This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Deliverable D 3.2

Test Demonstrators with DPS, Specific application Safety case

Project acronym:	M2O
Starting date:	01/12/2018
Duration (in months):	25
Call (part) identifier:	H2020-S2RJU/OC-IP5-01-2018
Grant agreement no:	826087
Due date of deliverable:	Month 25
Actual submission date:	15/02/2021
Responsible/Author:	NIER
Dissemination level:	PU
Status:	Final

Reviewed: (yes)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Document history		
Revision	*Date*	*Description*
1.0	15/02/2021	First emission

Report contributors		
Name	*Beneficiary Short Name*	*Details of contribution*
Stefano La Rovere	NIER	Interaction with FR8RAIL II partners. Development of the deliverable. Review of LTD studies.
Daniele Vitale	NIER	Development of the deliverable.
Armand Toubol	NEW OPERA	Interaction with FR8RAIL II partners. Internal review of the deliverable.
Luciano Cantone	University of Rome, Tor Vergata	Interaction with FR8RAIL II partners. Development of LTD simulations (Appendix A). Internal review of the deliverable.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Acronyms

ATP	Automatic Train Protection
ABC	Actuator Brake Control (existing brake handle)
BP	Brake Pipe
CCUO	Vehicle control computer
DF	Down/Flat
DPS	Distributed Power System
ED	ElectroDynamic
HA	Hazard Analysis
IHA	Interface Hazard Analysis
IPTCom	Internet Protocol Based Communication for Trains
LCF	Longitudinal Compressive Forces
LTD	Long Train Dynamics
LTF	Longitudinal Tensile Forces
LTE	Long Term Evolution (4G-Wireless Network)
MIT	MITigation
MVB	Multifunction Vehicle Bus
PHA	Preliminary Hazard Analysis
RCDPS	Radio Controller for Distributed power system
SIL	Safety Integrity Level
TCMS	Train Control and Management System
TRL	Technology Readiness Level
TU	Traction Unit
TSI	Technical Specifications for Interoperability
UD	Up/Down
VPN	Virtual Private Network

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Table of contents

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

1 Definition of the system

1.1 Context

To achieve the objectives of the European Commission white paper on Transport 2011, aiming at a 30% shift to rail of road freight transportation over 300km by 2030, the rail freight transport market share has to increase strongly. As part of the Shift2Rail projects (FFL4E closed and FR8RAIL II currently on going), a Distributed Power System (DPS) has been developed by FR8RAIL II partners for increasing the capacity of goods trains and installed on locomotives of the BR 187 and BR 188 series. This DPS train allows implementing multiple traction through radio communication, being driven by one driver at the first Traction unit. The previous FP7 MARATHON project [13] has shown the feasibility of 1500m long coupled heavy trains with distributed power of two Traction Units (TU) running safely on the French network. Within this context, the Shift2Rail M2O project intends to extend the possibilities to multiple Traction units as Distributed Power System (DPS), in collaboration with FR8RAIL II project.

1.2 Purpose and scope

The present deliverable of the M2O project contributes to the demonstration that DPS train has been designed and developed according to the requirements defined in EN 50129 [5]. Precisely, it refers to the specific application of DPS train for the execution of the experimental test campaign, planned and managed by the FR8RAIL II project, defined by the trains consists (Demonstrator(s)) specified in §1.5.1, performing the tests described in §1.5.3, along the test track identified in §1.5.2.

The main objectives of this deliverable are:

- to describe the safety analyses performed during the (WP2 of the) M2O project and to provide a summary of their results, concerning a generic implementation of DPS trains in the context of an Integrated railway system (see §1.4.1) and providing a general base for the safety assessment of the present and future specific applications;
- to describe the specific safety activities performed during (the WP3 of the) M2O project on the DPS train Demonstrator(s), and specifically to address the actual implementation of safety requirements (i.e. mitigations specified during the safety analyses);

Safety relevant information produced and collected during the M2O project is provided by a structure of content (see §1.3) compliant with a Specific Application (SA) Safety Case, as defined by EN 50129 [5].

Within the context of a research project (see §1.1), the quality and organizational requirements deriving from the CENELEC standards have been not addressed.

The Safety management report (§2 of this document) concerns the relations between M2O and FR8RAIL II projects, the safety activities performed during the M2O project and their "position" within the lifecycle (as introduced by the EN 50126 [3]), with focus on the specification of safety requirements and on the related V&V activities.

Because of the scope of the M2O and FR8RAIL II projects, consistently with the TRL 5 of the devices designed by FR8RAIL II, the Technical Safety report (§3 of this document) relies upon a limited set of evidence. It collects the information made available from FR8RAIL II partners and identifies the remaining Verification and Validation (V&V) activities to be executed and the additional mitigations to be implemented (if any) for the safe execution of the experimental test campaign.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

1.3 Structure of the document

Safety relevant information are collected into a structure of content compliant with a "Specific Application Safety Case", as defined by EN 50129 [5]. Therefore the document includes the following sections:

§1 - **Definition of the system** (the present section), providing introductory information on the M2O project, in the purpose and scope of this document, on the functional and physical implementation of DPS train and on the experimental test campaign defining their specific application;

§2 - **Safety Management Report**, providing information on safety activities performed during the M2O project;

§3 - **Technical Safety Report**, providing a summary of the results coming from the activities performed during the M2O project, contributing to the safety demonstration of DPS train Demonstrator(s);

§4 - **Related Safety Case**, providing references to the Safety Cases of equipment's used by the system;

§5 - **Conclusion**, providing an executive summary of the contents of the previous sections.

In addition, the **Appendix A** provides the results coming from the specific simulations performed on the Demonstrator(s), as defined (by FR8RAIL II) for the execution of the experimental test campaign.

1.4 Subsystem Overview

1.4.1 General context

Figure 1 provides a graphical representation of the general context and defines the perimeter of the system considered in the following safety analyses.

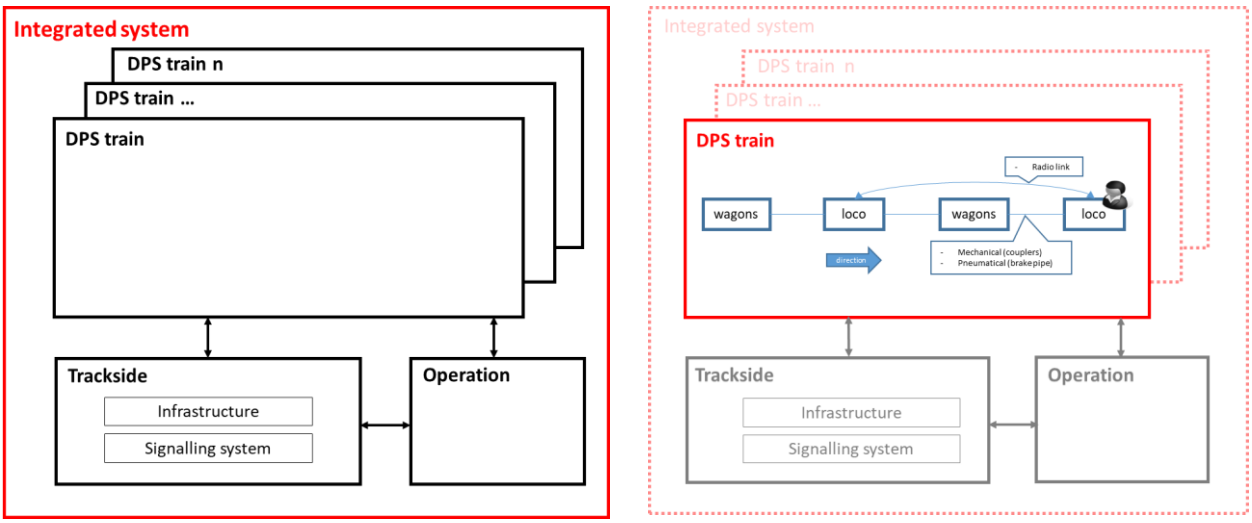


Figure 1 - General context, and "Long freight train" Integrated system (left) and DPS train (right)

The picture on the left side represents the whole "Integrated railway system", including different "long freight trains" equipped by Radio communication and Distributed Power System (DPS trains) and trackside elements. The picture on the right side focuses on a single DPS train, with its external interfaces.

Table 1 provides the hierarchical list of the different elements / factors of the Integrated railway system. The first level includes the trackside elements (belonging to the Infrastructure or to Signalling systems), the DPS train and some operational topics.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Level 1	Level 2	Level 3
1 - INFRASTRUCTURE	1.1 - Substructure elements	1.1.1 - Bridges integrity
		1.1.2 - Tunnels integrity
	1.2 - Superstructure elements	1.2.1 - Top ballast layer integrity
		1.2.2 - Sleepers integrity
		1.2.3 - Rail fastenings integrity
		1.2.4 - Running rails integrity
		1.2.5 - Points and crossings integrity
	1.3 - Rails and track	1.3.1 - Rails profile
		1.3.2 - Track width
		1.3.3 - Track height
		1.3.4 - Track twist
		1.3.5 - Track Curve
		1.3.6 - Track Gradient
		1.3.7 - Track Cant
		1.3.8 - Track Crest and trough
		1.3.9 - Track load carrying capacity
		1.3.10 - Direction of running
		1.3.11 - Electric neutral section
		1.3.12 - Loading gauge
2 - TRACKSIDE SIGNALLING SYSTEM	2.1 - Interlocking (central logic)	-
	2.2 - Automatic Train Protection (Trackside)	-
	2.3 - Trains routing and traffic regulation	-
	2.4 - Field Signaling equipment	2.4.1 - Train detection by track circuit
		2.4.2 - Train detection by axles counter
		2.4.3 - Signals
		2.4.4 - Switch point
		2.4.5 - Level crossing
		2.4.6 - Catenary and Power Supply
		2.4.7 - Hot box detector
3 - DPS TRAIN	3.1 - Running gear	3.3.1 - Wheelsets integrity
		3.3.2 - Suspension integrity
		3.3.3 - Bogie structure integrity
	3.2 - Wagon	3.4.1 - Load carrying units integrity
		3.4.2 - Frame integrity
	3.3 - Coupling system	-
	3.4 - Energy supply system & Pantograph	-
	3.5 - Automatic Train Protection (Trainboard)	-
	3.6 - Driver interface	-
	3.7 - Train Control & Management System	-
	3.8 - Braking and traction equipment	-
	3.9 - Distributed Power System (including Radio equipment)	-
4 - OPERATION	4.1 - Loading of wagons	4.1.1 - Load distribution
		4.1.2 - Load fastening
	4.2 - Train checks	-
	4.3 - Field equipment operation	4.3.1 - Switch point operation
		4.3.2 - Level crossing operation
	4.4 - Train manoeuvre	-
	4.5 - Management of off-normal conditions	-
	4.6 - System's elements (Traction units, wagons) coupling and decoupling	-

Table 1 - Integrated system, relevant elements / factors

1.4.2 DPS Train Functional description

The "specific" functions implemented by DPS trains [15] are described in Table 2 and referred to the two main phases: Train set-up and Train run. The last column specifies the section(s) of the Functional and system requirements specification providing details on the given function.

Phase	Main function	Description	Reference to [15]
Train set-up	Train composition	Forming the train according to the established composition, by coupling wagons and traction units.	4.1 Vehicle and train configuration
	Communication set-up	Connection of Traction units to the radio network, after entering the train number. Management of connections of each Traction unit to the radio network: the related status of leading and guided is established.	5.1 Communication set-up
	Train inauguration & configuration	Management of all input train parameters necessary for the start of mission in terms of: position and number of Traction units; position and Length of train parts; - load conditions.	-
	Train operational status management	Management of the operational status of DPS train	5.5 Unattended mode
	Train initial test	Execution of tests at the start of mission, to verify the train configuration and to detect latent failures, including Train initial tests.	-
Train run	Communication between Traction units	Management of data exchange between the guided and leading Traction units during the train mission	5.6 Safe and secure data transmission and monitoring
	Traction management	Management of traction according to set point (including traction cut-off as required).	10.1 Direction of travel 10.2 Set point 10.3 Limitation
	Service brake management	Application of (pneumatically controlled) brake force ensuring that the train's speed can be reduced or maintained on a slope and ensuring the temporary immobilization of the train. Remark: It is independent from the specific type of actuators.	11.1 Automatic brake 11.2 Independent Brake 11.4 Report 11.1.1 Communication Loss
	Emergency (pneumatic) brake management	Application of pneumatic brake force ensuring that the train can be stopped within the maximum allowable braking distance, by the application of the defined brake force.	11.1 Automatic brake 11.3 Emergency Braking 11.4 Report 11.1.1 Communication Loss
	Parking Brake management	Application of braking force ensuring the permanent immobilization of the train.	7 Parking Brake
	Energy management	Management of the pantographs, including their raising and lowering during power supply system changes (disconnection points / border crossing) and the associated main circuit breaker control.	6 Primary Energy 9 Train power supply
	Air management	Management of the main air reservoir (use of compressor)	8 Air management
	Automatic Train Protection management	Management of the status of ATP System (active / sleeping mode) on (leading / guided) Traction units.	4.3 ATP
	Diagnostic	Management of alarms related to operational relevant failures and disturbances and incidental scenario (i.e. fire).	13 Safe diagnostic
	System de-activation	Management of system de-activation and the related communication between the Traction units about the status of train.	-

Table 2 - DPS Train functions

1.4.3 DPS Train Physical description

With reference to Figure 7 (see §3.1.1), providing a high level representation of DPS train architecture, the following equipment are involved in the implementation of DPS:

- the new Radio equipment (one RCDPS and one LTE-antenna for each Traction unit) interfaced to the (adapted for DPS implementation) TCMS of the leading Traction unit and the Radio equipment interfaced to the existing TCMS of the guided Traction unit;
- the Brake panels of the leading Traction unit, including the existing brake panel, which operates on the Brake pipe (for the Emergency and Service brake application) and the new DPS panel, which is isolated from the Brake pipe (i.e. it monitors the pressure) and which reads the safety loop and communicates to the guided Traction Units (over a black-channel including MVB, TCMS, Radio);
- the Brake panels of the guided Traction unit, including the existing brake panel, which is assumed to be isolated from the Brake pipe, and the new DPS panel, which operates on BP (for the application of the Emergency and Service brake), communicates with the leading TU (over a black-channel including MVB, TCMS, Radio) and monitors the Brake pipe pressure;
- the Brake Pipe (unique for the leading and the guided Traction units).

1.5 Experimental test campaign

Even if the definition and execution of the experimental test campaign are out of the scope of the M2O project, its characterization, in terms of configuration of the test trains, tests to be performed and characteristics of the test track, defines the context of this specific application of DPS trains.

This experimental campaign concerns an extension of the stationary and running tests carried out (during 2019) with two BR 187 locomotives and a homogenous goods freight train (500 m in length, speed up to 100 km/h). It concerns test runs with a 660-700m train, investigating the starting and braking behaviour of long freight trains equipped by Distributed Power System and to measure longitudinal forces. The experimental runs are planned for the end of February 2021. DB Systemtechnik GmbH as RU is responsible for the operational performance of test runs.

The train consists under assessment, the test track and the specific tests to be performed are specified in the following sections (based on the Information provided by the FR8RAIL II partners [17]).

1.5.1 Test Trains

Test runs are made by freight trains with a total length of 660-700 m and with up to three Traction units equipped with DPS: two BR 187 (TRAXX AC3) and one BR 188 (TRAXX MS3). It allows to test different DPS train Demonstrators, i.e. different configurations of DPS trains in terms of number and position of TUs, by switching on/off the DPS system in the middle TU (acting as wagon when DPS is not active).

Figure 2 - Train consists

BR 187 are existing locomotives authorized for commercial operation, retrofitted with DPS. BR 188 has not yet been approved; the approval tests have been completed and the commissioning approval has been applied for.

The freight wagons are of the Eanos 59, Res 677, Facns 124 and Facns 133 types. All vehicles are approved bogie wagons. Some of the Eanos wagons will be loaded to achieve a total train mass of around 1700 tonnes (included the traction units)

One DB Systemtechnik unit measuring wagon is placed in the train, close to BR188, which is placed at train end. FR8RAIL II has not shared the parameters measured within the measuring wagon.

1.5.2 Test track

Test runs are planned on the Lichtenfels - Saalfeld (Saale) line.

The train will be assembled and disassembled in Eilenburg or Halle (Saale) after that tests have been completed. Since the train transfers are also to be carried out with active DPS, the transfer routes are also specified within the test routes.

The test track has a maximum slopes of 27‰. Section with the highest gradients along the track between Kronach and Probstzella (see Figure 6, §2.9.7).

1.5.3 Testing activities

Table 3 provides the list of the (main) tests to be performed by the DPS train Demonstrator(s) (see §1.5.1), along the test track (see §1.5.2).

ID	Description
1	Traction to Cruising
2	Cruising at Constant Speed
3	Cruising to Service Braking to Full Stop within normal Stopping Distance
4	Cruising to First Application Step Service Braking to Full Releasing
5	Cruising to Full Service Braking
6	Cruising to Independent Electro-Dynamic Braking to Full Service Braking
7	Cruising to Combined Independent Electro-Dynamic Braking and First Application Step Service Braking to Full Service Braking
8	Cruising to Emergency Braking Brake
9	Traction to Emergency Braking
10	Cruising to Independent Electro-Dynamic Braking to Emergency Braking
11	Cruising to Combined Independent Electro-Dynamic Braking and First Application Step Service Braking to Emergency Braking
12	Additional tests (if performed)

Table 3 - List of (main) tests

The early definition of the testing activities, shared between the M2O and FR8RAIL II partners, allowed the specification and execution of the Longitudinal Train Dynamics (LTD) simulations in order to estimate the in-train longitudinal forces experienced by the DPS train Demonstrators under the test (or worst) conditions. The final test plan (list of tests and their specification) will be finalized by FR8RAIL II partners, in compliance with the results of the activities performed during M2O, i.e. without experiencing more-severe conditions (from LTD perspective).

Additional tests (#12) could be performed (i.e. they have been proposed to FR8RAIL II partners based on the results coming from the LTD studies (see §3.2.4.1) in order to test DPS train considering:

- different gradients of ED brake removal;
- different time intervals for the automatic reduction of the traction force;
- both reactions of the guided Traction unit of DPS train to a brake pipe pressure drop (Full-service braking or Stepwise pressure reduction).

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

2 Safety Management Report

The "Safety Management Report" has the main purpose to provide evidence that the safety of DPS train has been managed during the M2O project by means of an effective safety management process, consistent with the management process for RAMS described in EN 50126 [3].

In general, the purpose of this process is to further reduce the incidence of safety-related human errors throughout the product life cycle, and thus minimise the residual risk of safety-related systematic faults. Specifically, safety activities have been performed during the M2O project in order:

- to gather the information available (also before the M2O project) on DPS trains safe concept and to provide it in a systematic form (i.e. through the development of hazard analyses);
- to ensure that hazardous conditions related to the operation of DPS trains are identified and properly considered in the specification of mitigations reducing risks to a tolerable level;
- to support the development of train dynamics simulations;
- to support the safety demonstration, through the specification of mitigations to be implemented by the DPS train or fulfilled by the operational context within a lager and general context (Integrated system in Figure 1);
- to verify the effective implementation of mitigations by the Demonstrator(s) set for test runs (see §1.4.3) based on information made available by the FR8RAIL II project.

The present section is structured in the following main paragraphs:

- Safety Life Cycle - it describe the "safety life-cycle phases" of the system and it identify the Verification & Validation activities;
- Relations with FR8RAIL II project - it describe the organization involved in the execution of technical activities during the M2O project, with focus on the relationship with FR8RAIL II project;
- Safety Plan - it describe the activities (technical and management) realized for every phase of the "safety life-cycle";
- Safety Requirement Specification - it describe the process for the specification of Safety requirements, the performed safety analyses and the criteria for the specification of their Safety Integrity Level (SIL);
- Hazard Log - it describes the activities realized to maintain the traceability between the hazards and the countermeasures to avoid them;
- Safety Verification and Validation Activities - it concerns the Verification and Validation activities aimed at verifying the fulfilment of the specified safety requirements;
- Longitudinal Train Dynamics studies - it concerns the studies performed on the during the M2O project on the Longitudinal Train Dynamics (LTD) of DPS trains.

2.1 Safety Life Cycle

Figure 3 provides the V-cycle representation introduced by the EN 50126 [3] and shows the "position" of the safety activities performed during the M2O project.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

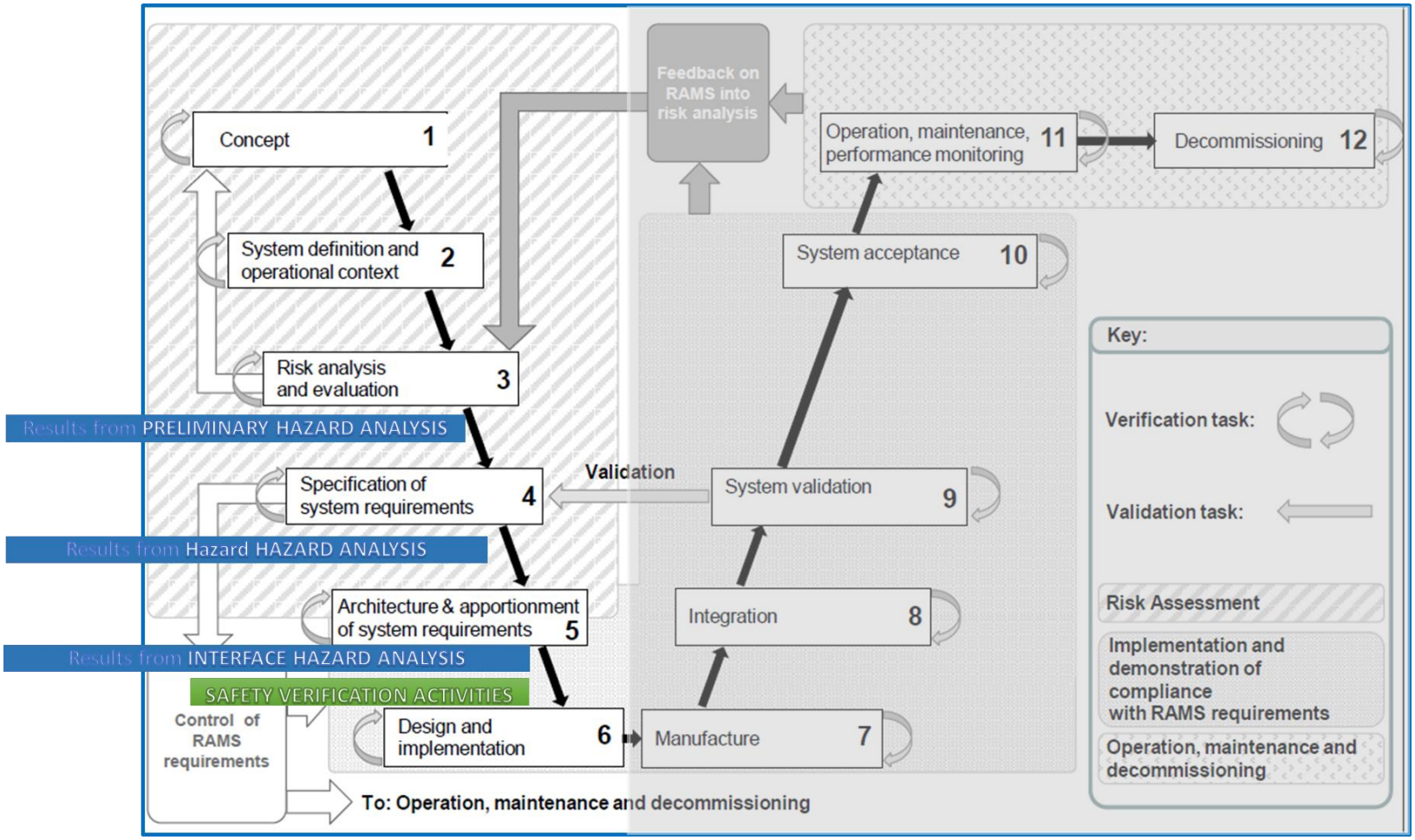


Figure 3 - V&V Cycle and Safety activities

2.2 Relations with FR8RAIL II project

The safety activities performed during the M2O project have been based on the input provided by the FR8RAIL II project.

Base input information concerns:

- the scope of safety analyses, which is defined by the functional specifications of DPS trains [14], [15];
- the scope of Longitudinal Train Dynamics studies, which is defined by the configuration of the DPS train Demonstrator(s) (see §1.5.1) and the characteristics of the test track (1.5.2).

The content and the results coming from the safety analyses performed during the M2O project (provided by the deliverable D2.2 64) have been shared and reviewed by the safety experts of the FR8RAIL II project.

