of actions are very similar; hence, the sub-functions are similar too. To recapitulate the sub-functions, the objective is validated the capacity of the ground Recovery System to interact with the ARTS to recover the mission or to restart it in case of a failure is detected. Moreover, the information must be reported.

4.20.1.3 Safety requirement

It is not consider a safety system neither in GoA1/2 not in GoA3/4. The safety capabilities are relied on the safety subsystems, as this is only a detection and reporting issue. In case of, at least, one issue may occurs in one of the safety subsystems, these subsystems will protects themselves.

4.20.1.4 Mission reliability impacts

The impact is considered low as, in case of a failure in both the ARTS and/or Ground Recovery System, the systems may be functional also. It is not possible a degraded mode for the ARTS and/or Ground Recovery.

4.20.1.5 Test at the start of the mission rationale

A set of failures are prepare in order to confirm that the ARTS- Ground Recovery System are able to handle the necessary actions such as:

- Failure detection.
- Stop the mission.
- Restart the mission.
- Notify to personnel and passengers about a failure.

4.20.2 Impacts of transition to GoA3/4

As it was defined before, the impact is minimum as the functionalities are not critical to the automatic functionality. However, the GoA1/2, based on the EN18530-2 groups G and E and EN18530 – 4 groups H,K and transversals, already had the functionalities that are defined in the below use case, it is changed the way they are automated. Such as:

- Provide trials results and manage properly those results in a data base (dates, space in data base,…).
- Start diagnosis data acquisition, processing and analysis.
- Register of failures and incidents.
- Provide diagnosis information.
- Manage maintenance mode.
- Manage emergency modes.
-

4.20.3 GoA3/4 Tests at the start of the mission rationale

The main drawback is the report of the failures in an automatic manner without human intervention. Therefore, the impact is high to move to GoA3/4, the safety conditions depend on the safety subsystems. However, the automatic view that the ATRS-Ground Recovery System pair introduces is impactful.

4.20.4 Use cases definition

As it is defined for the On Board Automatic Results, the key of this functionality is validating the restore capabilities of the compositions before the mission is started. In this case, the ground provides the decision for the mission. Nevertheless, the sub-functions and the way to procedure is the same with particular points due to the ground authority relegation.

The core context for the Use case is performing relevant actions to restore the system in failure from the ground in collaboration with the ATRS, which can range from switching to a backup system, restarting the system, continuation in degraded mode, etc. The Ground tackles the recovery actions, but they can be done by the ATRS if it is authorized to continue the mission (keeping the communication about the restoring actions to the Ground as it is done in the On Board Automatic Management).

Use Case	Restore subsystem in failure (inside train by trackside request)
ID	20X1
Actor	Ground | Autonomous Train Recovery System (ATRS) | Subsystem in failure
Goal	G_20X1: Ground order to perform actions and succeed in recovering the failed subsystem.
Safety relation	The use case is not safety related. The safety resides in the failed subsystem, which if not recoverable, will have its own fail-safe safeguards to prevent unsafe movement of the train with the failed system.
Precondition	The faulted subsystem has reported to the Ground (through ATRS) the type and magnitude of the failure.
Flow of events	1. A set of programmed failures are scheduled to be executed sequentially. 2. The sub-system failure detection (ATRS) detect each of these failures independently and by groups planned and report it to the Ground. 3. Different actions are carried depending on the failure. The Ground can tackle this action mainly, but also by the ATRS if the Ground authorizes it.
Post condition	The on-board subsystem that was in failure and on which actions have been taken to recover it is ready to start the operation.
Things that can go wrong	• If the actions order by Ground or ATRS to recover the failed subsystem do not succeed in recovering it, the subsystem is in failure or degraded mode, pending evaluation of whether or not the train can continue with the mission under these conditions. • Failure of the link between Ground and train.
Already implemented risk reduction measures	
Observations	

Table 89: Restore subsystem in failure (inside train by trackside request)

In order to proceed with the Use Case, the following input triggers it to get different outputs depending on the ATRS actuation.

- **Input Sub-Functions:**
  - **Failure Detection**

This sub-function is in charge of detecting that a subsystem of the train is in degraded or failure mode, and all relevant information is collected to determine what actions to take. The sub-function receives the required information from a failed on-board subsystem to be sent to the Ground and, then, been able to assess the type and magnitude of the failure and, then, the following actions are triggered:

1. A failure occurs in some subsystem that requires actions to recover it or to decide whether the train can continue to run under those conditions.

2. A communication link must be established between the on-board sub-systems that is monitored by the ATRS, with the appropriate communication protocol to receive relevant subsystem status information.
3. The failed subsystem shall report to the ATRS the type and magnitude of the failure.
4. The ATRS shall report to ground the type and magnitude of the failure.

Note: It is optional, depending on there are an ATRS that centralize the communication between train and ground for diagnosis and maintenance.

Result: The ATRS is able to evaluate possible actions to recover the failed subsystem.

- **Output Sun-Functions:**

After the detection of the cases and their corresponding report for the failing tests. The following outputs may occur depending on the failure detected and how these failures are handled. Each sub function serves as a conclusion for the test:

- **Restart the Mission**

If it is considered that the mission can be continued, even if it is in degraded mode, it is proceeded to continue. The Ground has evaluated the status of the required subsystem and considered that the train is able to continue the ongoing mission:

1. Ground has evaluated the status of the required subsystem and considered that the train is able to continue the ongoing mission.
2. Ground checks that all subsystems required for the mission are active, and if not, activates them.
3. Ground (via ATRS) sends the appropriate command to the safety subsystems in order to prepare them to restart the mission.
4. Ground (via ATRS) sends the ATO subsystem the commands to engage and continue the mission.