The specific Verification and Validation activities to be performed before the experimental test campaign have been identified by M2O and FR8RAIL II partners, as well as the further mitigations to be implemented because of the limited Verification and Validation activities.

The verification of the fulfilment of safety requirements by the Demonstrator(s) and more in general of the implementation of measures (mitigations) for the safe execution of the experimental test campaign relies on the information made available from FR8RAIL II partners. Indeed, they are in charge of the execution of the Verification and Validation activities, including:

- traceability between the mitigations specified by the safety analyses and the (safety) requirements specified for DPS train;
- evidence (to be provided before tests) of the fulfilment of safety requirements specified for DPS trains, by the Demonstrator(s) equipped by the DPS under development;
- evidence (to be provided before tests) of the fulfilment of safety application conditions exported to the remaining elements of the Integrated railway system, as relevant for tests execution;
- evidence (to be provided before tests) of the fulfilment of any additional mitigation required for the safe execution of the experimental test campaign, because of the limited evidence available from the Verification and Validation activities.

2.3 Safety Plan

The Safety plan of the activities performed during M2O project is provided by the deliverable D2.3 [20].

It specifies the safety activities performed for the system definition and operation (WP2) and for the safety demonstration of the DPS train(s) for test runs (WP3), and their relations with the different phases stated by the EN 50126 [3] (as possible).

The Safety plan also provides insights on the management of safety requirements coming from safety analyses, describes the content of the Hazard log, and explains the approach for the allocation of the Safety Integrity Level to the implemented functions, consistently with the risk acceptance stated by the applicable standards [3], [5].

The safety activities performed during the M2O project include:

- Safety analyses focused on the Integrated railway system including a generic implementation of "long freight trains" based on DPS and radio communication (independently from the specific technology) and trackside's elements (belonging to the Infrastructure or to Signalling systems), on the functional specifications and on the architecture implemented for DPS train, (as defined by FR8RAIL II project);
- Longitudinal Train Dynamics studies, providing supporting evidence on the safe behaviour of DPS train Demonstrator(s), in terms of Longitudinal Compressive Forces (LCF), Longitudinal Tensile Forces (LTFs) and stopping distance expected for DPS trains and their Demonstrator(s);
- Safety Verification and validation activities, specifically concerning their planning and the gathering of available information.

2.4 Safety Analysis Activities

In general, the purpose of the safety analyses is the identification of potential hazards and their associated risks, by means of either qualitative or quantitative methods. Subsequently, to each hazard adequate countermeasures are defined in order to reduce the associated risk to an acceptable level.

According to the Safety plan (provided as part of the deliverable D2.3 [20])[20], the main purposes of the safety analyses performed during the M20 project are:

- to gather the information available (also before the M2O project) on DPS trains safe concept and to provide it in a systematic form (i.e. through the development of hazard analyses);
- to ensure that hazardous conditions related to the operation of DPS trains are identified and properly considered in the specification of mitigations reducing risks to a tolerable level;
- to support the development of train dynamics simulations;
- to support the safety demonstration of Demonstrator(s), through the specification of mitigations to be implemented by the DPS train and to be exported as Safety related Application Condition to the other elements of the Integrated system.

The scope of these safety analyses is defined by the elements of the Integrated system listed in Table 1 and by the DPS train functional behaviour defined under the FR8RAIL II project [14], [15].

The results obtained by the safety analyses are the basis for the evaluation of the safety of each "specific application" of DPS trains, i.e. with reference to specific train(s) (i.e. Traction units and wagons types and train configurations) and track(s) where the running authorization applies.

According to Figure 4, three main safety analyses have been developed during the M2O project (described in the following sections). Their main results are the list of hazards (provided in § 3.1.3), the mitigations to be implemented (including the safety requirements to be implemented by DPS train and safety-related application conditions to be met by the remaining elements of the Integrated railway system), and the Safety Integrity Level allocated to the DPS train functions (provided in §3.1.4) and then to the (functional) safety requirements.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

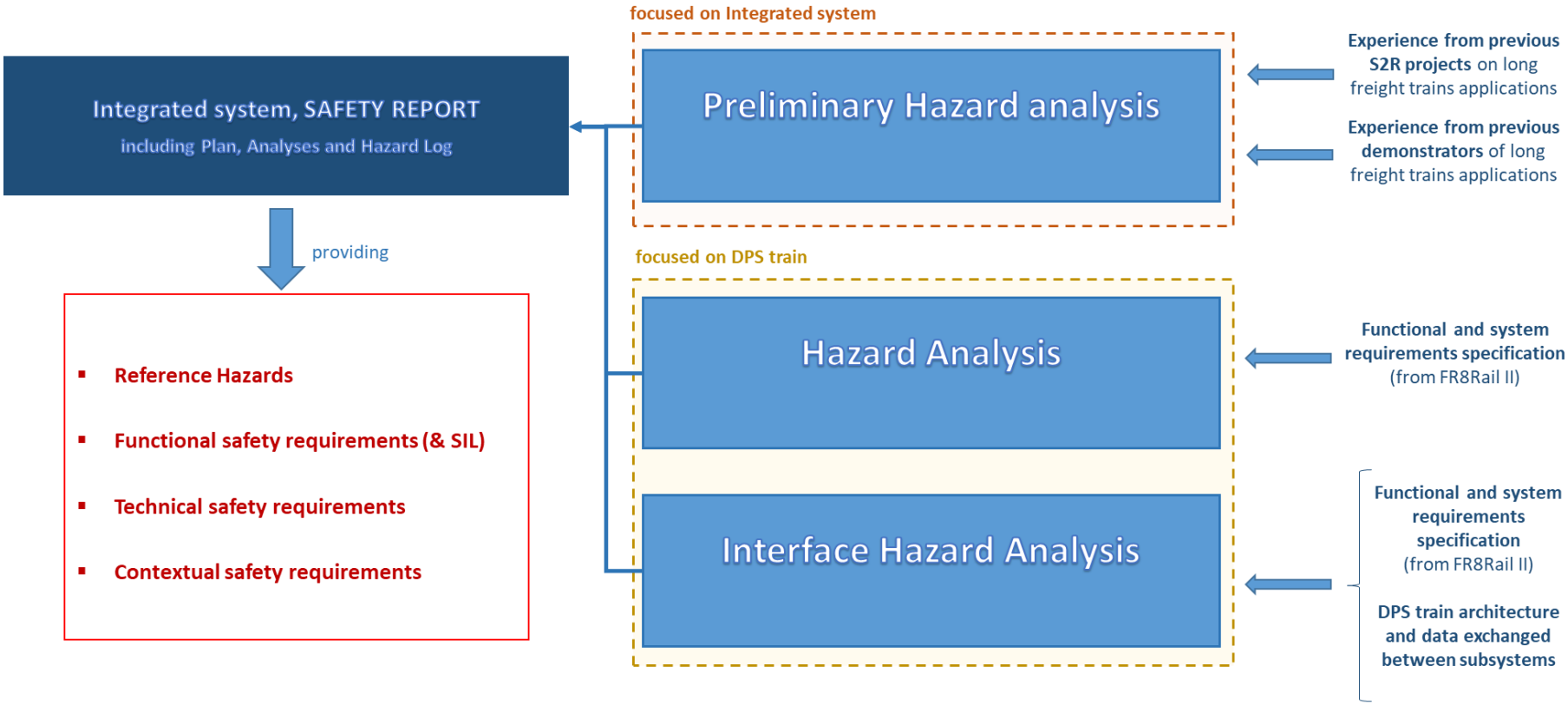


Figure 4 - Safety analysis process and activities

2.4.1 Preliminary Hazard Analysis

The Preliminary Hazard Analysis (PHA) has been developed for the entire Integrated railway system depicted in Figure 1, with the objective to identify the elements/factors (of the infrastructure, signalling systems, "long" freight trains and operations) that could lead to the occurrence of hazardous conditions, because of one or more specific characteristics of long freight trains, and to specify proper mitigations to be considered in the implementation of DPS train and in the setting of the operational context;

The elements of the Integrated railway system (hierarchically listed in Table 1) have been singularly addressed against the characteristics of long freight trains. The addressed characteristics of long freight trains are the increase of the train length and overall mass, the implementation of distributed traction and brake, the radio communication between Traction units, the presence and operation of multiple pantographs, the presence new equipment.

Specific hazards (i.e. strictly related to the DPS trains characteristics) and "conventional hazards" (i.e. usually applicable to freight trains) having an increase of risk because of one or more characteristics of DPS trains have been identified and assessed. The remaining conventional hazards are assumed to be properly mitigated by the existing technological and procedural provisions and are not further assessed nor mentioned in this document.

Mitigations are specified to reduce the risk related to the identified hazards, by reducing the probability of occurrence of potential accidents or their consequences.

The deliverable D2.3 [20] provides the table filled-in with the results obtained by the Preliminary Hazard Analysis and the list of mitigations specified during the PHA (PHA_MIT_xx).

2.4.2 Hazard Analysis

The Hazard Analysis (HA) has been developed for a specific implementation of (a single) DPS train, with the objective to assess the deviations from the expected behaviour in the execution of the "specific" functions listed in Table 2 (as defined in the Functional and system requirements specification [15]), identifying further hazardous conditions and specifying further mitigations (as needed).

In order to be systematic in the definition of the functional deviations from the excepted behaviour of the system to be singularly assessed, a HAZOP-like approach has been adopted.

In different cases, the effect of each postulated deviations is assessed during different scenarios: coupling of Traction units and wagons; start of mission; train at standstill; train run; train run and on-going pneumatic (service or emergency) brake application; train run and emergency brake command/request from Traction units; train run and fire in a guided Traction units; train running through a neutral section; train separation during running, change of pantographs.

The effects of each functional deviation have been described with reference to the worst possible scenario. The list of hazards has been integrated as needed.

The deliverable D2.3 [20] provides the table filled-in with the results obtained by the Hazard Analysis of the Integrated system and the list of mitigations specified during the HA (HA_MIT_xx).

2.4.3 Interface Hazard Analysis

The Interface Hazard Analysis (IHA) has been developed for a specific implementation of DPS train, with the objective to assess the potential deviations in the data and signals exchanged between DPS train subsystems (i.e. through its internal interfaces), identifying further hazardous conditions and specifying further mitigations (as needed).

With reference to the operational context in Figure 1, the IHA concerns a single long freight train. The IHA is based on the functional and system requirement [15] and on a high level representation of the DPS train architecture depicted in Figure 7.

The IHA is focused on the interface between the equipment involved in the DPS implementation (see §1.4.3). The existing and new interfaces related to DPS implementation (represented by red arrows in Figure 7) have been singularly identified and analysed by the IHA. In order to be systematic in the definition of the functional deviations to be singularly assessed, a HAZOP-like approach has been adopted.

The effects of each deviation in the exchange of data and signals through the internal interfaces is have been with reference to the worst possible scenario, without considering the implementation of any mitigation (Effect pre-mitigation). The list of hazards has been integrated as needed.

The deliverable D2.3 [20] provides the table filled-in with the results obtained by the Interface Hazard Analysis of the Integrated system and the list of mitigations specified during the HA (IHA_MIT_xx).

2.5 Safety Requirement Specification

The safety requirements to be met for the safe operation of DPS trains have been specified through the development of dedicated safety analyses (see §2.4), including the identification of the relevant hazardous conditions and the specification of the mitigations to be implemented in order to achieve an acceptable risk, according to defined criteria.

The mitigations specified during safety analyses have been classified through the three categories defined in the EN 50126 (Part2) [4]: Functional safety requirements, Technical safety requirements and Contextual safety requirements.

Functional safety requirements to be implemented by the DPS train that could concern: the expected functional behaviour of safety-related functions; the safety integrity requirements, the required behaviour in case of failure (enforcement and retention of safe state).

Technical safety requirements concerning constraints for the design, installation and use of the system, including the conformity to standards, regulation, and codes of practice. They could concern safety requirements to be implemented by the DPS and application conditions to be exported to the remaining elements of the Integrated railway system.

Contextual safety requirements cover operational and maintenance tasks. They are application conditions to be exported to the operators in charge of setting the operational context. They could concern the operational procedures for normal and abnormal modes and the specific actions expected for any category of personnel concerned (driver / staff).

A specific set of mitigations (SIL_MIT_xx) concerns the Safety Integrity required to each function implemented by DPS train.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

2.6 Risk Acceptance and Safety Integrity Level

The approach and criteria adopted for the allocation of the Safety Integrity Level (SIL) to the functions (and functional requirements) implemented by DPS trains have been introduced in the deliverable D2.3 [20], consistently with EN 50126 and EN 50129.

In general, the Safety Integrity Level (SIL) is assigned to the functions performed by the system, starting from the results of safety analysis and specifically from the potential damage produced by the hazardous scenario defined by their missed or incorrect execution.

The potential consequences of credible accidents related to the operation of DPS train are listed in Table 4 (defined a priori, and then verified by the safety analyses' results).

Consequences	
C_1	Damages to Infrastructure
C_2	Damage to Rolling Stock(s)
C_3	Injury or loss of life of the train driver or maintenance staff or other people
C_4	Loss of containment (for dangerous goods)

Table 4 - Consequences DPS Train functions

The above consequences could be the effect of different accidents, listed in Table 5 (defined a priori, and then verified by the safety analyses' results).

Accidents	
A_1	Collision between trains (rear, side, head-on)
A_2	Collision of the train with / damage to infrastructure
A_3	Collision of the train with obstacle (persons, animals, road vehicles)
A_4	Derailment / Overturning of the train
A_5	Cut of the train (separation)
A_6	Other accidents (Electrocution, Burns, Asphyxia, Suffocation, Poisoning, Contamination, Fire, Explosion)

Table 5 - Accidental conditions

While four Safety Integrity Levels are defined by EN 50129 [5], a simplified approach is adopted by reducing the graduation into two main levels - High and Low - according to Table 6.

Safety Integrity Levels by EN 50129 [5]	Safety Integrity Levels used in the following
Basic integrity	Basic integrity
SIL1	Low Safety Integrity
SIL2	
SIL3	High Safety Integrity
SIL4	

Table 6 - Safety Integrity Levels

The hazards identified by the performed safety analyses (see §2.4) are listed in Table 9 (see §3.1.3). They could lead to one or more accidents listed in Table 5 and then to the consequences in Table 4. All these hazards have the potential to produce fatalities and/or multiple severe injuries and/or major damage to the environment and/or major damages to main systems, i.e. they could have catastrophic consequences, at least in the worst case, according to the EN 50126 [1]. As general acceptance criteria, the tolerable hazard rate (frequency of occurrence of catastrophic consequences) shall be below the limit stated by the EN 50129 [5] for SIL4 (Tolerable Functional unsafe Failure Rate: 10^{-8} event/h) in order to achieve an acceptable risk level.

Two mitigation strategies are adopted:

- "high safety integrity" is required to the functions that could lead to hazardous conditions, guarantying a frequency of occurrence of hazardous failures less than 10^{-8} event/h (limit stated for SIL4 function by the EN 50129 [5]); no further functional or operational mitigation is required in this case;
- "low safety integrity" is required to the functions that could lead to hazardous conditions, guarantying a frequency of occurrence of hazardous failures less than 10^{-6} event/h (limit stated for SIL2 function by the EN 50129 [5]); in this case, additional operational mitigations are required, that shall be "effective" (i.e. able to avoid the event and to put and maintain the system into a safe state) and "reliable" (i.e. with a probability of failure/error not higher than 10^{-2}, to achieve the limit for the frequency of occurrence of catastrophic consequences).

The safety integrity levels allocated to the DPS train functions according to the above criteria are the reference for each specific application. In general, high safety integrity has to be considered equivalent to SIL 4 and low safety integrity equivalent to SIL 2; this shall be re-evaluated for each (generic and specific) application, based on implementation details concerning the (developed and validated) generic products.

2.7 Safety Verification and Validation Activities

In general, safety Verification and Validation (V&V) activities are carried out throughout inspection and review activities, which can themselves include independent analyses, tests and calculations, in order to achieve all the specified safety requirements and demonstrate the product safety level.

Within the M2O project, the safety V&V activities have the final goal to demonstrate that the mitigations identified by the safety analysis for DPS trains are implemented by the Demonstrator(s) developed by FR8RAIL II for the experimental campaign. Specifically, the activities are focused:

- on the fulfilment of Safety requirements in the configurations adopted by the Demonstrator(s), based on the available information (e.g. coming from train dynamic simulations) and on the further activities to be performed (out of M2O scope) toward a full compliance with EN 50129 [5];
- on the fulfilment of the safety-related Application conditions, e.g. coming from safety analyses, train dynamic simulations and factory testing (if any), by the Demonstrator(s) and related context for the execution of the experimental tests (infrastructure and trackside signalling system)
- on the identification and use of a "safety layer" that implements a set of defenses against communication threats (deletion; insertion; re-sequencing; corruption; delay), independently from the specific technology of the transmission system (GSM-R or LTE radio), compliant with the EN 50159 [7];

- on the train dynamic simulations and specifically on the consistency between the system definition, the safety analyses and the inputs used by simulations, and on the proper use of simulations' results in the global safety analysis, including the specification of the conditions to be met for an optimal traction and safe braking.

As intrinsic limitations related to the scope of the M2O and FR8RAIL II projects, no formal Verification and Validation process has been performed (nor planned) for the DPS development and integration within the Traction unit (see §2.7). Because of the scope of the M2O project, this Safety Case relies upon a limited set of evidence [20].

The focus is on the proper identification of the safety validation activities required for the safe execution of the experimental test campaign.

Table 7 provides the list of sources for safety validation, i.e. of the evidence to be collected and verified, grouped in three main categorises:

"Evidence for validation" specifies the sources of the evidence that safety-related requirements are specified, implemented and verified, to be collected before test runs (summarized in Table 7).

- *test track and train documentation*, proving evidence that Demonstrator(s)' vehicles are compatible with the track (e.g. train's axle load, length, mass and number of axles will not exceed the track limits (for which signalling equipment is designed and trackside equipment are installed), as for the "Reference system (see §2.9.3);
- *test instructions*, i.e. specification of the experimental tests to be performed, that shall provide the instructions to be provided to the staff, including references to the existing procedures / norms (when they apply as for conventional trains) and specific procedures (on DPS-specific topics, e.g. handling of the parking brake, train inauguration, train orientation, alarms, pantographs, Isolation of traction units, run without radio communication, run with DPS switch-off);
- *additional documentation*, including M2O deliverables on LTD and Radio communication (D2.1), Functional and system requirement specification (including Traceability matrix with mitigations), reports on activities to be performed before the test runs (Functional tests, Antennae interference),Admission for tests, specification of the safety layer for the TUS radio communication, (DPS/TCMS) Software and software test documentation and related Safety Cases (see §0).

Type	Evidence for validation	Evidence provided by
TEST TRACK & TRAIN DOCUMENTATION	Vehicle list	FR8RAIL II
	Test track (characteristic / limits)	FR8RAIL II
	Test track (constraints for shunting movement, if any)	FR8RAIL II
	Test track (evidence of no non-stopping area)	FR8RAIL II
	Test track (evidence on absence on neutral section)	FR8RAIL II
	Test track (signaling equipment and verification against vehicle characteristics)	FR8RAIL II

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Type	Evidence for validation	Evidence provided by
TEST INSTRUCTION	Test specification providing instruction to staff (reference to the existing procedures / norms on coupling and decoupling of wagons and Traction units)	FR8RAIL II
	Test specification providing instruction to staff (reference to the existing procedures / norms on departure of DPS train on steep slope)	FR8RAIL II
	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)	FR8RAIL II
	Test specification providing instruction to staff (reference to the existing procedures / norms on shunting movement).	FR8RAIL II
	Test specification providing instruction to staff (reference to the existing procedures / norms on unavailability of air in the main reservoirs)	FR8RAIL II
	Test specification providing instruction to staff (no dangerous goods on board)	FR8RAIL II
	Test specification providing instruction to staff (on handling of the parking brake)	FR8RAIL II
	Test specification providing instruction to staff (for setting limits of traction and/or dynamic brake effort)	FR8RAIL II
	Test specification providing instruction to staff (on train inauguration)	FR8RAIL II
	Test specification providing instruction to staff (for setting train orientation)	FR8RAIL II
	Test specification providing instruction to staff (for train initial test execution)	FR8RAIL II
	Test specification providing instruction to staff (on handling of / reaction to alarms)	FR8RAIL II
	Test specification providing instruction to staff (on management of pantographs)	FR8RAIL II
	Test specification providing instruction to staff (on Isolation of traction units in standstill)	FR8RAIL II
	Test specification providing instruction to staff (train run without radio communication)	FR8RAIL II
	Test specification providing instruction to staff (train run with DPS switch-off)	FR8RAIL II
ADDITIONAL DOCUMENTATION	M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))	M2O
	M2O deliverables on Radio communication (D2.1)	M2O
	Functional and system requirement specification (including Traceability matrix with mitigations)	FR8RAIL II
	Report on Functional tests (before test runs)	FR8RAIL II
	Report on antennae interference	FR8RAIL II
	Admission for experimental tests	FR8RAIL II (DB Netz)
	Specification of Safety layer for TUS radio communication	FR8RAIL II
	(DPS/TCMS) Software and software test documentation	FR8RAIL II
	Traction unit Safety Case(s) (at least for existing equipment / before revamping for DPS implementation)	FR8RAIL II

Table 7 - Sources of evidence for the DPS Validation

2.8 Hazard Logging

The main safety-relevant information coming from the safety analysis have been recorded in the Hazard Log (Annex of the deliverable D2.3 [20]). It provides the list of the hazardous conditions and specifies the potential accident(s) for each (macro) hazard and the mitigations to be implemented, by DPS trains or other elements of the Integrated system, in order to achieve a tolerable risk for each (specific) hazard.

2.9 Longitudinal Train Dynamics studies

The results coming from the studies performed during the M2O project on the Longitudinal Train Dynamics (LTD) of DPS trains are provided in different deliverables:

- D2.2 [19] providing results from the development of sensitivity analyses, in order to identify the most relevant parameters impacting LTD;
- D3.1 [21] providing results from general simulations addressing different train configurations, in terms of hauled mass, train length, number of Traction Units (TUs), and operational conditions, considering different radio technologies;
- D3.3 [22] providing results from preliminary simulations addressing a train family equipped by the DPS system based on LTE radio communication (i.e. compatible with the expected Demonstrator(s));
- D3.2 (Appendix A of this document) providing results from specific simulations on the Demonstrator(s), defined (by FR8RAIL II) in terms of train consist and specific tests to be performed.

General information concerning LTD studies is provided in the following sections. A summary of results coming from the simulations performed on DPS Trains is provided in the Technical Safety Report, discussing the correct functional operation (see §3.1.8) and the effects of faults (see §3.2.4).

2.9.1 TrainDy

Longitudinal Train Dynamics studies have been performed during the M2O project using TrainDy software. TrainDy is an UIC-approved software (developed in Matlab) that allows to solve both pneumatic models (venting of brake pipe and filling of brake cylinders) and mechanical models (computation of relative movement between consecutive wagons). It has been used to compute Longitudinal Compressive Forces (LCF) and Longitudinal Tensile Forces (LTF), as well as the breaking distance of trains and to understand the influence of technical parameters or operating conditions.

The deliverable D3.1 [21] provides a comparison between the results coming from TrainDy simulations and the measurements of in-train forces made during experimental tests (May 2019 by FFL4E). The TrainDy results are consistent with the experimental measurements, as reported in D3.1.

2.9.2 Preliminary simulations on the Demonstrator(s)

2.9.3 Relative Approach

Deliverable D3.3 [22] takes up on the results coming from above preliminary studies and is focused on the Longitudinal Train Dynamics of a train family equipped by the DPS system based on LTE radio communication, compared with ones of a train family already admitted to the traffic.

The relative approach envisaged by UIC Leaflet 421 [11] has been followed. Two train families are assessed in terms of Longitudinal Train Dynamics (LTD): a "Reference system", i.e. trains family already admitted to the traffic on the track selected for the tests; a "New system", i.e. trains family with TUs equipped by the DPS system. The new and Reference trains families are identical, since the types of wagons and their payloads are the same, except for the "technology" employed on the TU and for the number of "active" TU (i.e. a TU having its electronic part habilitated, otherwise it behaves as a wagon).

The Longitudinal Compressive Forces (LCF) and Longitudinal Tensile Forces (LTF) have been evaluated by LTD simulations for the new and Reference train families under different operative conditions (i.e. different train operations or manoeuvres and different track positions). The results for the new and Reference train families (obtained under the same condition) have been compared.

In case the longitudinal compressive forces of the new system are worse than the Reference system (this happens only in some "degraded" modes), it has been shown that longitudinal forces are not higher than ones estimated for other operational conditions (in "nominal" mode) where New system performs better than the Reference one, and anyway LCFs do not exceed 400 kN which is considered a safe value for Longitudinal Compressive Forces according to UIC Leaflet 421 [11].

2.9.4 Train Consists for LTD simulations

At the time of the preparation of deliverable D3.3, the final train consist was not yet decided; therefore, the analysis has been based on statistic virtual trains. Each train family is made of trains having length between 720 and 740 m (TU included) and hauled mass between 1800 and 1850 ton. Each family is made of 100 trains generated according to UIC Leaflet 421 [11]. The algorithm used to generate virtual trains is described in the appendix C of the deliverable D3.1 [21]. Trains are randomized in terms of wagon type and load distribution, within boundaries given by the existing trains running on the test track. Trains database has been provided by DB Systemtechnik, considering trains running on the railway test track (see §1.5.2).

LTD simulations have been developed (in D3.3) for the following train families:

- train family without DPS, with 2 TUs, one at each end of the consist, called "Reference train family";
- DPS train families with 2 TUs, one placed at each end of the consist;
- DPS train family with 2 TUs, one placed in front and a second one in the middle of the consist;
- DPS train family with 3 TUs, one at each end of the consist and the third one in the middle.

A general configuration made by 3 TUs have been considered performing LTD simulations: one TU at the beginning, one at the end and one in the middle of the train. The above DPS train families are obtained by setting "activated" the different TUs (when the TU is not active it behaves as a wagon):

- LWL, i.e. active TUs are at the beginning and at the end, while TU in the middle is not active;
- LWLW, i.e. active TUs are at the beginning and in the middle, while TU at the end is not active;
- LWLWL, i.e. train consist in which all TU are active.

According to Figure 5, the train consist of the Reference train family is LWL; the train consists of DPS trains family are LWL, LWLW and LWLWL.

Figure 5 - Train consists

2.9.5 Trains modelling

Reference trains family modelling

In the Reference trains there are two Drivers, one for each active TU, communicating by themselves by dedicated provisions (i.e. independent of other train equipment).

The driver on the second TU supports driving the train by the application of traction and ED force and intervenes on the brake pipe in case of:

- an emergency brake is commanded by the driver on first TU; the delay between the command communicated by the first driver and the reaction of the second one (i.e. between the venting of brake pipe at the first TU and the venting of brake pipe at the second TU); is modelled by a random variable following a Gaussian distribution with mean value equal to 5 s and coefficient of variation equal to 0.1;
- an unexpected behaviour of the brake pipe pressure is recognized (even without any communication from the driver on first TU); in this (degraded) case, the emergency braking is actuated by the driver when the pressure on the second TU in brake pipe is equal or lower to 3.5 bar.

DPS trains family modelling

In general, in DPS train there is only one Driver at the first TU. The DPS system fills or vents the brake pipe upon proper command transferred by the radio communication. According to deliverable D2.1 [18], for LTE technology, the delay between the command (and filling/venting of brake pipe) at the leading TU and the filling/venting of brake pipe at guided TU is modelled by a Gaussian random variable, with a time interval 0.9 s +/- 15% (see §3.1.6.4). For each virtual train, this delay is randomly changed, and different among the two guided TU (if any) on each train.

The brake pipe of DPS train implements an independent way for the application of a distributed brake, acting as back-up of the radio communication between TUs. The DPS at the guided TUs monitors the pressure in the brake pipe and vents it when a pressure drop of 0.2 bar is detected, independently from the status of the communication. Venting of brake pipe can be:

- through a stepwise reduction of pressure in brake pipe (with target at 4.5 bar, 4 bar and 3.5 bar);
- or directly by a full-service braking with target pressure at 3.5 bar.

The first way has been proved to be more effective in D3.3.

2.9.6 Train Operational (simulated) scenarios

LTD of DPS trains have been studied under "nominal" conditions (e.g. with proper radio communication and safe behaviour of DPS equipment) and under "degraded" conditions due to the loss of radio communication and to hazardous failures of DPS equipment. Ten Train operational scenarios considered in the LTD studies have been identified jointly with FR8RAIL II Partners, also based on results coming from the safety analyses.

The first four Train operational scenarios refer to planar straight railway track and DPS in nominal conditions, i.e. radio communication between TUs is available and DPS properly works:

- #1 - Train acceleration and then coasting (cruising);
- #2 - Full-service braking from coasting (cruising);
- #3 - Emergency braking from coasting (cruising);
- #4 - Train acceleration followed by an emergency braking.

The remaining scenarios refer to degraded conditions due to the loss of communication between TUs. Two train operational scenarios refer to the loss of radio communication between TUs before a new command is issued by the leading TU:

- #5 - Train is accelerating, the radio link is down (DPS on guided TU reacts after "time of radio communication loss"), and then the leading TU issues a braking.
- #6 - Train is braking (ED is activated), the radio link is down (DPS on guided TU reacts after "time of radio communication loss"), then the leading TU issues a "stronger" braking to stop the train; this scenario is meaningful on a downhill;

Three further train operational scenarios refer to the loss of radio communication between TUs *when* (i.e. in the same moment) a new command is issued by the leading TU:

- #7 and #8 - Train is braking (ED is activated), then the leading TU issues a "stronger" braking (full-service braking for #7 and emergency braking for #8) to stop the train and the radio link is down; DPS on guided TU reacts when it detects a pressure drop of 0.2 bar in brake pipe;
- #9 - Train is accelerating, then the leading TU issues an emergency to stop the train and the radio link is down; DPS on guided TU reacts when it detects a pressure drop of 0.2 bar in brake pipe.

The last scenario refers to the loss of radio communication between TUs when an emergency braking is commanded by the guided TU for any reason (e.g. fire on board):

- #10 -Train is running at a certain speed and an emergency braking is commanded by the guided TU and the radio link is down.

Further remarks on LTD simulations (made in the deliverable D3.3) are provided in the following:

- train speed (reached after acceleration in some scenarios) is 30 km/h for simulations focused on the in-train longitudinal forces (being more relevant at low train speed) and (up to) 100 km/h for simulations focused on the stopping distance (that increase with train speed);
- the maximum braking force is applied by all wagons and the maximum traction forces force is applied by all TUs (except when differently assumed, as for train-consist LWLWL);

- for LWLWL, only the 67% of maximum power is applied to provide the system with approximately the same amount of energy of the other train consists (with only two TU);
- the maximum braking force is applied by all wagons and the maximum traction forces force is applied by all TUs, based on the general considerations that if the traction forces are lower than the maximum values, the LTD is less enhanced; indeed, the train acceleration energizes the train in terms of kinetic energy (train speed) and potential energy (draw gears elongation), while during braking, the braking devices and the couplings dissipate/transform such energy; if the initial potential energy (but not the train speed) is increased by an higher traction force, the energy dissipation requires a higher deformation of buffers and draw gears, and this results in (usually) higher longitudinal forces;
- for each train family, the discussed statistics is the sum ($\mu \pm 3\ \sigma$) of the average (μ) longitudinal force plus or minus three times standard deviation (σ), to cover the around the 99.7% of cases (assuming Gaussian distribution); the minus sign is used for LCF, while plus sign is used for LTF;
- for train-consist LWLWL, it is assumed that the communication loss occurs on all Tus, which is considered more dangerous than the communication loss just on one TU.

Each train operational scenario has been simulated for DPS train family and for Reference train family.

The most relevant uncertain technical parameters affecting the Longitudinal Train Dynamics have been selected (in D2.2) and considered (in D3.3) during the generation of the virtual train consists, by sampling values and setting the technical parameters for each wagon of the Reference and DPS trains families.

2.9.7 Additional LTD studies

Additional LTD simulations have been performed in order to assess the longitudinal forces on trains over uphill/downhill railway track and to address (through parametric studies) the effect on LTD of wagons with LL shoes, of time interval for radio communication loss, and of two possible reactions of DPS when a pressure drop in the Brake pipe is detected.

2.9.7.1 LTD studies on uphill/downhill railway track

LTD studies have been performed during the M2O project both on planar track (D3.1) and on up/down hill track (D3.3, which considers also planar track as well).

The focus of LTD studies was on DPS trains family (including the Demonstrator(s)) envisaged to run on a defined infrastructure, characterized by a maximum slope equal 27‰, as for the test track (see §1.5.2).

Train operations have been simulated at different positions, with the highest gradients along the track between Kronach and Probstzella (in order to emphasize the effects on longitudinal train dynamics) as shown in Figure 6.

Points on the test track with maximum gradient (influencing the in-train longitudinal force) are identified and considered in the LTD simulations, for different degraded operating modes and manoeuvres: "UD" (Up/Down) for manoeuvres involving traction, "DF" (Down/Flat) for manoeuvres involving braking.

For each train operation, five representative points are chosen in the nearby of UD and DF (with a distance between them of around 150 m). In general, the likelihood of a traction application is bigger on an uphill and the likelihood of a braking (electrodynamic or electrodynamic + pneumatic) is bigger on downhill.

LTD simulations have been performed considering up and down-hill, for the train operational scenarios #5 and #9 (most hazardous ones on a planar track and emphasizing LTD around "UD") and #6 (emphasizing LTD around "DF").

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

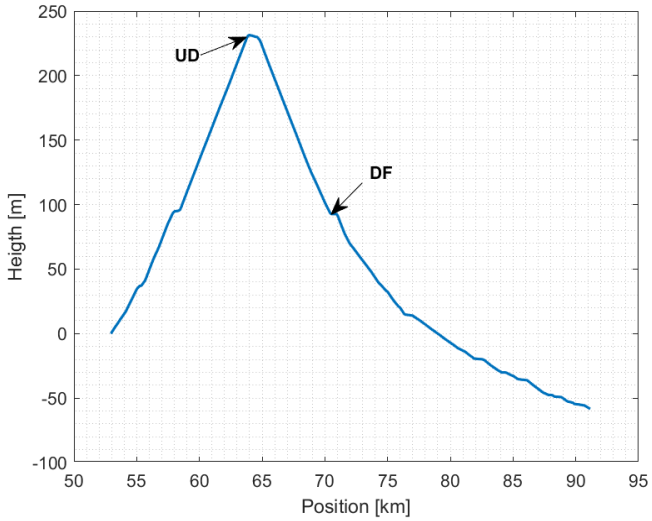


Figure 6 - Track with indication of the points UD and DF

2.9.7.2 Effect of wagons with LL shoes on LTD

Since there is a transition from cast iron to LL shoes, a parametric study is performed considering a variation of wagons equipped by LL shoe from 0% (i.e. all wagons are equipped by cast iron shoe) to 100 % (i.e. all wagons are equipped by LL shoe).

Simulations have been performed for LWLW train consist (with higher values of longitudinal force with respect to other train consists), considering a train acceleration followed by an emergency brake (worst train operational scenario, from LTD perspective, under normal operation).

2.9.7.3 Time of radio communication loss for automatic TU intervention

Standard DPS settings impose a traction removal that is modelled with a gradient of 60 kN/s when the time interval of communication loss equal to 2.5 s is reached. The parametric study is performed changing the time interval from 1.5 s to 10 s.

2.9.7.4 Stepwise reduction of pressure vs full-service braking

Two different options have been considered as reaction of the guided TU of DPS train to the detection of the brake pipe pressure drop (0.2 bar): Full-service braking and Stepwise pressure reduction.

The results of a preliminary simulation (provided in D3.1 [21]) have shown that if the DPS reacts performing a full-service braking when the pressure drops by 0.2 bar at the guided TU, because of an emergency brake triggered by the leading TU during a communication loss, is generally better than performing a stepwise pressure reduction, under the same conditions.

However, additional studies (provided in D3.3 [22]) have been performed addressing and comparing longitudinal forces for the two options, when the leading TU performs a first-application step braking (target pressure in brake pipe is 4.5 bar) from a full acceleration condition, and the radio communication is lost at the same time. These studies have proved that in above conditions, the stepwise pressure reduction provides lower in-train forces; moreover, other simulations reported in D3.3 have proved that the benefits of a full-service braking are minor with respect to stepwise pressure reduction.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

3 Technical Safety Report

The "Technical Safety Report" of the Safety Case has the main purpose to provide technical evidence of the DPS train fail-safe design and reference to the documents where evidence of the V&V activity is provided.

The present chapter is structured in the following main paragraphs:

- Assurance of Correct Functional Operation - it concerns the correct functioning (i.e. the expected behaviour) of DPS train under normal condition as specified in the functional and safety requirements;
- Effects of Faults - it concerns the expected behaviour of DPS train under faulted condition, i.e. the fulfilment of the safety requirements defining means for faults detection and following (re)actions;

  Operation with External Influences - it concerns the achievement of the functional and safety requirements against external influences;
- Safety-related Application Conditions - it concerns the mitigations that must be satisfied to assure the functioning of the system according to the functional and safety requirements.

3.1 Assurance of Correct Functional Operation

3.1.1 System Architecture Description

Figure 7 provides a high level representation of the DPS train architecture, which has been taken into account in the developement of the Interface Hazard Analysis (see §2.4.3). The existing and new interfaces related to the implementation of DPS equipment/functions are represented by red arrows. The existing interfaces, working as for conventional trains, are represented by black arrows if "active", grey otherwise.

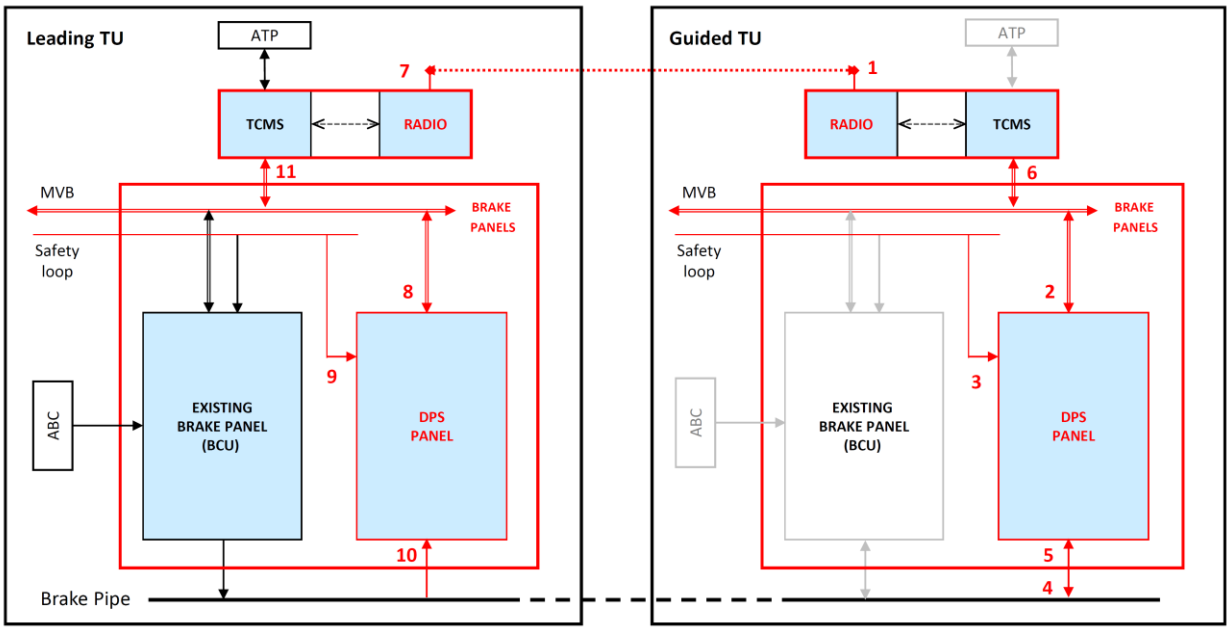


Figure 7 - DPS Train, main subsystems and internal Interface

3.1.2 Definition of Interfaces

Table 8 provides the list of (internal) interfaces between the above DPS Train subsystems that are singularly addressed by the IHA. Each interface is identified (by the identifier used in Figure 1). Main data/signals exchanged are specified in Table 8 for each interface and singularly addressed.

Interface		Main data / signals
1	TCMS L→ TCMS G	LG - Radio connection Status
		LG - Number / position of traction units
		LG - Distributed power switched on
		LG - Traction unit orientation
		LG - Traction request to set level
		LG - Service brake request to set level
		LG - Traction cut off command
		LG - Emergency brake command
		LG - Brake release command
		LG - Parking brake command
		LG - Selection of the network voltage / pantograph
		LG - Emergency pantograph fall down / opening of the circuit breaker
2	TCMS G→ BRAKE PANELS G	Distributed power switched on
		Communication ok
		Number / position of traction units
		Brake pipe vent command
3	SAFETY LOOP G → BRAKE PANELS G	Traction unit Safety loop1 / Safety loop2
4	BRAKE PANELS G → BRAKE PIPE	BP pressure setting / venting
5	BRAKE PIPE → BRAKE PANELS G	Brake pipe pressure from transducer#1 / transducer#2
6	BRAKE PANELS G → TCMS G	Unexpected brake pipe pressure reduction
		Emergency brake request
		DPS Brake status / Brake pipe pressure
7	TCMS G→ TCMS L	GL - Traction unit orientation
		GL - Radio connection Status
		GL - Emergency brake request
		GL - Traction apply report
		GL - Brake status / Brake pipe pressure reports
		GL - Air flow / Main reservoir pressure reports
		GL - Alarms (e.g. Fire, Motor temperature)
		GL - Selected network voltage / pantograph
		GL - Pantograph / Main circuit status report
8	TCMS L→ BRAKE PANELS L	Distributed power switched on
		Communication ok
		Number / position of traction units
9	SAFETY LOOP L → BRAKE PANELS L	Traction unit Safety loop1 / Safety loop2
10	BRAKE PIPE → BRAKE PANELS L	Brake pipe pressure from transducer#1 / transducer#2
11	BRAKE PANELS L → TCMS L	Traction interlock request
		Emergency brake command
		Service brake request to set level

Table 8 - Mitigations from the DPS train Hazard Analysis

3.1.3 Hazard Identification

The hazardous conditions related to the specific characteristics of DPS train (as defined for the PHA in §2.4.1) and to the functions implemented by DPS train (as defined in §1.4.2).

Table 9 provides the hierarchical list of hazards identified by means of the safety analyses performed during the M2O project, univocally identified. Fourteen "Macro hazards" are identified; some of them are decomposed into lower-level "Specific hazards", detailing the hazardous condition. The table also specifies the consequent accident for each Macro hazard (introduced in Table 5).

The identified hazards are recorded in the Hazard Log (Annex of the deliverable D2.3 [20]).

Some hazards were initially defined and then not included in the list because no relevant difference was identified from "conventional" applications, e.g.: changes in wheel contact forces, wheel profiles or distance between wheels; loss of integrity of train/track parts assuring train guidance capability; weather conditions affecting the adhesion between rail and wheels; contact with hazardous voltage, sharp edges, hot surfaces, slipping surfaces; vehicle movements beyond dynamic envelops; undue train movement to an incapacitated driver (not detected).

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard	
H_1	**Impaired (or lost) train running stability**	A_4	Derailment / Overturning of the train
H_1_1	**Increase of vehicle axle load**		
H_1_2	**Long bridges with excessive cross winds**		
H_1_3	**Long bridges with hazardous dynamic behaviour** (i.e. natural frequencies coupled with vibrations induced by trains)		
H_1_4	**Excessive overall mass of DPS train brake with respect to the infrastructure**		
H_1_5	**Excessive longitudinal forces transmitted to the infrastructure** due to the brake application by DPS train.		
H_2	**Interference between train and loading gauge due to changes in train shape**	A_2	Collision of the train with / damage to infrastructure
H_3	**Impaired (or lost) coupling between train units**	A_5	Cut of the train (separation)
H_3_1	**Loss of integrity of coupling** between units (Traction units or wagons)		
H_3_2	**Excessive stretch length** after stopping of the train due to distributed traction/braking		
H_4	**Excessive longitudinal forces between train units**	A_4	Derailment / Overturning of the train
		A_5	Cut of the train (separation)
H_4_1	Excessive in-train longitudinal forces **due to the distributed traction and braking performance**		
H_4_2	Excessive in-train longitudinal forces **due to specific track characteristics**		
H_4_3	Excessive in-train longitudinal forces **due to specific maneuver**		
H_4_4	Excessive in-train longitudinal forces **due to specific distribution of loads over wagons**		

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard	
H_5	**Excessive train braking distances or speed**	A_1	Collision between trains (rear, side, head-on)
		A_2	Collision of the train with / damage to infrastructure
		A_3	Collision of the train with obstacle (persons, animals, road vehicles)
		A_4	Derailment / Overturning of the train
H_5_1	Excessive train braking distances or speed **due to an impaired (or lost) braking capability**		
H_5_2	Excessive train braking distances or speed **due to an excessive timing of reaction for braking application**		
H_5_3	Excessive train braking distances or speed **due to distributed traction and braking performance**		
H_5_4	Excessive train speed **due to an undue release of brakes**		
H_5_5	**Temporary speed restriction not fulfilled with the whole length of the train**		
H_5_6	**Missed / ineffective reduction of the train speed by the driver** (acting on traction and brake).		
H_6	**Undue train braking or train unduly immobilized**	A_6	Other accidents (Electrocution, Burns, Asphyxia, Suffocation, Poisoning, Contamination, Fire, Explosion)
H_7	**Undue train movement**	A_1	Collision between trains (rear, side, head-on)
		A_2	Collision of the train with / damage to infrastructure
		A_3	Collision of the train with obstacle (persons, animals, road vehicles)
H_7_1	Undue train movement due to a **failure / undue release of parking or holding brake**		
H_7_2	Undue train movement due to a **shunting operation made by the driver**		
H_7_3	Undue train movement **in an area where shunting is not allowed**		
H_8	**Damage to overhead contact line (catenary) and/or trainborne power supply equipment**	A_2	Collision of the train with / damage to infrastructure
H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to **incorrect selection of pantograph(s)**		
H_8_2	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to an **incorrect management of power supply equipment** (i.e. opening and closing of the main circuit breakers and/or lowering and arising of pantograph(s))		
H_9	**Incorrect detection of track occupancy/clearance**	A_1	Collision between trains (rear, side, head-on)
H_9_1	**Incorrect detection of track occupancy/clearance due to a too high number of block sections simultaneously occupied by a train, to be managed by the interlocking central logic**		

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard	
H_9_2	**Incorrect detection of track occupancy/clearance due to a too high number of axles of a single train to be counted** (by axle-counter, if applicable)		
H_10	**Hazardous operation of train/maintenance staff**	All accident	
H_10_1	**Incorrect (unsafe) train composition or configuration due to staff error**		
H_10_2	**Intendent change of train configuration data by staff during operation**		
H_10_3	Unsafe maneuver of the train, due to a **wrong orientation**		
H_10_4	**Unsafe maneuver of the driver**, which does not remember the received prescriptions after a long train stop or after driver change		
H_10_5	**Unsafe management of train equipment in the crossing of neutral section due to staff error**		
H_10_6	**Improper use of compressor to restore the minimum pressure in the main air reservoir**		
H_10_7	**Unsafe condition of the train after end-of mission due to staff error**		
H_11	**Interference with track-side equipment**	All accident	
H_11_1	The **distance between a main signal and a critical points** (e.g. switch point, level crossing, hotbox-detector, balises providing protective messages **is too short to host the train.**		
H_11_2	**A main signal stop the train with the pantograph of the guided Traction units under a neutral section** of the catenary (preventing contribution to traction)		
H_11_3	The **braking distance is too long to stop the train at the first main signal after a Hotbox-detector**.		
H_11_4	**New switch points** (e.g. introduced to allow shunting movement and stop of DPS train) **are not taken into account by the interlocking central logic**		
H_11_5	**Level crossing unduly switched on** before the full passage of the end of the train		
H_11_6	**Switch point unduly maneuvered or released or** before the full passage of the end of the train.		
H_12	**Train misrouted on a wrong (non-adequate) line**	All accident	
H_13	**Ineffective DPS train initial tests**	All accident	
H_13_1	**Missed or incomplete execution** of DPS train initial tests		
H_13_2	**Incorrect execution** of DPS train initial tests		
H_14	**Other hazardous conditions on train**	A_4	Derailment / Overturning of the train
H_14_1	**Fire on-board** during train run		
H_14_2	**Operational relevant failures and disturbances** during train run		

Table 9 - List of Hazards

3.1.4 Safety Integrity level

Table 10 provides the specific set of mitigations that has been specified by the safety analyses (documented in the deliverable D2.3 [20]), concerning the Safety Integrity required to each function implemented by DPS train (see Table 2).