Result: The train would continue the ongoing mission

- **Cancel the mission**

If it is considered that it is not possible to continue with the mission, it is cancelled. The train will be kept in security conditions until it is decided from ground how to rescue the train.

1. Ground has attempted to recover the failed subsystem, but after re-evaluating, the status of the train's subsystems has decided that the train is not fit to continue with the mission.
2. Ground performs an activation protocol of the emergency systems configured to put the train in safe conditions while the train could be rescued, or the train could be transferred in degraded conditions to the next station if the mission would have been started.

Result: Train waiting would be rescued or running in degraded conditions to the next station.

- **Restart the Mission by the ATRS**

1. The train is recovered from a subsystem failure and is able to continue with the current mission, and is awaiting ground authorization to do so.
2. Ground evaluates the overall status received from the train indicating that the train is ready to resume the mission normally or in degraded condition.
3. After verifying that the mission can be continued, the ground sends the authorization to the train (via ATRS) to continue with the mission.

Result: The train could be able to continue the mission to be started.

5 CONCLUSIONS

The working group went through different phases to arrive to generate this document.

In the initial phase contributors conducted brainstorming activity to focus the goals, the way of working, and the main arguments to be investigated to reach the objective of the WP.

The second phase was characterized by the definition of the methodology, put in place in the deliverable structure, by which different actors are facilitated in generating harmonized contribution.

In the third phase each contributor analysed independently the train functions he was in charge of, using his experience and other contributor feedbacks in identifying, by the defined methodologies, the use cases for tests at the start of the mission of GoA3/4 trains.

In the fourth phase all contributions are integrated in the document and the output of the activities done in every phase is summarized, underlining the added values.

The first result of this process is the **standard method identified to define the tests to be performed at the start of the mission.**

The GoA3/4 train tests to be performed at the start of the mission have been identified by **gap analysis with the GoA1/2 train due to different boundary condition**.

The different boundary conditions are mainly the ***replacement of manual operation performed by the humans with automatic procedures, in case of***

- **tests execution**
- **degraded condition activation after a failure during the mission.**
- **test results management**

The autonomous test execution and degraded condition activation could require the introduction in the train of new technologies which could impact as well the type of tests to be performed at the start of the mission.

The analysis done evidenced ***that existing tests performed at the start of the mission of not autonomous trains are generally carried over also on autonomous trains, but with adaptation due to new conditions given by the automatization of the testing process and new technologies needed to manage autonomous trains.***

Several testing use cases are defined and related sequence of actions identified (see List of tables at the beginning of the document for use cases list).

Certain ***new tests could be necessary on GoA3/4 trains,*** depending on the technologies that will be implemented due to the transition from not autonomous to autonomous trains:

- Test of lights
- Test of sanding rate and consistency
- Test of sand level
- Test of Interlock
- Test of passenger door back-up closing
- Test of passenger door isolation
- Test of train positioning

- Test of obstacle perception

The analysis evidenced the **potential necessity of *new technical solutions*** to manage the GoA3/4 trains:

- Lights pattern testing device
- Horn function testing device
- Sanding rate and consistency testing system
- Sand level diagnostic system
- Passenger doors back-up closing independent/redundant system (if door system is not sufficiently reliable/single fault tolerant)
- Passenger doors local isolation with remote control (if door system is not sufficiently reliable/single fault tolerant)
- Passenger alarm system sufficiently reliable or passenger alarm safe state which guarantee the running capability or passenger alarm degraded condition remote activation in case of failure
- Passenger Alarm Device remote isolation or sufficiently reliable/single fault tolerant device
- Passenger Alarm Device remote reset availability
- Precise positioning and perception systems (and digital maps)

Several of these new technologies above evidenced are related to degraded condition management. They could be further equipment to be tested during the start of the mission test, to be sure of the availability of the function during the mission.

A comparison with GoA4 metro application existing technologies for any of the above functions is also suggested to verify the similarity in terms of safety requirements, mission reliability targets and applicability of the control architecture and technical solutions, to evaluate if they can be carried over on GoA3/4 trains.

Further contribution given is related to the case of not fully successful test results and degraded condition management. In such a case **decision taking process is required in GoA3/4 trains** permitting to decide in an autonomous way or with the help of the ground if to start or to cancel the mission.

The train is the integration of the functionalities, not only the sum of them. Test of single function could lead to activate degraded condition which could still guarantee the availability of the function during the mission at acceptable conditions for the function itself, but the combination of different degraded function could be no more acceptable for the train due to the crossed influences of the risks among the functions.

This crossed influence and the decision taking logics of test results need a further investigation.

Further subjects to investigate are:

- the management of the ***system*** **self-test at power on.**

  Power-on and tests before the start of the mission can happen in different time frame or can be in sequence. The contributors considered this aspect in different way: ATO, ATP, Positioning tests propose related use cases, other system not.

At the start of the mission all the *systems*, with or without safety and mission reliability impact, should be in principle switched-on and with self-test passed. The result of these self test should be a precondition to perform the test at the start of the mission and its results in any case influence the final result.

Based on above-described outputs, the D3.1 Deliverable **can contribute to the development of GoA3/4 ATO and new generation TCMS** for the management of GoA3/4 train automatic tests before the departures because provide specific use case which can become the reference for the development of the related control functions, evidences new technologies/technical solutions which could be necessary to develop for GoA3/4 train and indicate subjects to be more investigated.

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