ID	Description
SIL_MIT_01	The **Communication between Traction units** shall be implemented by DPS train with a **Low Safety integrity level,** in compliance with the standards on safety-related electronic systems for signaling (EN 50129), on software for railway control and protection systems (EN 50128) and on safety-related communication in transmission systems (EN50159).
SIL_MIT_02	The **Air management** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_03	The **Energy management** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_04	**Diagnostic** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_05	The **System de-activation** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_06	The **Traction management** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_07	The **Train inauguration & configuration** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_08	The **Train initial test** shall be implemented by DPS train with a **Low Safety integrity level,** in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_09	The **Train operational status** management shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_10	The **Service brake management** shall be implemented by DPS train with a **Low Safety integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_11	The **Emergency brake management** shall be implemented by DPS train with a **High Safety Integrity level,** in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_12	The **Parking Brake management** shall be implemented by DPS train with a **High Safety Integrity level**, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).
SIL_MIT_13	The **Automatic Train Protection management** shall be implemented by DPS train with a **High Safety Integrity leve**l, in compliance with the standards on safety-related electronic systems for signaling (EN 50129) and on software for railway control and protection systems (EN 50128).

Table 10 - Safety Integrity Level required to DPS Train functions

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

3.1.5 Safety Concept

The safety concept of DPS trains is consistent with the Safety Integrity Level allocation stated in Table 10.

Low safety integrity functions are be implemented by SIL1/SIL2 Train's equipment (as for conventional train) at each Traction unit and by the (Low safety integrity) radio communication between the leading TU and each guided TU, involving the (SIL2) TCMS and the non-trusted communication system (radio equipment and LTE-network, see §3.1.6.1). It applies to the functions required for the DPS train set-up (i.e. train inauguration and configuration and train initial tests), to the energy management and Diagnostics, and to the remote control of traction and service brake at the guided Traction units.

The implementation of a Low safety integrity radio communication requires the use of a proper safety layer (SDTv2 has been selected) and developments of the equipment (TCMS) operating on the application data guarantying the same safety integrity (see §3.1.6.3). The use of an open transmission system requires the implementation of provision for a secure exchange of data, even if test runs are limited in space and time, and the full development for future commercial implementation of DPS trains is out the scope of the activities (see §3.1.6.2).

Operational procedures are identified as additional mitigations (requiring specific instruction to the driver, performing checks and confirmation), to reduce risk to an acceptable level (see §3.4).

Concerning DPS train Demonstrators, because of the lack of evidence from safety validation, each guided Traction unit shall be manned and specific instruction shall be specified for the staff about checks to be perform and confirmation to be provided to the driver (at the leading Traction unit) during the train set-up (see §3.4).

High safety integrity functions are implemented by SIL3/4 trains equipment involving:

- the interface with ATP (normally operating at the leading TU and in Sleeping mode at each guided TU);
- the Parking brake (implemented as SIL4 functions or managed through operational procedure for the experimental test campaign);
- the Emergency brake, requiring the proper communication of the EB command from the leading to each Traction unit and behaviour of the DPS equipment.

In order to achieve an acceptable risk for the hazardous condition due to a (temporary) loss of communication (i.e. unavailable of the radio remote control) when an Emergency brake has to be applied, an independent mechanism for braking is implemented. It is based on the monitoring of the Brake pipe pressure at each (leading and guided) Traction unit and the reaction (stepwise or full service braking) at the detection of a defined pressure decrease, independently from the status of the radio communication.

In-train longitudinal forces experienced by DPS train are evaluated under different operative conditions (i.e. different train manoeuvres and track positions), considering the radio communication performance (see §3.1.6.4) and its potential unavailability, and compared with ones experienced by trains already admitted to the traffic on the test track (see §2.9.3). As main result coming from LTD simulations (see §2.9, §3.1.8, §3.2.4 and Appendix A), DPS train Demonstrators experience longitudinal forces and breaking distance not higher than for Reference trains (already admitted to the traffic on the track selected for the tests) or anyway acceptable. For the specific configuration of the DPS train Demonstrators, this applies also in case of concurrent loss of radio communication between the Traction units (TUs) and hazardous failure of DPS at the guided TUs (in the monitoring of the Brake pipe pressure and breaking assistance). Therefore, no specific action is required to personnel attending the guided TUs concerning brake application.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

3.1.6 Communication between Traction units

The developed Distributed Power System (DPS) allows implementing multiple traction through radio communication between the Traction units. The communication concept, the provisions for a secure and safe communication and the achievable performance are discussed in the following sections.

3.1.6.1 Communication concept

DPS implementation aims at increasing the train length of freight trains by distributing additional Traction units (from one to four) throughout the (same) train consist. As there is no electrical connection available to remote control the guided Traction units (in the middle or at the end of the freight train), a wireless connection is established.

The vehicles communication related to on-board and radio transmission is illustrated in Figure 8 [16], [18].

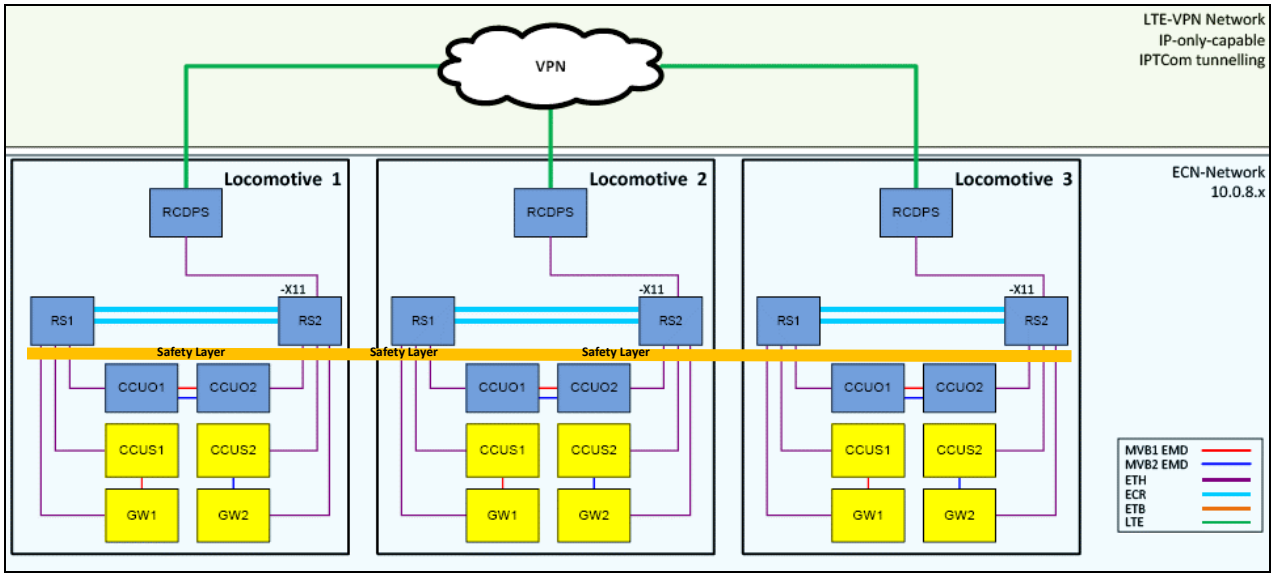


Figure 8 - Overview of vehicle communication - based on LTE / IP

The exchange of data between the leading and guided Traction units is based on IPTCom communication over LTE-Network, implemented by the on-board Radio Controller for Distributed power system (RCDPS).

At each Traction unit, RCDPS acts as transparent gateway from the wired vehicle network to the wireless LTE-Network. It establishes the LTE-connection to the specific Virtual Private Network (see §3.1.6.2), provides a transparent channel for safe communication (see §3.1.6.3), is controlled via a "Control-Telegram" from the Application (Vehicle control computer, CCUO) and provides status-telegrams.

According to the deliverable D2.1 [18], LTE[1] has been selected mainly because point to multipoint communication is possible, IP communication can be used instead of proprietary communication protocol, low latency communication is introduced by network elements.

The communication performance (see §3.1.6.4) is assessed in the deliverable D2.1 [18] and accounted for the LTD simulation (see §2.9.5).

[1] LTE is a bridge technology to 5G (change over is expected to be a short step. The technology used by the RCDPS is replaceable (4G or 5G can be used).

3.1.6.2 Secure Communication Concept

The following (technological-neutral) mitigation is specified during the safety analyses to implement a safe radio communication between the Traction units.

The radio communication between the leading and guided Traction units of DPS train shall comply with the standards on safety-related communication in open transmission system (EN 50159) and be protected against masqueraded messages, unauthorized access, intentional takeover of the control through unauthorized third parties and intentional disturbances of radio signals (jamming), e.g. establishing the connection by a secure exchange of pairing keys based on the UIC vehicle numbers. (HA_MIT_11)

To assure an adequate degree of security in the radio communication between the Traction units of DPS train, data are exchanged through a Virtual Private Network (VPN) and private Access Point Name (APN) is used to separate the data traffic from other public mobiles, avoiding routing via Internet and without end-to-end encryption of the data traffic.

After checking the coverage by LTE along the test track, the Vodafone network has been selected for the execution of test runs. MDEX corporation has been selected as the VPN provider for connecting LTE subscribers to each other. The private APN provided by MDEX is widely used for Machine-to-machine communication and include cyber security provisions. The concept is to isolate the mobile to ground traffic form other customers and route this traffic to an encrypted VP to a corporate network.

On train, network security is ensured by the RCDPS, which manages the VPN access credentials and the wireless connectivity (configurable via separate interface).

Due to a limitation in the integration of the Vodafone network into the VPN of MDEX, no "direct" data exchange between the mobile participants is possible. This is solved by a dedicated software that receives data from the mobile participants in a Control Center tunnel and sends it on. The communication between mobiles is only enabled by the Control Center. This makes it possible to enforce traffic rules and to monitor and record the entire data traffic centrally and live.

As shown in Figure 9, the mobile participants (RCDPS) are configured to send their data via UDP to the IP address of the Control Center tunnel. The Control Center software distributes data according to the registered mobile participants. Traffic is only forwarded to Traction Unit which are registered to the same Train Number. No direct IP routing is established between the traction vehicles.

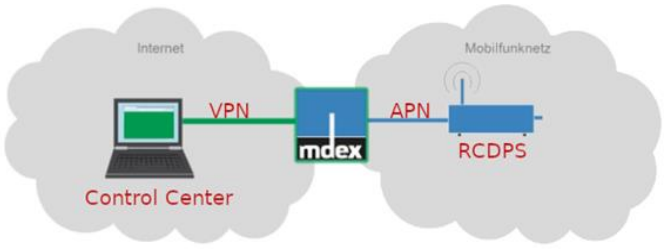


Figure 9 - Private Network (left side: VPN over Internet; right side: private APN access)

The software for the Control Center tunnel used for test runs is executed at the Funkwerk Systems GmbH site in Kölleda. It establishes a connection via OpenVPN tunnel over Internet to VPN provider MDEX.

Anyway, no definitive evidence is available on the robustness of the above security provisions, if/when the LTE network is used for DPS trains commercial use (extended in time and space).

3.1.6.3 Safe Communication Concept

EN 50159 [7] specifies the communication-related requirements for functional and technical safety. Safety requirements are usually implemented in the safety-related equipment, designed and validated according to EN 50129 [7]. Besides the source and destination of safety-related communication, the reference architecture deals with a non safety-related ("black channel"), open transmission system, including provisions for transmission and access protection. The following (technological-neutral) mitigations are specified to implement a safe radio communication between the Traction units.

The leading Traction unit of DPS train shall send commands to all the connected guided Traction units by means of cyclic process data. (HA_MIT_10)

The radio communication between the leading and guided Traction units of DPS train shall comply with the standard for safety-related communication in open transmission system (EN 50159) and based on a Safety Layer providing measures against communication threats (messages corruption, resequencing, repetition, insertion), managed by devices compliant with the standard for safety-related electronic systems for signaling (EN 50129). (HA_MIT_14)

The Safe Data Transmission version 2 (SDTv2) safety layer is adopted for the communication between the Traction units [16]. SDTv2 is an end-to-end protocol allowing the transmission of safety related data between a safe data source and many safe data sinks, over an untrusted communication channel (independently from the network technology, e.g. GSM-R and LTE), for safety functions up to SIL2. SDT, defined by IEC 61375-2-3 ([10], Annex B), fulfils IEC 62280 [8] (based on EN 50159 [7]) and support the transmission of safety related data between a safe data source and or many safe data sinks.

3.1.6.4 Radio communication performance

Latency in the radio communication between Traction units has potential on train behaviour, when brake application is required during train run. Specifically, the time required for radio communication introduces delay between the venting of the train brake pipe at the leading Traction unit and the venting of the brake pipe at each guided Traction unit; excessive latency could reduce the effectiveness of the braking action, with increase of the train stopping distances, and/or increase longitudinal forces between units. A model of the processing and transmission of data on the traction vehicles and between the cars has been developed for latency calculation. The end-to-end calculation cover the local processing and transmission time on Loco1, on LTE network and on Loco2. Specifically:

- the Loco1 contribution includes the CCUxx processing and transmission times, the LAN/network transmission time between network nodes, and the RCDPS receiving and processing times;
- the LTE-network contribution includes the Transmission time to base station (upload), the Processing time, and the Receiving from the base station (download);
- the Loco2 contribution includes the RCDPS processing and transmission times, the LAN/network transmission time between network nodes, and CCUxx receiving and processing times.

Latency between Train Controller Unit and Radio Controller (RCDPS) for both TU's (end-to-end with radio communication) is estimated by laboratory test to be 390 ms (+/- 15%). Laboratory performance test made on GSM-R was validated by the test run (during 2019), resulting in an additional 0.5 s; the same value is used for LTE, waiting for experimental data coming from FR8RAIL II experimental tests. Consistently, in the modelling of DPS trains family based on LTE technology (§2.9.5), 0.9 s +/- 15%[2] (first contribution rounded up) is used for the delay between the command at the leading TU and its actuation at guided TU.

[2] Specified as "system wide latency (driver at leading TU … brake pipe valve of guided TU" in the deliverable D2.1 [18].

3.1.7 Fulfilment of Safety requirements specification

The Appendix B provides the safety requirements specified during the safety analyses (see §2.4), to be verified for each specific application of DPS train, and details on the strategy for the validation of the DPS train Demonstrator(s), set for the execution of the experimental test campaign introduced in §1.5. For each applicable requirement, it specifies the activities to be finalized before test runs and the sources of the evidence that safety-related requirements are specified, implemented and verified to be collected. Table 18 concerns the Technical and Contextual safety requirements. Table 17 concerns the Safety functional requirements.

The expected functional behaviour of DPS train is described in the following sections through the functional safety requirements specified during the safety analyses (see §2.4).

3.1.7.1 Safety requirements for DPS train initial set-up

The following safety requirements have been specified during safety analyses for the DPS train initial set-up. They describe the expected behaviour in the Communication set-up, Train inauguration & configuration and execution of Train initial test. The Safety Integrity Level allocated to the functions carried out by DPS Train according to §2.6 (see Table 10) is propagated to the related functional requirements. In the following, "High SIL" is specified for requirements having a High Safety Integrity; Low Safety Integrity applies to the remaining functional safety requirements (without explicit indication).

Each Traction unit of DPS train shall be identified during the train inauguration and configuration through a unique identifier (e.g. UIC-train number). (HA_MIT_02)

DPS Train shall guarantee the integrity of train configuration data and make impossible any change after a valid Start of mission. (HA_MIT_04)

Before the DPS train departure, the leading Traction unit shall communicate (by radio) to all the guided Traction units the orientation set by the driver (at the first set and at any change). Each guided Traction unit shall communicate (by radio) to the leading Traction unit the set train orientation, for the Driver acknowledgment. Otherwise (if the acknowledgment process is not implemented or not possible, e.g. in case of permanent loss of radio communication), a specific test shall be performed before the train departure in order to verify that all the Traction units have a coherent orientation (at the first set and at any change), e.g. by staff verifying the orientation set at the different Traction unit or by operating a small movement of the train. (HA_MIT_09)

After DPS train inauguration, the train run shall be possible only in case of: complete set of valid configuration data, acknowledged by the Driver AND positive results from checks of diagnostic function(s) AND positive results from valid Train Initial tests, acknowledged by the Driver AND consistent train orientation at different Traction units, acknowledged by the Driver. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition. (HA_MIT_03)

The DPS switch-off and the unavailability of power supply for train equipment shall lead to a safe state by the: reset the train inauguration (new train inauguration shall be performed in case of DPS switch-on); inhibition of the remote (i.e. by radio) control through the termination of radio communication between the Traction units; brake application in order to maintain or to put the train at standstill condition. (HA_MIT_16)

3.1.7.2 Safety requirements for DPS train run

The following safety requirements have been specified during safety analyses, describing the correct functional operation during the DPS train run. They describe the expected behaviour in the Communication between Traction units, Traction, Pneumatic (Emergency) brake, Parking brake, Energy, Automatic Train Protection management. The Safety Integrity Level allocated to the DPS Train functions (see Table 10) is propagated to the related functional requirements.

Traction management

Each Traction unit of DPS train shall guarantee that traction is cut off when brake is applied or brake application is commanded. (HA_MIT_25)

After that a traction cut-off command is received from the leading Traction unit of DPS Train, each guided Traction unit shall maintain the traction cut-off until the release command is received from the leading Traction unit. (HA_MIT_17)

Each Traction unit of DPS Train shall limit the traction and dynamic brake forces to the maximum values specified for the specific application. (HA_MIT_18)

Pneumatic (Emergency) brake management

The Leading Traction unit of a DPS train shall send an emergency brake command to all the guided Traction units (to guarantee the continuity of the brake) and vent the brake pipe (i.e. actuate an Emergency brake) in case of request generated by the driver, OR by the safety loop and protection systems in the leading Traction unit, OR by a EB request coming from a guided Traction unit. (HA_MIT_27, High SIL)

The Leading Traction unit of a DPS train shall apply the Emergency brake (when required) by venting the brake pipe independently from the status of radio communication and from the generation of the command to the guided Traction units. (HA_MIT_28, High SIL)

The guided Traction units of DPS train shall vent the brake pipe when the emergency brake command is received via radio communication from the leading Traction unit. (HA_MIT_22, High SIL)

The guided Traction units of DPS train, in case of detection of any condition requiring the train stop (i.e. under which conventional train apply EB up to train standstill), shall cut off the traction, vent the brake pipe and communicate the Emergency brake request to the leading Traction unit). (HA_MIT_29, High SIL for BP venting)

Parking brake management

DPS Train shall guarantee the Parking brake application (assuring the standstill condition), specifically during the Train initial test, as for conventional trains. (HA_MIT_01, High SIL) The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition. (HA_MIT_46, High SIL)

Energy management

The leading Traction unit of DPS train shall send to the guided Traction units the information on the network system and voltage introduced by the driver and used for the selection of its pantograph and shall verify the consistency of the pantograph selected by the guided Traction unit. (HA_MIT_32)

The guided Traction units of DPS train shall select the pantograph to be used according to the applicable network and voltage system and shall communicate to the leading Traction unit the selected pantograph. (HA_MIT_34)

Automatic Train Protection management

The On-board ATP of each guided Traction unit in DPS train shall be in an operating mode (e.g. ERTM/ETCS Sleeping mode) guarantying that no train movement supervision is performed. (HA_MIT_36) The leading Traction units shall guarantee the consistency between the information (movement authority, speed restriction, emergency brake) acquired from the trackside signaling (ATP) system and the remote controls provided to the guided Traction units to implement a distributed traction and braking. (HA_MIT_35)

The radio communication between the Traction units of DPS train shall not influence and not be influenced by the radio communication between the on-board and track-side ATP equipment (HA_MIT_37)

3.1.8 LTD simulations under correct functional operation

Among the results coming from the safety analyses (see §2.4), some mitigations concern the development of LTD simulations, to be performed for each class of specific applications.

For each class of specific applications, it shall be verified that the in-train longitudinal forces in DPS train are acceptable (compared to absolute limits or to a Reference train configuration already authorized for operation) in all the conditions defined by the train configuration (position of Traction units and loaded wagons), credible degraded operating modes (interruption of radio communication), train manoeuvres (traction, brake, particular operations), and track characteristics (e.g. maximum track gradient). Unsafe Train configurations (i.e. distribution of loaded wagons) shall be identified (if any) by simulations of in-train longitudinal forces and braking distance of DPS trains. (PHA_MIT_15)

For each class of specific application, train equipment (braking system in each Traction unit) shall guarantee the application of brake forces consistently with the operational status and the commands received. The acceptability of degraded conditions (due to failures leading to a reduction of the braking effort), if defined, shall be verified by simulations of in-train longitudinal forces and braking distance. (PHA_MIT_16)

For each class of specific applications, it shall be verified that in-train longitudinal forces and braking distance of DPS trains are acceptable (compared to absolute limits or to a reference train configuration already authorized for operation), accounting for: the (worst case) time required for EB application, when a command generated by the control system is received by the brake system; the time needed to generate this command: a. worst case with radio on (includes performance of the control system and uncertainty on radio communication latency); b. worst case with radio off (includes performance of the control system, with the pressure sensors on the brake pipe). (PHA_MIT_17)

For each class of specific applications, if the effective brake (sum of dynamic and pneumatic braking contributions) could decrease in case of loss of the radio communication between the Traction units of DPS train, simulations shall demonstrate that (because of potential train acceleration) braking distance degradation and in-train longitudinal forces are still acceptable. The contribution of dynamic brake shall not be considered for the fulfilment of braking distance (if/as applicable). (PHA_MIT_18)

LTD simulations have been performed during the M2O project in order to comply with the above mitigations. A summary of the results coming from the LTD studies is provided in the following sections: §3.1.8.1 concerning the Preliminary simulations on the DPS trains family (compatible with Demonstrator(s)) and §3.1.8.2 concerning the specific simulations on the Demonstrator(s).

Additional results coming from the LTD studies concerning degraded conditions are provided in §3.2.4.

3.1.8.1 Preliminary LTD simulations under correct functional operation

According to the deliverable D3.3 [22], based on the results obtained by the preliminary LTD studies, DPS trains are usually better than the Reference trains.

As main result from the preliminary parametric study performed on the use of (LL and cast iron) shoes, the LCF are higher (both for Reference and DPS trains families) when the wagons are all equipped by LL shoes. Based on this result, all the LTD simulations (i.e. under different train operational scenarios) have been performed assuming that all wagons are equipped with LL shoes.

In planar straight railway track and under DPS nominal (i.e. failure-free) conditions (#1, #2 and #3 operational scenarios, reported in §2.9.6), the longitudinal forces for a full-service braking and an emergency braking are comparable. For this reason, next simulation scenarios (in degraded mode) consider just the emergency braking and not the full-service braking. The worst normal operation scenario, according to TrainDy simulations and FFL4E experimental measurements (from LTD perspective), is a train acceleration (up to 30 km/h) followed by an emergency brake (#4 operational scenario). Also in this case, DPS train families (all trains consists) are always better (i.e. safer) than the Reference system (i.e. 10 m^3 LCF of the Reference system is always higher than for DPS systems).

Additional studies (see §3.2.4.1) have been performed under the degraded operational condition due to the loss of the radio communication between the Traction units, also addressing the effect of the track gradient on the in-train longitudinal forces and the effect of the DPS introduction on the stopping distance.

Additional studies (see §3.2.4.1) have been developed under degraded operational conditions, including the loss of the radio communication between the Traction units (also addressing the effect of the track gradient on in-train longitudinal forces) and DPS failure (addressing the effect on the stopping distance).

3.1.8.2 Specific LTD simulations under correct functional operation

Specific LTD simulations have been performed for the configuration of DPS train Demonstrators as defined (in agreement with FR8RAIL II) for the execution of the experimental test campaign, in terms of train consist(s) and specific tests to be performed (see §1.5).

The simulated train operations have been selected in in order to emphasize the in-train longitudinal forces (based on the results obtained by the preliminary simulations) and concern: traction up to 30 km/h, followed by an emergency braking in nominal and in degraded (loss of radio communication) conditions. The same operations have been simulated for trains in "LL" and "G" braking regimes.

In general, the most important results coming from the preliminary LTD simulations (documented in D3.3 [22], concerning "G" braking regime) are confirmed; specifically, in-train longitudinal forces decrease because of mass and length reduction with respect to trains families simulated in D3.3.

Higher in-train forces occur in braking regime LL with respect to G, while higher stopping distance occurred in braking regime G (as for conventional trains).

Specifically, under normal condition (when the brake at the guided Traction units is triggered by radio):

- DPS trains have better performance in terms of (lower) in-train compressive forces with respect to the Reference train (i.e. without DPS);

[3] In is worthwhile recall that 10 m LCF at a certain place is equal to the minimum LCF (in absolute sense) occurred in 10 m before; therefore, it is not a running average.

- DPS can result in higher in-train tensile forces for some train configurations (LWLW, typically) but anyway, such forces are of no concern for disruption risk (the ratios between the in-train forces and the admissible values according to UIC 421 [11], considering a radius of curvature of 300 m close to the minimum value for the test track, have been addressed for LL braking regime; LTF do not exceed 550 kN which is a "safe" value for Longitudinal Compressive Forces considered as admissible value in D3.1);
- the introduction of DPS provides benefit for (i.e. reduces) the stopping distance with respect to the Reference train (i.e. without DPS) .

Details on the performed simulations and on the obtained results are provided in the Appendix A.

Additional simulations have been performed considering the track gradient (up/down hill scenarios), under the degraded condition due to loss of radio communication between the Traction units (see §3.2.4.1).

3.2 Effects of Faults

The effects of single faults are described in §3.2.1, based on the hazardous condition due to an incorrect execution of the function(s) implemented by the DPS train (see §1.4.2).

The capability to detect (single) faults and the actions following detection are described in the subsequent sections §3.2.2 and §3.2.3, through the functional safety requirements specified as mitigations during the safety analyses (see §2.4).

3.2.1 Effects of Single Faults

The effects of single faults have been examined through the safety analysis carried out for DPS trains, introduced in §2.4.

For each function implemented by DPS train (introduced and described in Table 2), Table 11 provides:

- the (worst) hazardous condition(s) due to an incorrect execution of the function(s), as specified during the safety analyses;
- the Safety Integrity Level (SIL) allocated according the criteria stated in §2.6;
- further mitigations in order to achieve a tolerable risk level (specifically for low safety integrity functions).

The SIL assigned in Table 11 to each function has been propagated to all the related mitigations (functional safety requirements).

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Main function	(Worst) Hazardous scenario	SIL	Further mitigations	
Train composition	**Inconsistency between the train physical composition and configuration data**, leading to an hazardous management of distributed traction and brake with **missed stop of DPS train within the maximum allowable braking distance** (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Safety function not involving safety-related electronic systems	PHA_MIT_22	Procedures shall be defined on the coupling and decoupling of wagons and Traction units for the composition of DPS train according to the applicable rules and constraints (e.g. on Traction units and wagons types and positions, and distribution of loads), specifying the actions, checks and responsibility of the driver / staff.
			HA_MIT_03	After DPS train inauguration, the train run shall be possible only in case of: _ complete set of valid configuration data, acknowledged by the Driver AND _ positive results from checks of diagnostic function(s) AND _ positive results from valid Train Initial tests, acknowledged by the Driver; _ consistent train orientation at different Traction units, acknowledged by the Driver Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
Communication set-up	**Incomplete exchange of data between DPS train locomotives and use of potential unsafe configuration data,** leading to an hazardous management of distributed traction and brake with **missed stop of DPS train within the maximum allowable braking distance** (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Basic integrity level	HA_MIT_03	After DPS train inauguration, the train run shall be possible only in case of: _ complete set of valid configuration data, acknowledged by the Driver AND _ positive results from checks of diagnostic function(s) AND _ positive results from valid Train Initial tests, acknowledged by the Driver; _ consistent train orientation at different Traction units, acknowledged by the Driver Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
			HA_MIT_43	Procedure shall be defined specifying the actions and the responsibility of the driver after DPS train inauguration, including the check that all and only the Traction units designated to participate are connected to the network.
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.
Train inauguration & configuration	**Potential unsafe set of configuration data,** leading to an hazardous management of distributed traction and brake with **missed stop of DPS train within the maximum allowable braking distance** (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety integrity level	PHA_MIT_25	Procedures shall be defined for the first setting and any change of DPS train orientation, specifying the actions and the responsibility of the driver, including the acknowledgment of the coherency between the train orientation set at the different Traction units and/or the execution of the train orientation test (eventually involving other staff operators).
			HA_MIT_03	After DPS train inauguration, the train run shall be possible only in case of: _ complete set of valid configuration data, acknowledged by the Driver AND _ positive results from checks of diagnostic function(s) AND _ positive results from valid Train Initial tests, acknowledged by the Driver; _ consistent train orientation at different Traction units, acknowledged by the Driver Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Main function	(Worst) Hazardous scenario	SIL	Further mitigations	
Train operational status management	**Missed or undue remote controls from the leading locomotive to the guided one(s)**, leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety integrity level	PHA_MIT_25	Procedures shall be defined for the first setting and any change of DPS train orientation, specifying the actions and the responsibility of the driver, including the acknowledgment of the coherency between the train orientation set at the different Traction units and/or the execution of the train orientation test (eventually involving other staff operators).
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.
Train initial test	**Latent failure and/or incorrect configuration data remain non detected,** leading to an hazardous management of distributed traction and brake with **missed stop of DPS train within the maximum allowable braking distance** (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety integrity level	PHA_MIT_23	Procedures shall be defined specifying the actions and the responsibility of the driver/staff of DPS train in the execution of the Train initial tests, including: _the application of the Parking brake at all the Traction units before tests execution and until their conclusion, _the enabling of the entire brake pipe (i.e. involving all the Traction units) before tests execution, _the acknowledgement of positive and valid results from tests.
			PHA_MIT_32	Procedures shall be defined specifying the actions and the responsibility of the driver of DPS train in the release of the Parking brake, as for conventional trains. Specifically, the Parking brake shall be not released during the Train initial test.
			HA_MIT_42	Procedure shall be defined specifying the actions and the responsibility of the driver of DPS train in the evaluation of results from the Train initial tests, which shall be not more valid (requiring the re-execution of the full set of tests) in case of modification of the train composition, modification of the brake mode set at the Traction units, modification of the brake pipe status, and anyway with a defined frequency (i.e. the period between two consecutive complete set of brake tests shall be compatible with the detection of latent failures).
Communication between Traction units	**Missed or incorrect exchange of remote controls between the DPS train locomotives** ,leading to an hazardous management of distributed traction and brake with **missed stop of DPS train within the maximum allowable braking**	Low Safety integrity level	HA_MIT_30	The guided Traction units of DPS train, in case of reduction of the brake pipe pressure shall apply the traction cut off with a defined ramp down and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance.Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train).

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Main function	(Worst) Hazardous scenario	SIL	Further mitigations	
	distance (and potential collision of DPS train with other trains, infrastructure or obstacle) **and/or excessive in-train longitudinal forces** (and potential train separation and/or derailment).		HA_MIT_31	The leading Traction units of DPS train, in case of reduction of the brake pipe pressure, shall cut off the traction with a defined ramp down, and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train).
			HA_MIT_44	Procedure shall be defined specifying the actions and the responsibility of the driver for train run when the radio communication between the Traction units is permanently lost, avoiding that DPS train remains for indefinite time under degraded operating mode, and stopping the train in a safe condition.
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.
Traction management	DPS train speed beyond the actual limit due to an ineffective management of traction and dynamic brake and/or excessive in-train longitudinal forces (and potential DPS train separation and/or derailment).	Low Safety integrity level	PHA_MIT_28	Procedures shall be defined if the Traction units of DPS train are able to provide traction and/or dynamic brake effort beyond the threshold limits and these limits can be modified or deactivated by the driver.
			PHA_MIT_29	Procedures shall be defined specifying the actions and the responsibility of the driver for the departure of DPS train on steep slope.
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.
			HA_MIT_19	Each Traction unit of DPS Train shall apply the traction cut off if the brake pipe pressure is below a defined limit, independently from the status of the radio connection and received information, with a defined ramp down.
Service brake management	**Ineffective pneumatic brake with potential exceeding of space and/or speed limits** (and potential collision of DPS train with other trains, infrastructure or obstacle and/or derailment) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety integrity level	HA_MIT_27	The Leading Traction unit of a DPS train shall send an emergency brake command to all the guided Traction units (to guarantee the continuity of the brake) and vent the brake pipe (i.e. actuate an Emergency brake) in case of request generated by the driver, OR by the safety loop and protection systems in the leading Traction unit, OR by a EB request coming from a guided Traction unit.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Main function	(Worst) Hazardous scenario	SIL	Further mitigations	
Emergency brake management	Missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	High Safety Integrity level	PHA_MIT_30	Procedure shall be defined in case the unavailability of air in the main reservoirs of the different Traction units of DPS train is communicated to the driver and no provision is implemented to inhibit the train run, specifying the required actions and responsibility (to assure the brake inexhaustibility for the entire DPS train).
Parking Brake management	**Ineffective permanent immobilization and undue train movemen**t, with potential collision of DPS train (with other trains, infrastructure or obstacle)	High Safety Integrity level	PHA_MIT_32	Procedures shall be defined specifying the actions and the responsibility of the driver of DPS train in the release of the Parking brake, as for conventional trains . Specifically, the Parking brake shall be not released during the Train initial test.
Energy management	**Potential damage to the infrastructure** (catenary overhead) **and/or to the DPS train** (on-board power supply system).	Low Safety integrity level	PHA_MIT_31	Procedures shall be defined for the management of pantographs of DPS train, specifying the actions and the responsibility of the driver:_for checking that pantograph - if manually selected - is consistent with the network and voltage system, as for conventional trains;_for assuring that each Traction unit crosses the neutral section when disconnected from the power supply system (e.g. by operating the main circuit breakers);_for avoiding that pantograph of different Traction units are connected at the same time to different power supply systems (in case of high voltage connection).
Air management	Ineffective pneumatic brake and **missed stop of DPS train within the maximum allowable braking distance** (and potential collision with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety integrity level	PHA_MIT_30	Procedure shall be defined in case the unavailability of air in the main reservoirs of the different Traction units of DPS train is communicated to the driver and no provision is implemented to inhibit the train run, specifying the required actions and responsibility (to assure the brake inexhaustibility for the entire DPS train).
			HA_MIT_06	The DPS Train initial tests shall validate the train configuration and verify the braking capability through the following checks: _ availability of (pneumatic / electric) energy source, according to the inexhaustibility requirement; _ brake pipe integrity (leak); _ brake pipe continuity (extended on DPS train, based on radio communication between Traction units); _ capability to apply the Emergency brake requested by the driver, and through the safety loop and protection systems in the leading and guided Traction units; _ capability to monitor the brake pipe pressure and react to a pressure drop (i.e. to assist the pressure reduction up to the vent of the brake pipe) initiated by the leading Traction unit and by each guided Traction unit.
Automatic Train Protection management	**DPS train speed beyond the actual limit** (and potential train derailment) **and/or missed stop of DPS train** within the maximum allowable braking distance (and potential collision with other trains, infrastructure or obstacle)	High Safety Integrity level	PHA_MIT_26	Procedures shall be defined if the management of traction and dynamic brake forces in DPS train at specific infrastructure locations (e.g. in areas of switches, or due to a temporary speed restriction) is under the responsibility of the driver (i.e. train movement supervision is not implemented by the ATP system), as for conventional trains.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Main function	(Worst) Hazardous scenario	SIL	Further mitigations	
Diagnostic	Hazardous condition due to the **missed or delayed reaction to operational relevant failures and disturbances or to a on-board fire event**.	Low Safety integrity level	PHA_MIT_33	Procedures shall be defined specifying the actions required to the driver of DPS train for the management of alarms (requiring non-automatic reactions at train level).
			HA_MIT_06	The DPS Train initial tests shall validate the train configuration and verify the braking capability through the following checks: _ availability of (pneumatic / electric) energy source, according to the inexhaustibility requirement; _ brake pipe integrity (leak); _ brake pipe continuity (extended on DPS train, based on radio communication between Traction units); _ capability to apply the Emergency brake requested by the driver, and through the safety loop and protection systems in the leading and guided Traction units; _ capability to monitor the brake pipe pressure and react to a pressure drop (i.e. to assist the pressure reduction up to the vent of the brake pipe) initiated by the leading Traction unit and by each guided Traction unit.
			HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.
System de-activation	Undue deactivation of DPS equipment, leading to an hazardous management of distributed traction and brake with **missed stop of the train within the maximum allowable braking distance** (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or **excessive in-train longitudinal forces** (and potential train separation and/or derailment).	Low Safety Integrity level	HA_MIT_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off. Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.

Table 11 - Safety integrity level allocation to DPS Train functions and further mitigations

3.2.2 Detection of Single Faults

3.2.2.1 Detection of radio communication loss

The leading and guided Traction units of DPS train shall monitor the radio communication by a continuous exchange of messages, once established. (HA_MIT_05)

Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units. (HA_MIT_08)

The leading and guided Traction units of DPS train shall exchange a life sign through radio communication (i.e. to detect interruption, since process data are send periodically). (HA_MIT_13)

The leading and guided Traction units of DPS train shall monitor the radio communication and detect a communication interruption if: the communication channel is terminated abruptly, OR messages are received with frozen life sign, OR no valid message is received. (HA_MIT_12)

3.2.2.2 Detection of other failures

The DPS Train initial tests shall validate the train configuration and verify the braking capability through the following checks: availability of (pneumatic / electric) energy source, according to the inexhaustibility requirement; brake pipe integrity (leak); brake pipe continuity (extended on DPS train, based on radio communication between Traction units); capability to apply the Emergency brake requested by the driver, and through the safety loop and protection systems in the leading and guided Traction units; capability to monitor the brake pipe pressure and react to a pressure drop (i.e. to assist the pressure reduction up to the vent of the brake pipe) initiated by the leading Traction unit and by each guided Traction unit. (HA_MIT_06)

The guided Traction units of DPS train shall communicate to the leading Traction unit - by radio - the correct execution of the brake test. (HA_MIT_07)

The leading Traction unit of DPS train shall continuously monitor and inform the driver about the status of the guided Traction units, (including traction / brake / alarm). (HA_MIT_38)

The guided Traction units of a DPS Train shall report by radio communication its capability of applying traction and dynamic and pneumatic brake forces to the leading Traction unit. (HA_MIT_20)

The guided Traction units of DPS train shall report the actual status of the local pneumatic brake (applied/released) and the local measured brake pipe pressure to the leading Traction unit. (HA_MIT_20)

The alarms in a guided Traction unit requiring a reaction at DPS train level (e.g. train speed reduction, train stop, activation of protective unit) shall be communicated to the leading Traction unit. (HA_MIT_40)

Each Traction units of DSP Train shall monitor the availability of air pressure in the main reservoir detect if no sufficient air pressure is available in its main air reservoir, and trigger an appropriate action (e.g. traction interlock and/or message to driver as for conventional train) inhibiting the train running if the inexhaustibility of the brake is not guaranteed for the entire DPS train. Brake inexhaustibility requirement: without any source of energy for brake actuation (pressure and air flow / electric energy), the Brake system shall guarantee the application of the minimum (Emergency) brake force for at least 2 times (i.e. brake cannot be released if it cannot be applied again). (HA_MIT_21, High SIL for Brake inexhaustibility requirement)

3.2.3 Action following Detection

3.2.3.1 Action following radio communication loss

Each guided Traction unit of DPS train shall complete any on-going brake application (i.e. assistance to the brake pipe pressure reduction) if the radio communication with the leading Traction unit is interrupted. (HA_MIT_23)

Each guided Traction unit of DPS train shall cancel any on-going brake release (i.e. brake pipe refilling shall be inhibited) if the radio communication with the leading Traction unit is interrupted. (HA_MIT_24)

The (leading and guided) Traction units of DPS train shall complete the on-going procedure for the lowering of pantographs if the communication between the Traction units is interrupted. (HA_MIT_33)

3.2.3.2 Action following decrease of pressure in the Brake pipe

Each Traction unit of DPS Train shall apply the traction cut off if the brake pipe pressure is below a defined limit, independently from the status of the radio connection and received information, with a defined ramp down. (HA_MIT_19)

The guided Traction units of DPS train, in case of reduction of the brake pipe pressure shall cut off the traction with a defined ramp down and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train).(HA_MIT_30)

The leading Traction units of DPS train, in case of reduction of the brake pipe pressure, shall cut off the traction with a defined ramp down, and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train). (HA_MIT_31)

3.2.3.3 Action following other failures

The leading Traction unit of DPS train shall assure safe condition (no train run, train stop) in case of critical failures (no/ineffective brake or no/incorrect measure of brake pipe pressure) at any (Leading or Guided) Traction unit. (HA_MIT_26)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

3.2.4 LTD under degraded operation conditions

3.2.4.1 Preliminary LTD simulations under degraded operation conditions

According to the deliverable D3.3 [22], under the degraded conditions due loss of radio communication, when the braking at the guided Traction unit is triggered by the detection of a pressure drop (0.2 bar) in the brake pipe, DPS trains are usually better than Reference trains, i.e. they experience equal or lower Longitudinal Compressive Forces (LCF) under the same train operational scenarios. The only exception concerns the operational scenarios starting with the train applying ED brake. In general, the gradient for removal of ED brake is a parameter that affects the LCF. Specifically, LCF experienced by DPS train starting with the ED brake applied is much lower than in other train operational scenarios (e.g. #5 and #9). It has been suggested to test DPS train considering different gradients of ED brake removal (see D3.3 [22]).

Simulations addressing the effect of **track gradient** have been performed under the degraded operational condition due to the loss of the radio communication between the Traction units. As far as the relative approach is concerned, even if usually LCF and LTF depend on the track gradient, the difference between the Reference and DPS train (families) is less affected. Usually, DPS trains are better than Reference trains; when it is not always the case, e.g. train running on downhill with the need to remove ED braking, LCFs are lower than those estimated for other train operational scenarios or anyway LCFs do not exceed 400 kN which is considered a safe value for Longitudinal Compressive Forces according to UIC Leaflet 421 [11].

Concerning the **reaction of the guided TU** to a brake pipe pressure drop (0.2 bar), there are no substantial differences between LCF estimated for the two options (Full-service braking or Stepwise pressure reduction). Stepwise reduction of pressure is associated to lower values of LTF with respect to full-service braking. These results advice to implement the stepwise pressure reduction instead of the full-service braking upon detection of pressure drop in brake pipe. Anyway, it has been suggested (in the deliverable D3.3) to test both reactions of the guided Traction unit to a brake pipe pressure drop (Full-service braking or Stepwise pressure reduction) and to confirm the results of simulations (developed in D3.3).

As additional result, there is no benefit in **removing traction** in case of radio communication loss (i.e. also in the period between the detection of the communication loss and the detection of the 0.2 bar Brake pipe pressure decrease), from the perspective of in-train longitudinal forces.

Specific studies have been performed during the M2O project concerning the **stopping distance** of DPS train in case of loss of radio communication between the Traction units, showing the effect of the two strategies for venting the brake pipe (stepwise or full brake) when pressure reduction is detected. The relative percentage difference between the main stopping distance of Reference trains and the different DPS train consists has been computed, according to train modelling described in §2.9.5, considering high train speeds (i.e. changing the initial train speed from 80 to 100 km/h with 10 km/h steps). The obtained results allow to conclude that the stopping distance of the DPS trains is always lower than for Reference trains, both in case of stepwise pressure reduction and (even better) in case of full-service braking triggered by the guided TU.

Failures of DPS equipment, which do not apply the braking action when required by radio (if available) and by the pressure drop in the brake pipe have been addressed in D3.3. Preliminary LTD simulations have been performed in the deliverable D3.3 assuming this hypothetical hazardous failure. According to § 1 and to §4, this is not the case because of the limited evidence available from the V&V activities.

3.2.4.2 Specific LTD simulations under degraded operation conditions

Additional LTD simulations have been performed for the specific configuration of the DPS train Demonstrators, addressing:

- the effect on the in-train longitudinal force and on the stopping distance of the loss of radio communication (conservatively focused on Emergency braking from full acceleration (9xxx));
- the effect on the in-train longitudinal force and on the stopping distance of the failures of DPS equipment.

In case of **loss of radio communication** between the Traction units (i.e. when brake is triggered by a detected reduction of the brake pipe), the in-train compressive forces decrease, whereas in-train tensile forces increase with respect to the normal condition (i.e. when brake is triggered by radio communication). Anyway, the main results of the specific simulations performed for normal operations (see §3.1.8.2) are confirmed also in case of loss of radio communication: DPS train Demonstrators have better performance in terms of in-train compressive forces with respect to trains but can result in higher in-train tensile forces for some train configurations (LWLW, typically) that anyway are of no concern for disruption risk.

Concerning the train stopping distance, estimated by deterministic analysis with train in regime G (see A.4), the introduction of DPS provides benefits (in terms of reduction of the in-train longitudinal force and on the stopping distance) also in case of loss of radio communication (when the braking at the guided Traction unit is triggered by a reduction of the pressure in the brake pipe).

Moreover, there is no increase of the stopping distance of Demonstrators in case of of-removal of traction at the loss of radio communication, while the benefit from the in-train longitudinal forces perspective was evaluated by the preliminary LTD simulation (see §3.2.4.1). It also applies to LWLWL in case of equal total traction force applied (see A.4). On this topic, it has been suggested to test DPS train considering different time intervals for the automatic reduction of the traction force, in case of loss of radio communication, before any detection of brake pipe pressure drop [22].

In case of (hazardous) **failures of DPS equipment**, the performances of the DPS train Demonstrators are the same of the Reference train, i.e. with no higher in-train longitudinal force and on the stopping distance. Therefore, no additional mitigation is required for the execution of the test runs, in spite of the limited evidence available from the Verification and Validation activities. Anyway, also in case of emergency brake from (full) acceleration, the stopping distance is lower than the limit stated in UIC 544-1 [12] (for this type of train, having a percentage of braked weight around 80%) which is around 920 m (in brake position G, see A.4).

Details on the performed simulations and on the obtained results are provided in the Appendix A.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

3.3 Operation with External Influences

The following safety requirements have been specified during safety analyses: *The radio communication between the Traction units of DPS train shall not influence and not be influenced by the radio communication between the on-board and track-side ATP equipment (if used). (HA_MIT_37)*

A specific test activity is planned to provide evidence that no interference is between the LTE-Antennae and the existing devices (Report on antennae interference in Table 7).

The main steps to be performed (in the future) towards full compliance with EN 50129 [5] concern the development of a formal V&V process. Within this context, it is expected that DPS equipment are tested according to EN 50125-3 [8].

3.4 Safety-related Application Conditions

This section provides the Safety-Related Application Conditions specified during the M2O project and the validation strategy set for the execution of the experimental test campaign introduced in §1.5, agreed with the FR8RAIL II partners.

Table 12 provides the list of mitigations specified during Safety analyses (see §2.4), classified as Contextual safety requirements, to be fulfilled by the specification of operational procedures, i.e. Safety-related Application Conditions exported to "Operation" (element within the context defined in §1.4.1).

The column "Validation strategy" specifies the Verification and Validation (V&V) activities to be finalized (before the test runs) in order to gather evidence of the fulfilment of the applicable mitigations.

The column "Evidence for validation" specifies the sources of the evidence that safety-related requirements are specified, implemented and verified, to be collected before test runs (summarized in Table 7).

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

D	Description	Validation strategy	Evidence for validation
PHA_MIT_07	Procedures shall be defined specifying the actions and the responsibility of the driver / staff for fulfilment of requirements about the loading gauge (maximum height and width for railway vehicles and their loads), as for "conventional" trains.	Test train will only consist of homologated locomotive (one locomotive is not yet fully homologated but permitted for test runs) and wagons. Existing procedures / norms (as for the Reference system) apply to the test runs.	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)
PHA_MIT_22	Procedures shall be defined on the coupling and decoupling of wagons and Traction units for the composition of DPS train according to the applicable rules and constraints (e.g. on Traction units and wagons types and positions, and distribution of loads), specifying the actions, checks and responsibility of the driver / staff.	Existing procedures / norms concerning general rules and constraints for the coupling and decoupling of wagons and Traction units (as for the Reference system) apply to the test runs. Specific constraints on train composition coming from in-train longitudinal studies, if any, will be included in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on coupling and decoupling of wagons and Traction units) M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))
PHA_MIT_23	Procedures shall be defined specifying the actions and the responsibility of the driver/staff of DPS train in the execution of the Train initial tests, including: _the application of the Parking brake at all the Traction units before tests execution and until their conclusion, _the enabling of the entire brake pipe (i.e. involving all the Traction units) before tests execution,_the acknowledgement of positive and valid results from tests.	Specific procedure concerning the execution of the Train initial tests will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (for Train initial test execution)
PHA_MIT_24	Procedures shall be defined specifying the actions, constraints and responsibility of the driver of DPS train to perform shunting movement, as for conventional trains .	Existing procedures / norms (as for the Reference system) apply to the test runs. Test track will be checked on additional constraints for shunting movement.	Test specification providing instruction to staff (reference to the existing procedures / norms on shunting movement). Test track (constraints for shunting movement, if any)
PHA_MIT_25	Procedures shall be defined for the first setting and any change of DPS train orientation, specifying the actions and the responsibility of the driver, including the acknowledgment of the coherency between the train orientation set at the different Traction units and/or the execution of the train orientation test (eventually involving other staff operators).	Actions and checks for train orientation will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (for setting of train orientation)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

D	Description	Validation strategy	Evidence for validation
PHA_MIT_26	Procedures shall be defined if the management of traction and dynamic brake forces in DPS train at specific infrastructure locations (e.g. in areas of switches, or due to a temporary speed restriction) is under the responsibility of the driver (i.e. train movement supervision is not implemented by the ATP system), as for conventional trains.	The operation of the train and handling of traction and dynamic brake will follow the applicable rules (as for the Reference system), which will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on handling of traction and dynamic brake)
PHA_MIT_27	Procedures shall be defined in order to avoid that applicable prescriptions for train running (received by trackside signalling operators) are not remembered by the driver of DPS train after a long train stop or after driver change, as for conventional trains.	The operation of the train and handling of traction and dynamic brake will follow the applicable rules (as for the Reference system), which will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on handling of traction and dynamic brake)
PHA_MIT_28	Procedures shall be defined if the Traction units of DPS train are able to provide traction and/or dynamic brake effort beyond the threshold limits and these limits can be modified or deactivated by the driver.	Actions and checks for setting of maximum traction/dynamic brake force values will be defined and documented in the test specification (including driver instructions).	Test specification providing instruction to staff (for setting limits of traction and/or dynamic brake effort)
PHA_MIT_29	Procedures shall be defined specifying the actions and the responsibility of the driver for the departure of DPS train on steep slope.	The driver will follow the existing rules and procedures (as for the Reference system) for the departure of DPS train on steep slope, which will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on departure of DPS train on steep slope)
PHA_MIT_30	Procedure shall be defined in case the unavailability of air in the main reservoirs of the different Traction units of DPS train is communicated to the driver and no provision is implemented to inhibit the train run, specifying the required actions and responsibility (to assure the brake inexhaustibility for the entire DPS train).	Test train length, mass, number of axles and axle load will not exceed the allowable limits for the test track. Thus, the supervision of main reservoir pressure of the leading locomotive (including the actions taken when thresholds of the pressure are crossed) is sufficient to guarantee a safe management of this hazard. Inexhaustibility of car brakes is guaranteed by design of the UIC pneumatic brake system. The participating locomotives supply energy from for the brake applications from "Reservebehälter", which guarantees inexhaustibility by their dimensioning.	Test specification providing instruction to staff (reference to the existing procedures / norms on unavailability of air in the main reservoirs)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

D	Description	Validation strategy	Evidence for validation
PHA_MIT_31	Procedures shall be defined for the management of pantographs of DPS train, specifying the actions and the responsibility of the driver: _for checking that pantograph - if manually selected - is consistent with the network and voltage system, as for conventional trains; _for assuring that each Traction unit crosses the neutral section when disconnected from the power supply system (e.g. by operating the main circuit breakers); _for avoiding that pantograph of different Traction units are connected at the same time to different power supply systems (in case of high voltage connection).	There are no neutral sections in the test track. On the choice of pantographs: User instructions will be included into test specification.	Test track (evidence on absence on neutral section) Test specification providing instruction to staff (on management of pantographs)
PHA_MIT_32	Procedures shall be defined specifying the actions and the responsibility of the driver of DPS train in the release of the Parking brake, as for conventional trains . Specifically, the Parking brake shall be not released during the Train initial test.	Handling of the parking brake will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (on handling of the parking brake)
PHA_MIT_33	Procedures shall be defined specifying the actions required to the driver of DPS train for the management of alarms (requiring non-automatic reactions at train level).	Handling of alarms will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (on handling of alarms)
PHA_MIT_34	Procedures shall be defined specifying the actions and the responsibility of the driver / staff for fulfilment of requirements about the positioning of wagons with dangerous goods (e.g. minimum distance), as for "conventional train.	Wagons in test train do not have any dangerous goods on board.	Vehicle list Test specification providing instruction to staff (no dangerous goods on board)
HA_MIT_41	The reaction to the alarms generated in the leading and guided Traction units (e.g. visualization to the driver and/or emergency brake commanded by the leading Traction unit) shall be defined.	Specific procedure concerning the reaction to the alarms generated in the leading and guided Traction units will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (on handling of / reaction to alarms)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

D	Description	Validation strategy	Evidence for validation
HA_MIT_42	Procedure shall be defined specifying the actions and the responsibility of the driver of DPS train in the evaluation of results from the Train initial tests, which shall be not more valid (requiring the re-execution of the full set of tests) in case of modification of the train composition, modification of the brake mode set at the Traction units, modification of the brake pipe status, and anyway with a defined frequency (i.e. the period between two consecutive complete set of brake tests shall be compatible with the detection of latent failures).	Existing procedures / norms concerning general rules and constraints for the evaluation of results and validity of the Train initial tests (as for the reference system) apply to the test runs. Specific actions / checks for the execution of the Train initial tests will be included in the test specification (including driver instructions).	Test specification providing instruction to staff (for train initial test execution)
HA_MIT_43	Procedure shall be defined specifying the actions and the responsibility of the driver after DPS train inauguration, including the check that all and only the Traction units designated to participate are connected to the network.	Specific procedure concerning the DPS train inauguration, including the check that all and only the Traction units designated to participate are connected to the network, will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (on train inauguration)
HA_MIT_44	Procedure shall be defined specifying the actions and the responsibility of the driver for train run when the radio communication between the Traction units is permanently lost, avoiding that DPS train remains for indefinite time under degraded operating mode, and stopping the train in a safe condition.	Specific procedure concerning the train run when the radio communication between the Traction units is permanently lost will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (train run without radio communication)
HA_MIT_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off.	Driving procedures for test train with DPS switched of follow the rules and standards for conventional trains. Dedicated instructions under which conditions the trains is driven as conventional train will be included in the test specification and communicated to drivers.	Test specification providing instruction to staff (train run with DPS switch-off)

Table 12 - Application conditions exported to Operation and validation strategy and evidence

Table 13 provides the additional safety-related application conditions (not already specified in the D3.2) exported to "Operation", with their validation strategy and evidence to be provided.

Additional essential application conditions concern the availability of the admission of tests from the German rail infrastructure (AC_01) and the execution of test and transfer runs in compliance with the applicable rules and guidelines (AC_03).

An additional application condition (AC_04) is specified in order to assure a secure and safe radio communication (§3.1.5), through checks to be performed during the DPS train set-up.

Further application conditions require that each guided Traction Unit of the DPS train Demonstrator(s) is manned (AC_05, AC_06, AC_07). They follow from intrinsic limitations related to the scope of the M2O and FR8RAIL II projects. Indeed, no formal Verification and Validation process has been performed (nor planned) for the DPS development and integration within the Traction unit (see §2.7) and no reference to Generic Product Safety case for (DPS revamped) Traction unit and/or its systems is available (see §4).

ID	Description	Validation strategy	Evidence for validation
AC_01	The admission of the test runs given by the German rail infrastructure shall be available.	Admission for experimental tests to be available before test execution.	Admission for experimental tests
AC_02	The implementation of technological and procedural provisions for the mitigations of "conventional hazards" (i.e. generally applicable to freight trains) shall be verified.	Admission for experimental tests to be available before test execution.	Admission for experimental tests
AC_03	All test and transfer runs shall be performed in compliance with the railway operating rules and guidelines applicable to the test track.	Specific operating rules and guidelines applicable to the test track will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)
AC_04	After the Communication set-up and Train inauguration of the DPS train Demonstrator(s), it shall be verified that all the Traction units connected to a specific VPN for radio communication are physically located in the same Train Consist.	Checks on connection to VPN will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)
AC_05	Each guided Traction Unit of the DPS train Demonstrator(s) shall be manned.	Presence and responsibility of staff at the guided Traction units will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)
AC_06	The staff attending the guided Traction Units of the DPS train Demonstrator(s) shall have an independent way of communication with the driver (at the leading Traction Unit)	Presence and responsibility of staff at the guided Traction units will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)
AC_07	Procedures shall be defined specifying the actions and responsibility of the staff at each guided Traction unit of the DPS train Demonstrator(s), including checks and confirmation of the train set-up (i.e. inauguration and configuration, and train initial test).	Presence and responsibility of staff at the guided Traction units will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (reference to the existing procedures / norms on loading gauge)

Table 13 - Additional application conditions exported to Operation and validation strategy and evidence

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

4 Related Safety Case

The present section corresponds to the section called "Related Safety Case" of the Safety Case.

Toward a Specific Application Safety Case fully compliant with EN 50129 [5], references shall be provided to the Safety Case of each "generic product" constituting the DPS train's Traction unit and involved in the implementation of the functions listed in Table 2 (see §1.4.2), including the new Radio equipment, the TCMS (adapted for DPS), the new DPS panel (integrated within the leading and the guided Traction units).

As intrinsic limitation related to the scope of the M2O and FR8RAIL II projects, no formal Verification and Validation process has been performed (nor planned) for the DPS development and integration within the Traction unit (see §2.7) and no reference to Generic Product Safety case for (DPS revamped) Traction unit and/or its systems is available.

The main steps to be performed in the future, towards full compliance with EN 50129 [5], come from the above limitations. They concern the development of a formal Verification and Validation process for the DPS equipment and the modified existing train equipment, and for their integration within the specific Traction unit (including the verification of the fulfilment of the safety-related application conditions exported by each subsystem), and the production of the related Generic Product and Generic Application Safety cases.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

5 Conclusion

The present deliverable of the M2O project contributes to the demonstration that DPS train has been designed and developed according to the requirements defined in EN 50129 [5]. The activities performed during the M2O project are specified in the Safety plan (deliverable D2.3 [20]). Safety relevant information is collected by this document, by a structure of content (see §1.3) compliant with a Specific Application (SA) Safety Case.

Safety analyses have been performed (see §2.4), providing a set of hazardous conditions (see §3.1.3) related to the operation of DPS trains and a set of mitigations to be implemented by DPS trains or exported to the remaining elements of the railway system (see §2.5). These results are the basis for the evaluation of safety of each "specific application" of DPS trains and specifically of the experimental test campaign introduced in §1.5.

With focus on the experimental tests, DPS train Demonstrator(s) will include Traction units approved (BR 187) or under approval (BR 188), retrofitted with DPS, and approved wagons (Eanos 59, Res 677, Facns 124, Facns 133). Train length, mass, number of axles and axle load will not exceed the allowable limits for the test track.

According to the deliverable D2.1 [18], LTE-network has been selected for the radio communication between the Traction units, mainly because point to multipoint communication is possible, IP communication can be used instead of proprietary communication protocol, low latency communication is introduced by network elements. It also allows overcoming problems of the number of antennas and channels permanently occupied (ERTMS occupies permanently 2 channels with the highest priorities).

SDTv2 [10] been selected as safety layer, consistently with the (Low) safety integrity required to the radio communication.

The security provisions implemented for the LTE communication during the test runs (limited in space and time) include the use of special credentials for the access of mobile to the private APN, the absence of direct communication between mobiles and the enforcing of traffic rule and monitoring of sessions and data traffic performed at the Control Center (see §3.1.6.2). Anyway, no definitive evidence is available on the robustness of the security provisions implemented for the experimental test campaign, if/when the LTE network is used for DPS trains commercial use (extended in time and space), which is out of M2O scope.

The safety demonstration of the brake functionality during a potential loss of the radio communication between the Traction units relies on an independent mechanism for braking application implemented at each Traction units, based on the monitoring of the Brake pipe pressure.

Because of the scope of the M2O and FR8RAIL II projects, the Technical Safety report (§3 of this document) relies upon a limited set of evidence. It collects results coming from the LTD studies performed within the M2O project and the information made available from FR8RAIL II partners.

Detailed sets of safety validation activities to be executed before the test runs and of the related evidence to be provided by FR8RAIL II have been specified (see Table 7 and Appendix B); they include:

- evidence closing the design stage, i.e. traceability between the safety functional requirements (specified by the safety analyses) and the (last version of) functional requirements stated by FR8RAIL II projects and/or the related functional tests;
- evidence about the proper implementation of the safety functional requirements (by functional tests);

- evidence concerning the operation during the execution of test runs, and specifically the compatibility between the DPS train Demonstrator(s) and the test track and the instruction provided to the staff/driver(s);
- evidence concerning the no interference between the LTE-Antennae and the existing devices.

Concerning the experimental test campaign, based on the lack of evidence on the correct implementation of the safety functional requirements, specific operational procedures (i.e. additional application conditions stated in §3.4) shall be implemented.

As main result coming from LTD simulations performed during the M2O project (see §2.9, §3.1.8, §3.2.4 and Appendix A), DPS train Demonstrators experience longitudinal forces and stopping distance not higher than for Reference trains (already admitted to the traffic on the track selected for tests execution) or anyway acceptable (i.e. lower than the admissible values, according to UIC 421 [11]).

Based on the results coming from LTD studies developed for the specific DPS train Demonstrators, the introduction of DPS provides benefits concerning the reduction of the in-train longitudinal compressive force and of the stopping distance, both under normal condition (when braking at the guided Traction units is triggered by the radio communication) and degraded condition (i.e. in case of loss of radio communication, when braking at the guided Traction units is triggered by the detection of a pressure drop in the brake pipe). Higher in-train tensile forces occur for some train configurations (LWLW), anyway below the admissible value.

In case of (hazardous) failures of DPS equipment, which do not apply the braking action when required by radio (if available) and by the pressure drop in the brake pipe, the performances of the DPS train Demonstrators are the same of the Reference train, i.e. no higher in-train longitudinal force and stopping distance. Therefore, no additional mitigations are required for the execution of the test runs, in spite of the limited evidence available from the Verification and Validation activities. This potentially hazardous failures could be not acceptable during the future commercial service of DPS train, but that will be mitigated through a fully developed Verification and Validation (V&V) process of DPS equipment and their integration within the locomotives.

Based on the results coming from LTD studies developed for the specific DPS train Demonstrators, considering the trainset having the lowest in-train forces (both in compression and in tension), the "best" trainset has been identified (see Figure 16). It can be tested with and without DPS, in all possible arrangements of active Traction Units, under all the operational scenarios addressed by the LTD simulations documented in the Appendix A.

The main steps to be performed in the future, towards full compliance with EN 50129 [5], concern the development of a formal Verification and Validation process for the DPS equipment and the modified existing train equipment, and for their integration within the specific Traction unit, and the production of the related Generic Product and Generic Application Safety cases.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

References

[1] Commission Regulation (EU) No 1299/2014 of 18 November 2014 on the technical specifications for interoperability relating to the 'infrastructure' subsystem of the rail system in the European Union Text with EEA relevance.

[2] Commission Regulation (EU) No 1302/2014 of 18 November 2014 concerning a technical specification for interoperability relating to the rolling stock — locomotives and passenger rolling stock subsystem of the rail system in the European Union (Text with EEA relevance)Text with EEA relevance.

[3] CEI EN 50126-1: 2018, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process.

[4] CEI EN 50126-2: 2019, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) Part 2: Systems Approach to Safety.

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

[6] EN 50128: 2011, Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems.

[7] EN 50159:2011, Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems.

[8] EN 50125-3 Railway applications - Environmental conditions for equipment Part 3: Equipment for signalling and telecommunications

[9] IEC 62280:2014, Railway applications - Communication, signalling and processing systems - Safety related communication in transmission system

[10] IEC 61375-2-3, Electronic railway equipment - Train communication network (TCN) - Part 2-3: TCN communication profile

[11] Leaflet UIC 421, Rules of the consist and braking of international freight trains, 9th edition, January 2012.

[12] UIC 544-1:2014-10 Brakes - Braking performance

[13] MARATHON (Make Rail The Hope for protecting Nature), project ended on 30 September 2014, URL: https://cordis.europa.eu/project/rcn/98327/reporting/en

[14] FR8RAIL II project, 20190827 (DB) Requirements LT V6.

[15] FR8RAIL II project, D5.2 - Functional and system requirements specification. (BT_dbl2.0).

[16] FR8Rail II project, WP7, Distributed Power System, TCMS Communication Concept.

[17] DB Netz AG, Antrag auf Durchführung eines Abstimmungsverfahrens gemäß Ril 810.0400 bei der DB Netz AG für Probefahrten eines langen Güterzuges mit verteilter Traktionsleistung Pro- jektes Shift2Rail/LongTrains.

[18] M2O project, Deliverable D2.1 - GSM-R or LTE design solution.

[19] M2O project, Deliverable D2.2 - TrainDy, Sensitivity Analysis.

[20] M2O project, Deliverable D2.3 - Integrate system, Safety report.

[21] M2O project, Deliverable D3.1 - LTD simulations report.

[22] M2O project, Deliverable D3.3 - TrainDy simulations for experimental tests d system, Safety report.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Appendix A Demonstrator(s) - Train dynamic simulation

This appendix provides the results coming from the specific simulations performed on the Demonstrator trains, as defined (in agreement with FR8RAIL II) for the execution of the experimental test campaign, in terms of train consist(s) and specific tests to be performed.

Results refer to train operations that emphasize longitudinal train dynamics and that have been already simulated in D3.3; beyond D3.3, the "long locomotive"[4] braking regime (LL) is also tested, here. With respect to D3.3, the trains simulated in this appendix have a lower length (around 650 m vs 730 m, Traction Units included) and a lower hauled mass (around 1500 t vs 1825 t, Traction Units excluded): a train like the one that will be tested by FR8RAIL II Partners is already allowed to traffic with one Traction Unit (TU) at the beginning of the consist and the other at its end, without DPS functionalities.

Because of mass and length reduction with respect to statistic trains tested in D3.3, it is possible to anticipate that the in-train forces are lower than those of D3.3, in "goods" or "freight" braking regime (G), and the most important results of D3.3 are all confirmed. Nevertheless, the test campaign will allow the testing of DPS functionalities, creating the conditions for its future implementation.

A.1. Vehicles of experimental train

The wagons used for the test campaign, along with their payload, are reported in Table 14.

	Facns-124	Res-676	Facns-133	Eanos_x-59
Tare [t]	25	24.5	22	23.56
Length [m]	19.04	19.9	16	15.74
Payload [t]	0	0	0	63

Table 14 - Wagons used in test campaign.

Two types of Traction Units (TUs) are used: two BR187 and one BR188, having small differences in terms of mass, length, and braking performances. The list of vehicles is completed by a measuring coach placed close to a BR187 TU, at the end of trainset. The trainset is like:

BR188, Measuring Coach, Wagons, BR187, Wagons, BR187

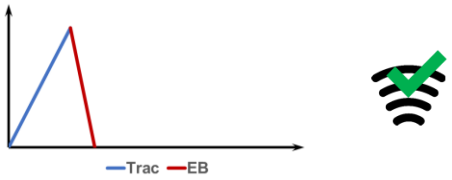
[4] According to this braking regime, the first TU and the following 5 wagons brake in regime G ("goods"), the remaining vehicles in P ("passengers"). In "goods" or "freight" braking regime, all vehicles brake in regime G. "Passengers" and "goods" regimes differ upon the filling time of brake cylinders, mainly.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

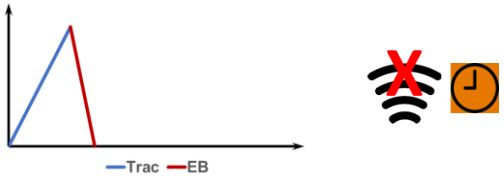
A.2. Determination of trainset for the test campaign

The FR8RAIL II Partners provided a trainset with wagons between the first and second TU and between the second and third TU. The positions of these wagons have been randomly permuted to find an order of wagons where the in-train forces are minimal in all conditions: a) with and without DPS and b) with a variable number of activated TUs in DPS train: LWL, LWLW, and LWLWL, following the nomenclature of D3.3. The train operations used at this aim are:

a) Traction up to 30 km/h followed by an emergency braking in nominal conditions and in braking regime LL:



b) Traction up to 30 km/h followed by an emergency braking in degraded conditions (radio link is lost when the emergency braking is applied) in braking regime LL:



c) As above, but in braking regime G.

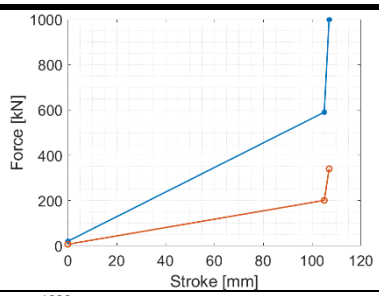
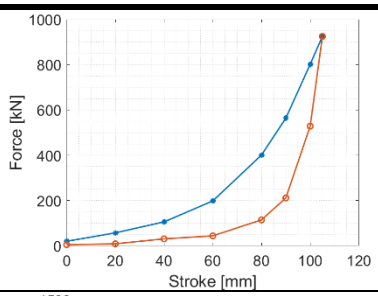
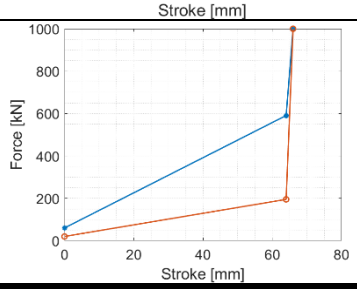
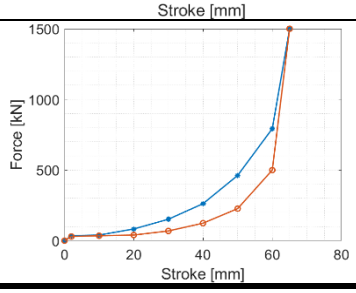
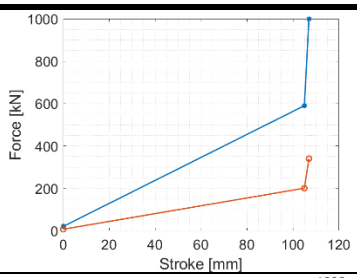
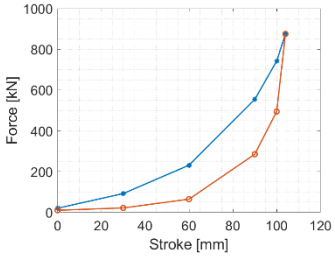
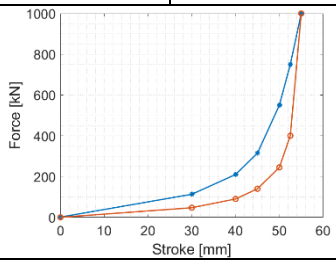
Above train operations have proved to be able to emphasize the in-train forces in D3.3 and for this reason they have been used. They have been performed on a straight track without any gradient, considering two directions for the motion:

- "FW", forward, when the first TU is the BR188 and the measuring coach is at beginning of trainset.
- "BW", backward, when the first TU is the BR187 and the measuring coach is at the end of trainset.

As in D3.3, the in-train performances of reference (REF) trains (without DPS) and DPS trains are compared in terms of maximum in-train compressive (LCF) and tensile forces (LTF), for different numbers and positions of active TUs.

Simulations of this section are performed without any technical parameter variation. Simulations of following sections, on selected trainset, will also consider this effect for the technical parameters identified in D2.2. In addition, the wagons can be equipped by different types of buffers/draw gears, whose force-stroke characteristics are reported in Table 15.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

	Eanos_x-59	
Buffing gears		
Draw gears		
	Facs-124	
Buffing gears		
Draw gears		

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

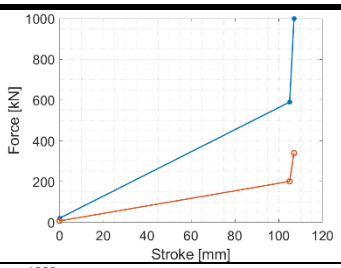
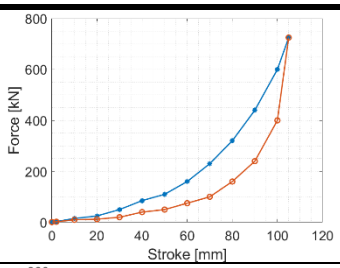
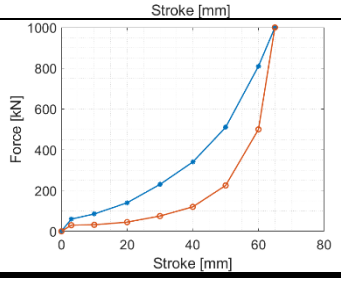
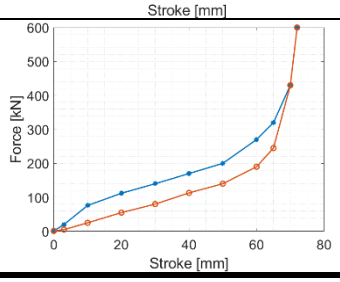
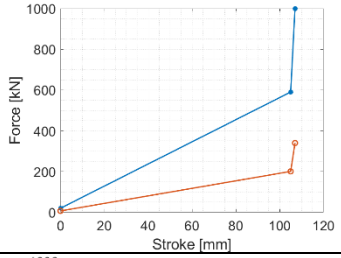
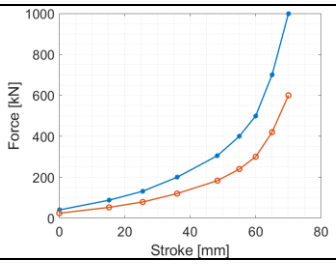
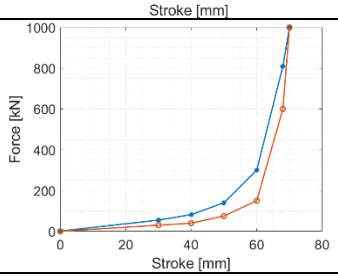
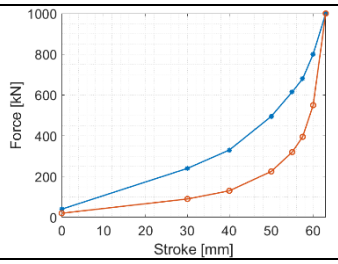
	Facs-133	
Buffing gears		
Draw gears		
	Res-676	
Buffing gears		
Draw gears	  	

Table 15 - Force-stroke characteristics of wagons coupling elements.

Results of above point a) are reported in Figure 10 and Figure 11. In Figure 10, each circle refers to a train, with specific order of wagons; the in-train compressive forces (LCF) of REF trains are always bigger than those of DPS trains whereas the in-train tensile forces (LTF) are usually bigger than those of DPS trains. The Figure 11 is similar, but it refers to "BW" direction.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

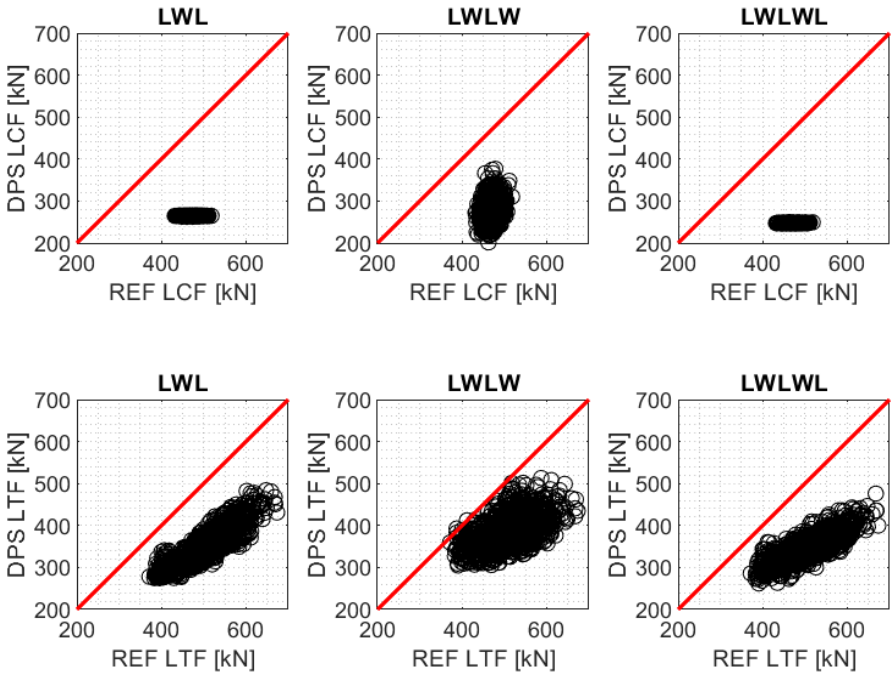


Figure 10 - Acceleration up to 30 km/h followed by an emergency braking in direction "FW", braking regime LL and nominal mode. Case a)

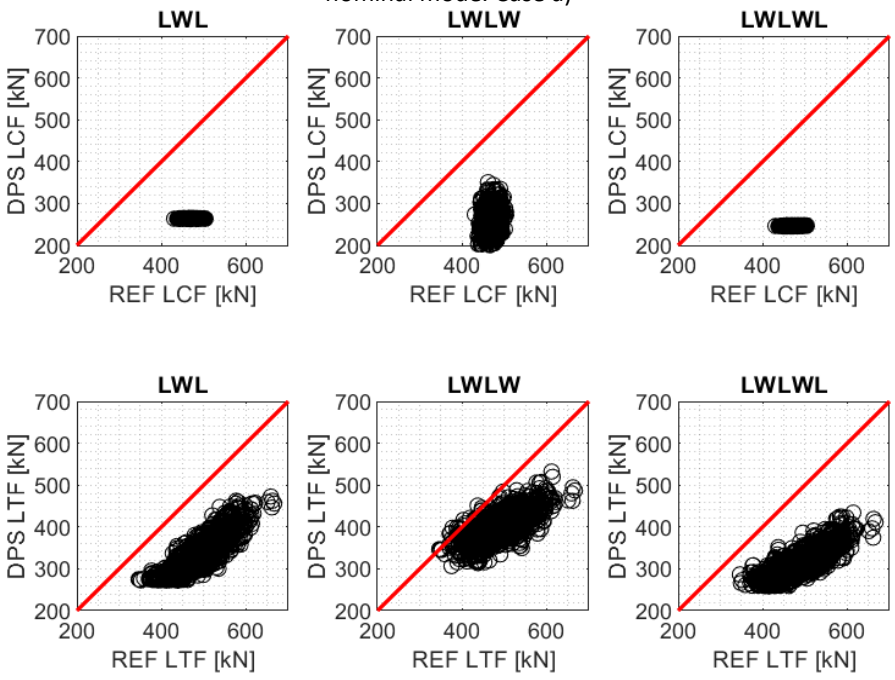


Figure 11 - As in Figure 10 (Acceleration up to 30 km/h followed by an emergency braking, braking regime LL and nominal mode), but in "BW" direction. Case a)

Results of above point b) are reported in Figure 12 and Figure 13. Comparing Figure 12 to previous Figure 10, it is possible to say:

- In-train compressive forces increase in degraded mode, whereas in-train tensile forces decrease. Quickly venting the brake pipe from the end (in nominal mode) increases the tensile forces, whereas the brake pipe venting from the train end is slower in degraded mode.
- Train configuration LWLW shows higher in-train tensile forces with DPS than without DPS. Anyway, these in-train tensile forces are of no concern, since there are lower than 550 kN, which was considered as admissible value in D3.1.

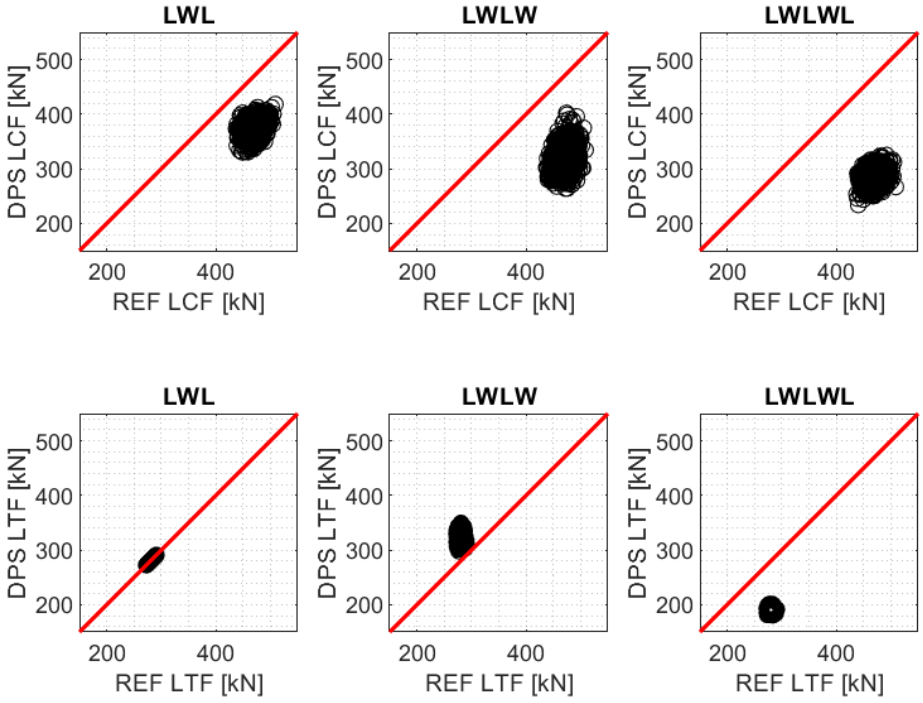


Figure 12 - Acceleration up to 30 km/h followed by an emergency braking in direction "FW", braking regime LL and radio link loss. Case b)

Results of above point c) are reported in Figure 14 and Figure 15: they confirm that higher in-train forces occur in braking regime LL with respect to G braking regime; moreover, DPS trains have better performance in terms of in-train compressive forces with respect to trains without DPS.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

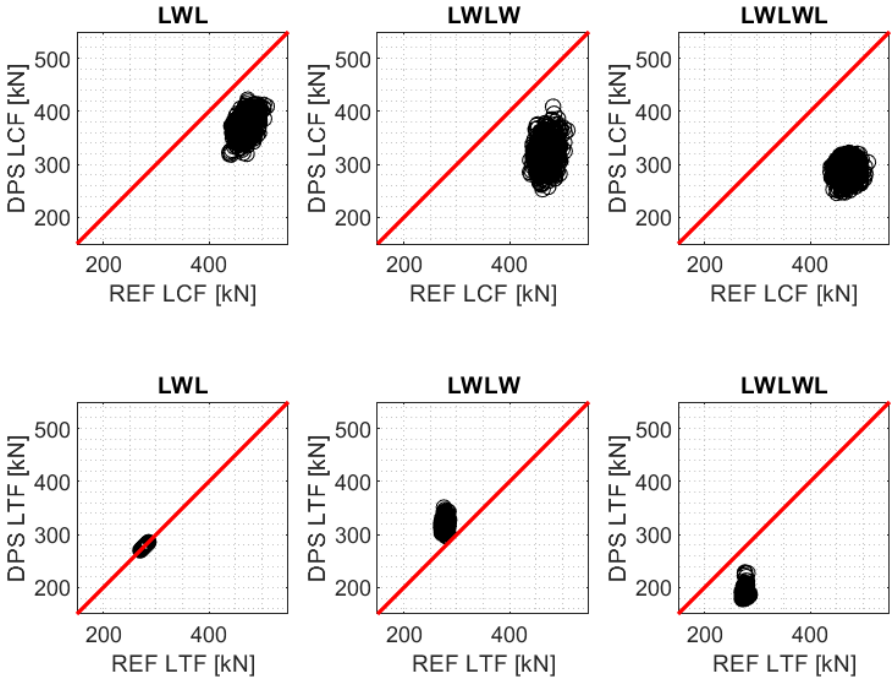


Figure 13 - As Figure 12 (Acceleration up to 30 km/h followed by an emergency braking, braking regime LL and radio link loss), but in "BW" direction. Case b)

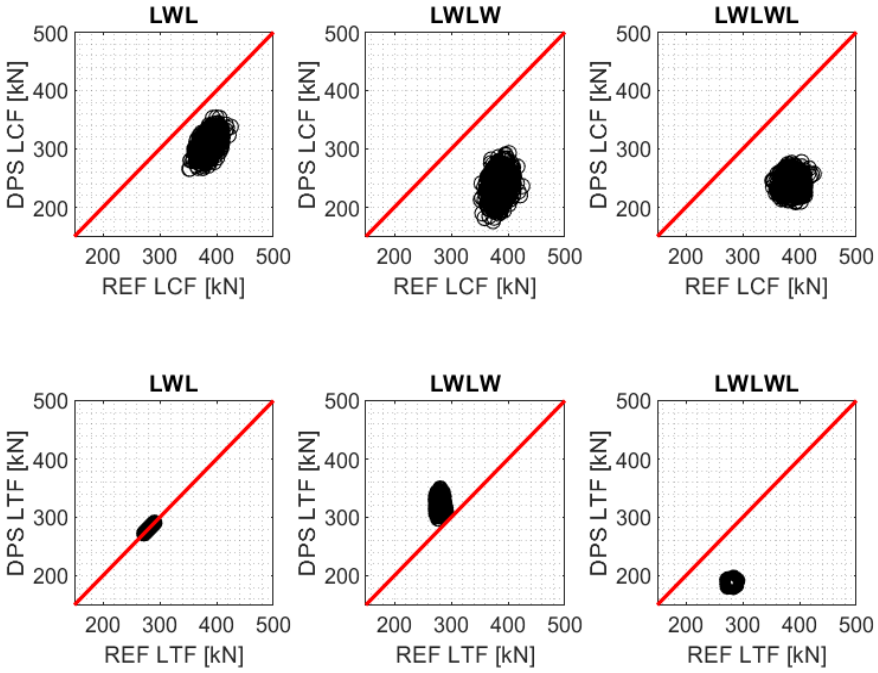


Figure 14 - Acceleration up to 30 km/h followed by an emergency braking in direction "FW", braking regime G and radio link loss. Case c)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

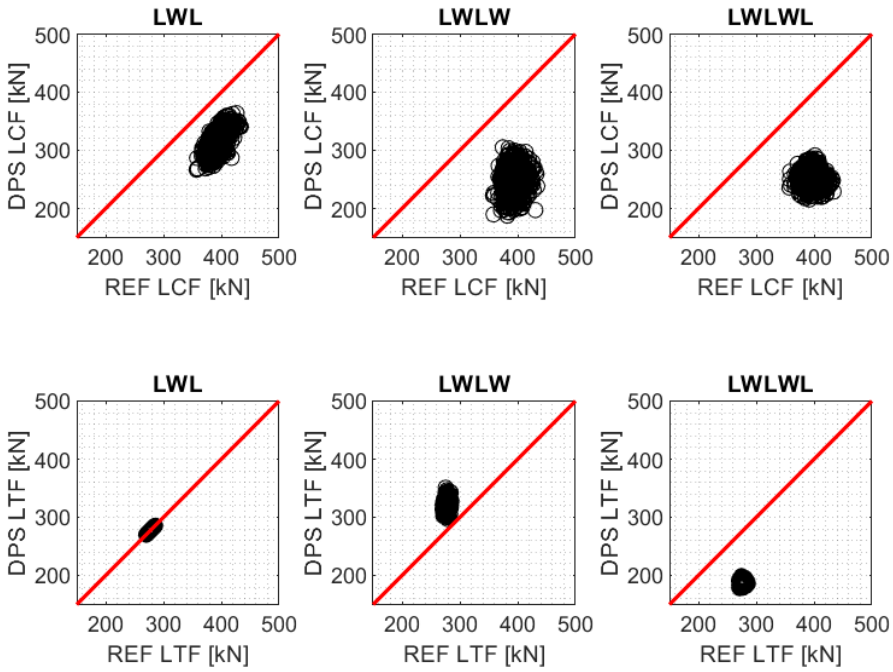


Figure 15 - As Figure 14 (Acceleration up to 30 km/h followed by an emergency braking, braking regime G and radio link loss), but in "BW" direction. Case c).

Considering the trainset having the lowest in-train forces (both in compression and in tension) in all previous scenarios, it is possible to find the "best" trainset among those simulated.

Figure 16 reports the screenshot, from TrainDy software, of selected trainset, which will be further simulated in the next sections. This trainset can be simulated with and without DPS in all possible arrangements of active TUs, since with DPS the in-train compressive forces and tensile forces are lower than the REF counterparts, and when this is not true, the values are of no concern, i.e., they are lower than the admissible values, according to UIC 421. For this reason, the experimental test campaign will test more demonstrators, being possible several arrangements of active TUs, corresponding to different future use cases.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

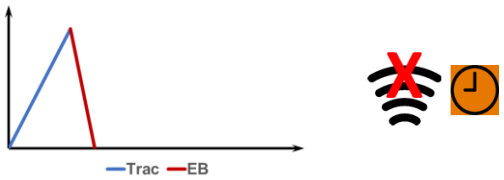
Position	Type	Manoeuvre	Wagon Length [m]	Train Length [m]	Brake Pipe Length [m]	GP coupl. status	Load [t]	Tare [t]
1	BR188	Man01L	18.9	18.9	37.8	☐	0	86
2	Measuring		26.4	45.3	29.04	☐	0	63
3	Facns-133		16	61.3	16	☐	0	22
4	Res-676		19.9	81.2	19.9	☐	0	24.5
5	Facns-124		19.04	100.24	19.04	☐	0	25
6	Facns-133		16	116.24	16	☐	0	22
7	Res-676		19.9	136.14	19.9	☐	0	24.5
8	Facns-124		19.04	155.18	19.04	☐	0	25
9	Eanos_x-59		15.74	170.92	15.74	☐	60	23.56
10	Facns-124		19.04	189.96	19.04	☐	0	25
11	Facns-124		19.04	209	19.04	☐	0	25
12	Eanos_x-59		15.74	224.74	15.74	☐	60	23.56
13	Facns-133		16	240.74	16	☐	0	22
14	Eanos_x-59		15.74	256.48	15.74	☐	60	23.56
15	Eanos_x-59		15.74	272.22	15.74	☐	60	23.56
16	Eanos_x-59		15.74	287.96	15.74	☐	60	23.56
17	Res-676		19.9	307.86	19.9	☐	0	24.5
18	Facns-133		16	323.86	16	☐	0	22
19	BR187	Man01G	18.9	342.76	37.8	☐	0	84
20	Eanos_x-59		15.74	358.5	15.74	☐	60	23.56
21	Eanos_x-59		15.74	374.24	15.74	☐	60	23.56
22	Eanos_x-59		15.74	389.98	15.74	☐	60	23.56
23	Eanos_x-59		15.74	405.72	15.74	☐	60	23.56
24	Facns-133		16	421.72	16	☐	0	22
25	Facns-133		16	437.72	16	☐	0	22
26	Res-676		19.9	457.62	19.9	☐	0	24.5
27	Eanos_x-59		15.74	473.36	15.74	☐	60	23.56
28	Eanos_x-59		15.74	489.1	15.74	☐	60	23.56
29	Facns-124		19.04	508.14	19.04	☐	0	25
30	Facns-133		16	524.14	16	☐	0	22
31	Res-676		19.9	544.04	19.9	☐	0	24.5
32	Res-676		19.9	563.94	19.9	☐	0	24.5
33	Res-676		19.9	583.84	19.9	☐	0	24.5
34	Res-676		19.9	603.74	19.9	☐	0	24.5
35	Facns-124		19.04	622.78	19.04	☐	0	25
36	BR187	Man01G	18.9	641.68	37.8	☐	0	84

Figure 16 - TrainDy software screenshot of the selected trainset

A.3. Simulations on up/down hill, with technical parameters

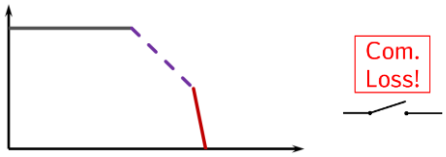
In this section, two train operations are considered (following the simulation results reported in D3.3):

a) Traction up to 30 km/h followed by an emergency braking (9xxx), in braking regime LL and G, when there is a radio communication loss and train is around point UD (see Figure 6 and §9.2 of D3.3):



This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

b) Electrodynamic braking + First Application Step of braking (target pressure in brake pipe is 4.5 bar) followed by an emergency braking (6x1x), when the speed is 30 km/h (starting from 40 km/h), in degraded conditions. This scenario is identical to that of §9.4 reported in D3.3. The braking regimes simulated are both LL and G.



The train operations considered here were the most severe according to D3.3, on up/down hill track.

Since the measuring coach is not braking, the tests with Longo Locomotive braking regime are executed only in BW direction, so that the measuring coach is at the end of the trainset.

The results of next figures consider the variations of technical parameters, identified in D2.2. For the trainset showed in Figure 16, besides the variation of technical parameters identified by the sensitivity analysis, the variation of buffers and draw gears characteristics has been also considered, since FR8RAIL II Partners have provided, for each wagon, some possible alternatives for the elastic characteristics of buffers and draw gears. The results will show that it is more relevant the position on the track than the variation of technical parameters, for the evaluation of LTD.

A.3.1 9xxx up/down hill

Figure 17 shows the in-train forces, their variation and ratio with admissible values (both in compression and in tension) for direction BW, considering braking regime LL and different starting positions, as in §9.2 of D3.3. Figure 18 and Figure 19 refer to braking regime G for FW and BW directions, respectively. In these figures, radio communication among the leading ad guided TUs is missing; the emergency braking is commanded from 30 km/h after traction; the radio communication is lost when the emergency braking is commanded.

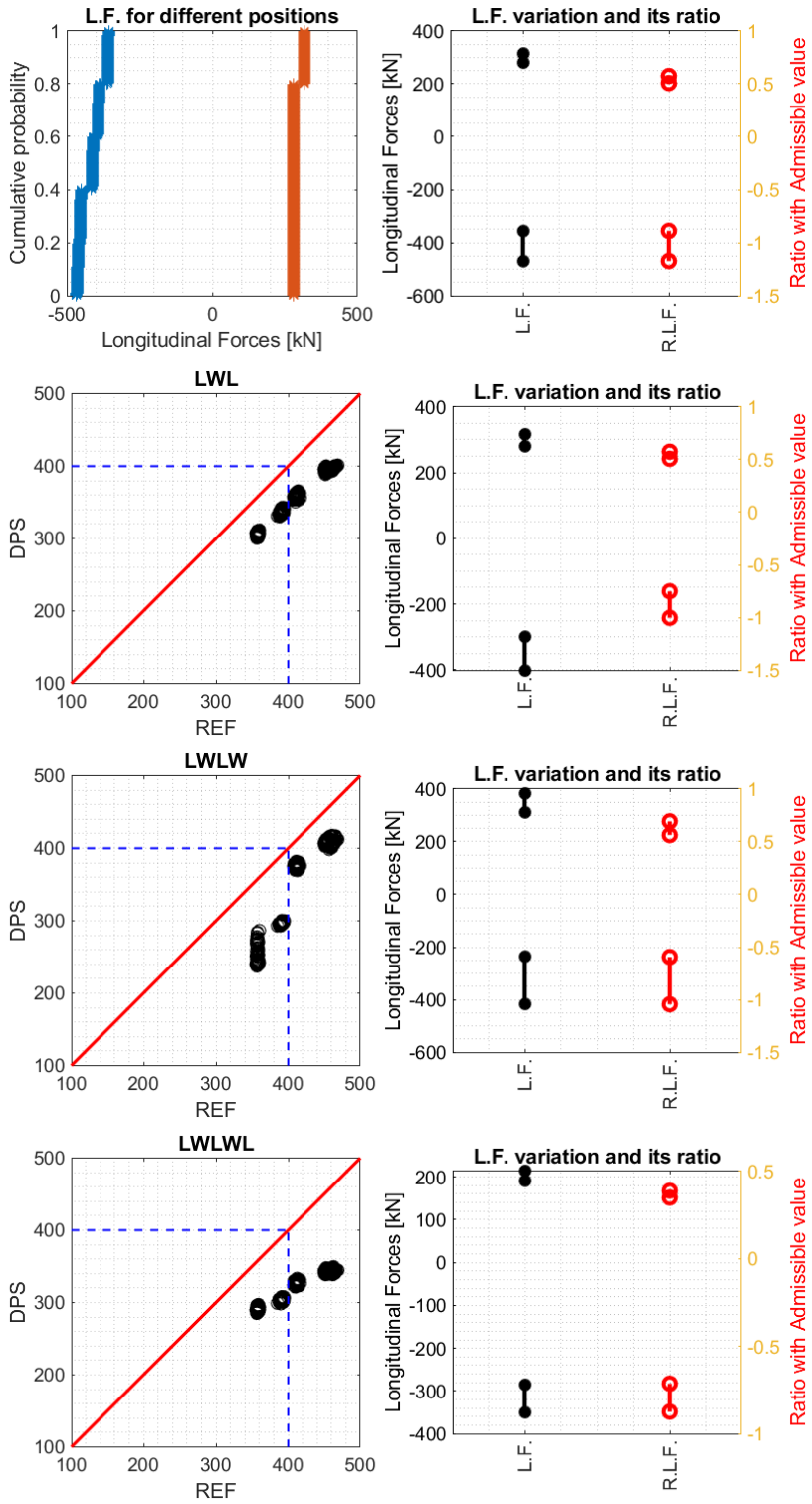


Figure 17 - 9xxx in LL (BW)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

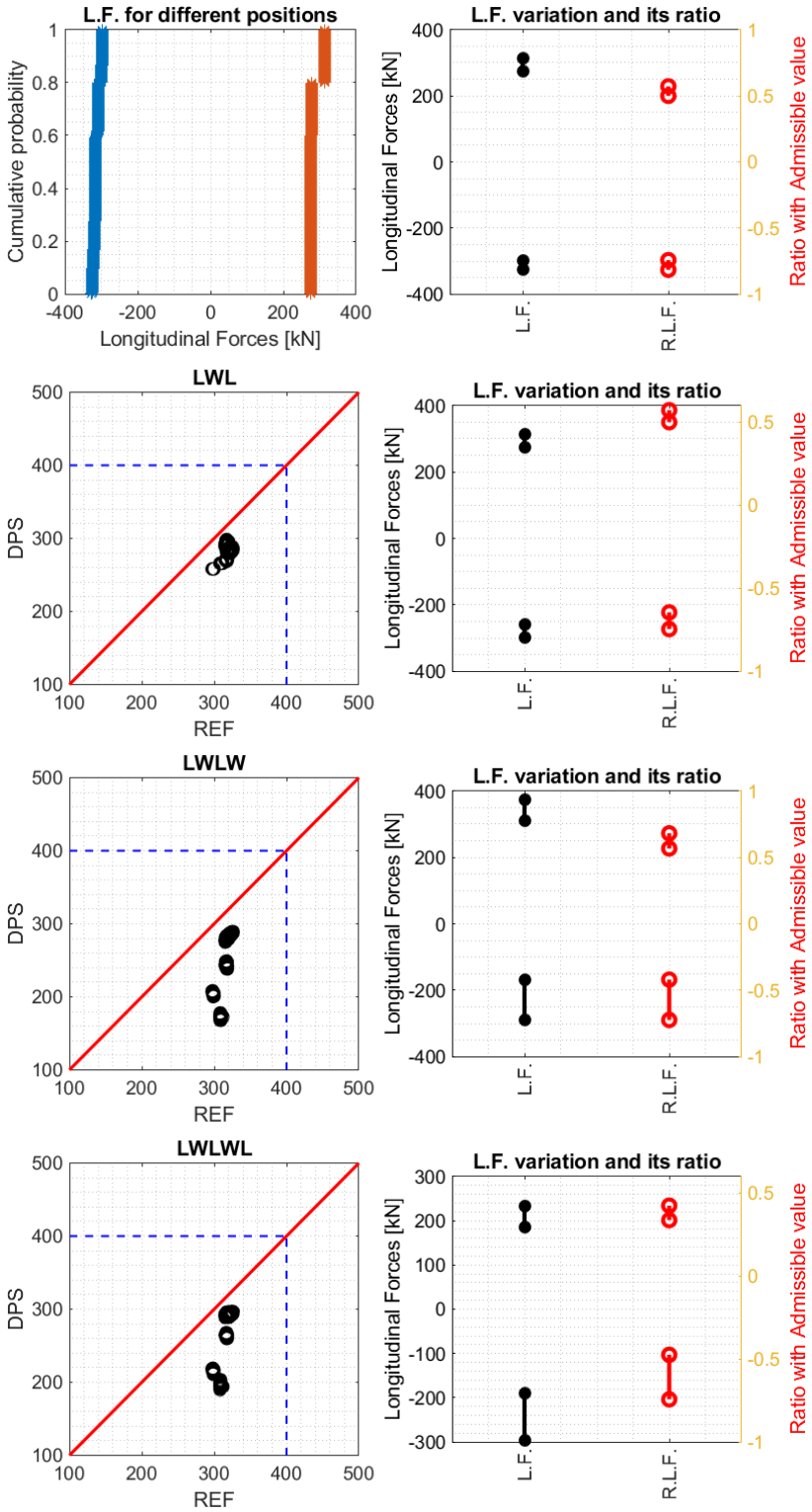


Figure 18 - 9xxx in G (FW)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

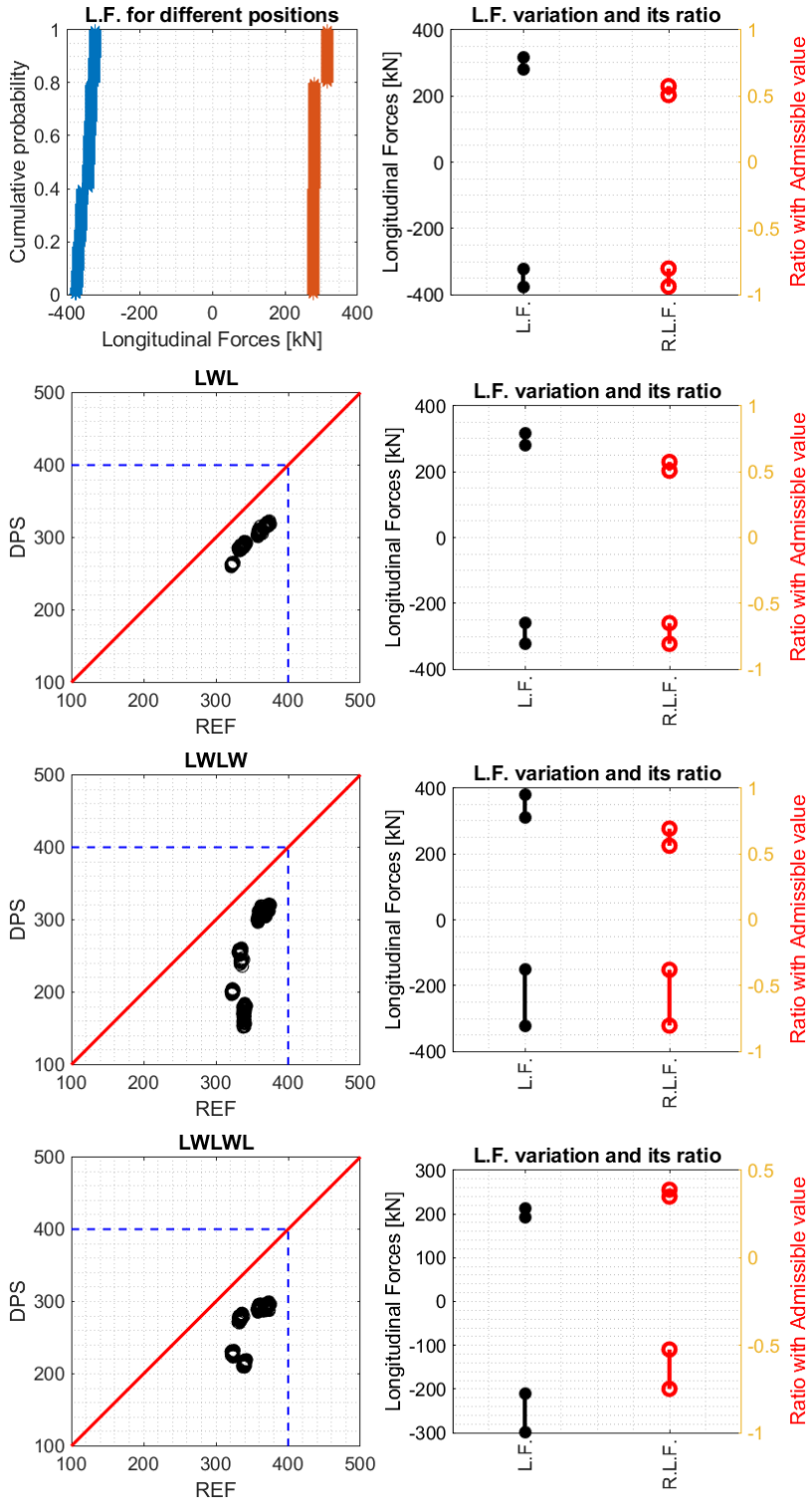


Figure 19 - 9xxx in G (BW)

Above figures confirms that DPS is always beneficial for in-train compressive forces. In LL braking regime, also with DPS, the LCF can be higher than 400 kN, but they are lower than the Reference system. It is worthwhile to underline that when the trainset is in configuration LWLWL, the results have been computed, as in D3.3, with 67% of maximum power at each TU, having in this way the same amount of traction force of the Reference system, roughly; differently, the LCF can be higher than Reference system.

Only for LL braking regime, which provides higher LCF, it is addressed also the condition in which the DPS fails to detect the pressure drop of 0.2 bar in brake pipe: in this condition, the interlock reduces the traction force, when it detects a pressure of 4.5 bar in brake pipe. No other action is required to the Driver, i.e., Driver does not command any braking. In this way, the DPS train is very similar to REF train or it is even safer, as shown by Figure 20.

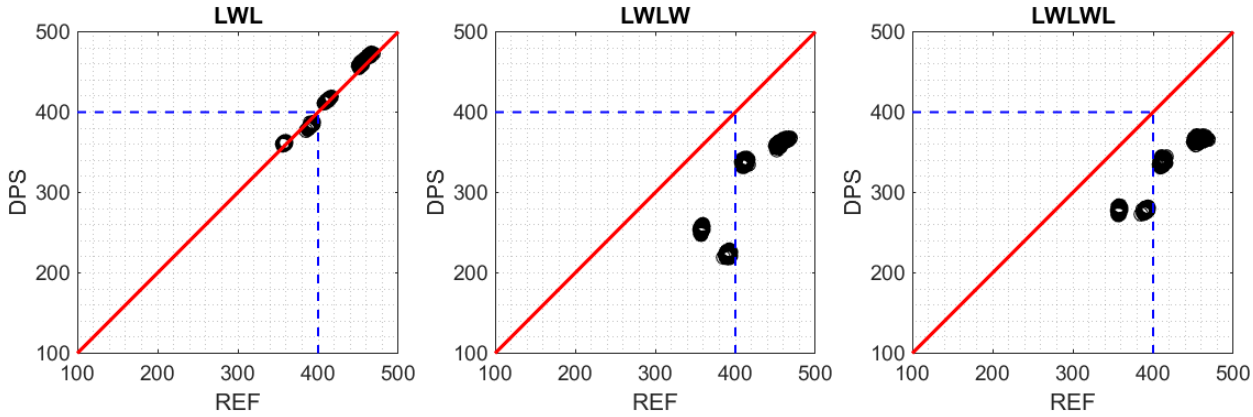


Figure 20 - 9xxx in L (BW), when DPS fails to detect a pressure drop of 0.2 bar and the traction force is removed by interlock system.

A.3.2 6x1x down hill

Figure 21 shows the in-train forces, their variation and ratio with admissible values for direction BW, considering braking regime LL and different starting positions, as in §9.4 of D3.3. Figure 22 and Figure 23 refer to braking regime G for FW and BW directions, respectively. In these figures, the train starting speed is 40 km/h and electrodynamic braking + First Application Step of Braking (target pressure in brake pipe 4.5 bar) are applied; when the speed reached 30 km/h the radio link is lost and the electrodynamic braking is removed after a time of communication loss set to 2.5 s. When the electrodynamic braking is removed the emergency braking is commanded. In this scenario, the DPS trains performs worse than REF trains (in some cases), but the LCF are lower than 400 kN (as in D3.3).

These figures confirm the results of §9.4 of D3.3: in this situation, anyway, the in-train forces are lower because of lower train mass and length. As expected, i.e. as for conventional trains, the in-train forces are higher in LL braking regime than in G.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

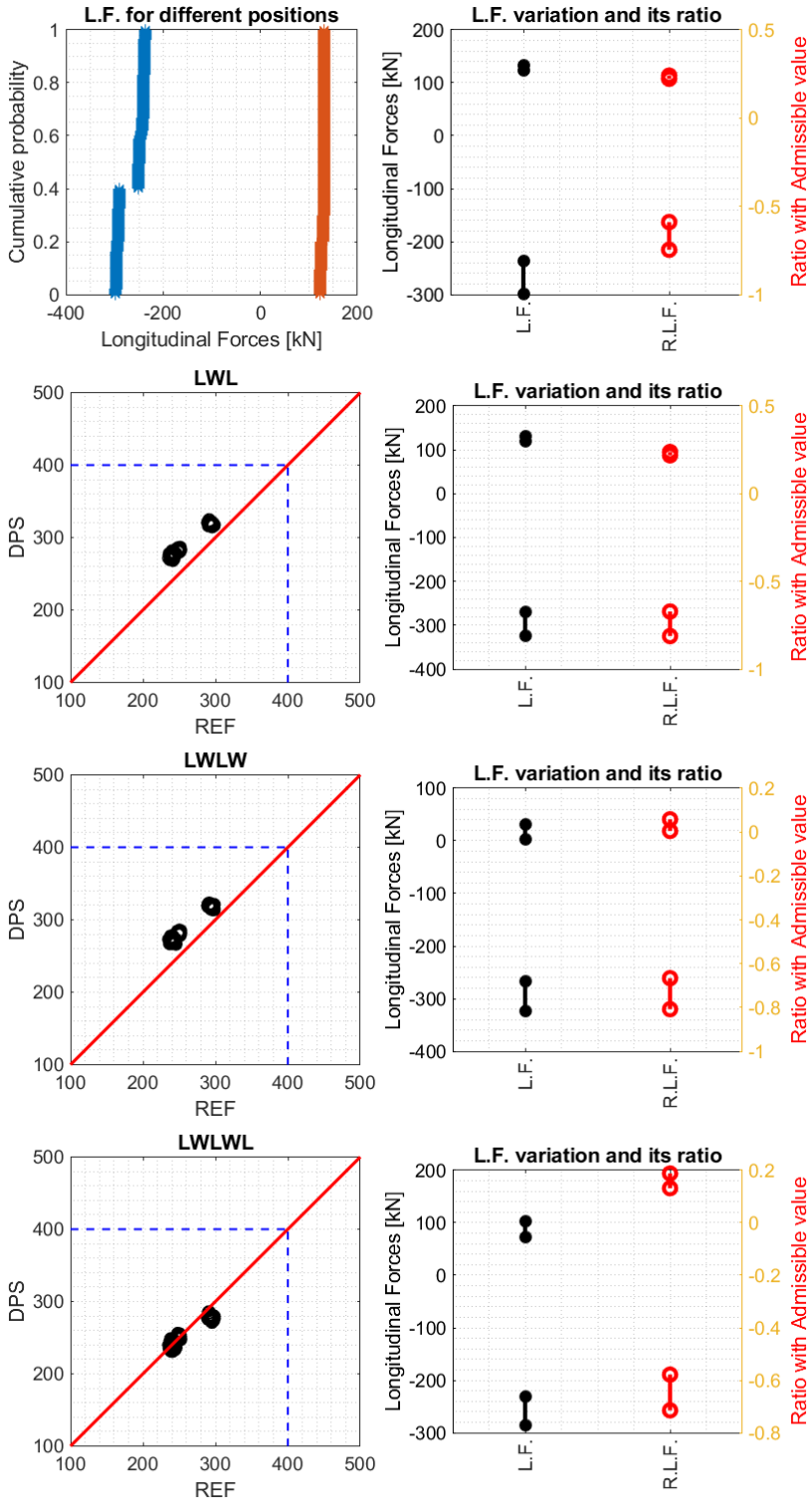


Figure 21 - 6x1x in LL (BW)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

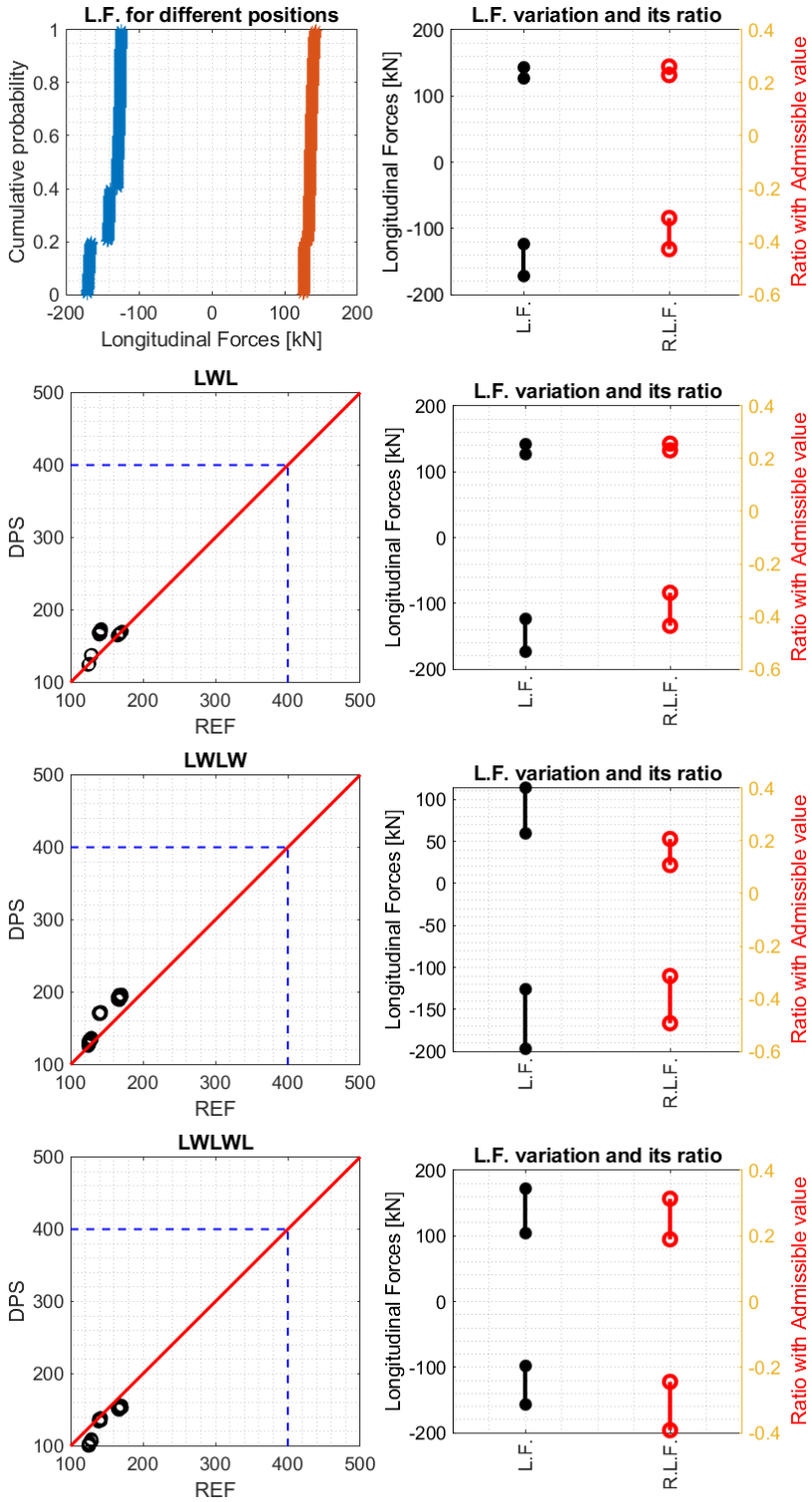


Figure 22 - 6x1x in G (FW)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

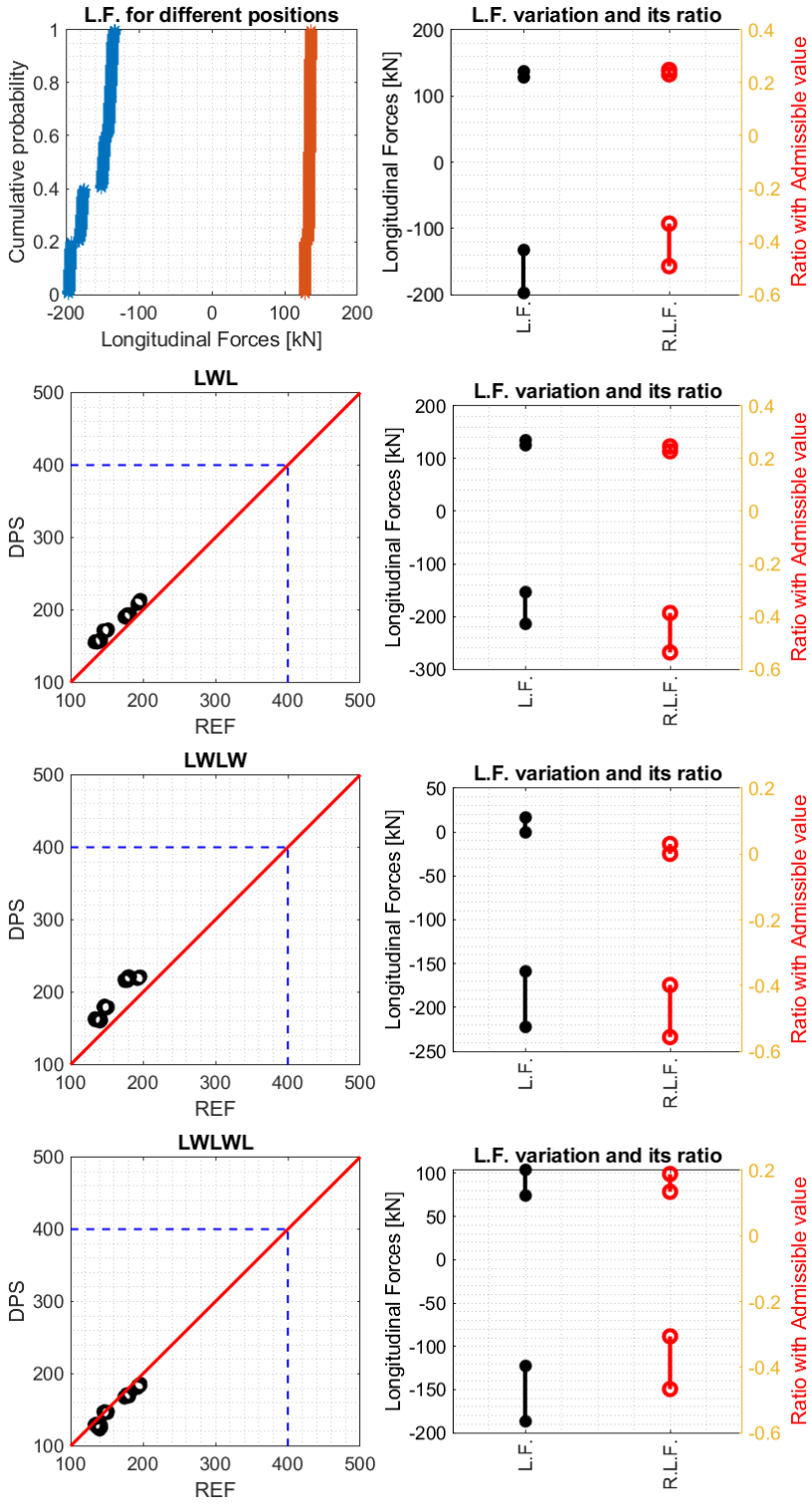


Figure 23 - 6x1x in G (BW)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

A.4. Considerations on stopping distance

This section analyses the performance of DPS in terms of stopping distance, considering the occurrence of DPS failure in detecting the pressure drop of 0.2 bar in brake pipe. The analysis is deterministic and only in regime G, where the highest stopping distances are expected. There is no need employ a statistic analysis to show the benefits of DPS solution since changing the parameters change the numeric results but not the conclusions about the benefits of DPS with respect to the Reference system. The Reference system is considered in nominal mode (5 s delay between the brake pipe venting at first and remote TUs) and in degraded mode (loco interlock intervenes at 4.5 bar and braking is commanded by second Driver when pressure in brake pipe is 3.5 bar).

DPS system is considered working in three ways: On (radio link in "on"), Off (radio link is "off"), Fail (DPS fails in detecting the pressure drop of 0.2 bar in brake pipe).

Two train operations are considered:

- Emergency braking from (full) acceleration (9xxx);
- Emergency braking from coasting (3xxx).

Emergency braking is commanded when train speed is 100 km/h.

The advice coming from simulation on longitudinal forces is to avoid an automatic traction reduction when there is a radio communication loss. Instead of performing a parametric study, with different times for communication loss, the only condition considered is when acceleration is full on all TU and the radio communication loss occurs when the Driver commands the emergency braking: in this way, the traction is kept until:

- DPS detects the pressure drop of 0.2 bar in brake pipe (radio off).
- the interlock intervenes at a pressure drop of 0.5 bar in brake pipe (in case DPS fails to detect 0.2 bar of pressure drop in brake pipe).

Table 16 provides a summary of the results coming from the simulation performed to assess the train stopping distance.

Emergency braking at 100 km/h from full traction				
		Nominal	Degraded	
REF	LWL	863	864	
		On	Off	Fail
DPS	LWL	812	847	864
	LWLW	811	841	855
	LWLWL	833 (806)	875 (844)	898 (860)
Emergency braking at 100 km/h from coasting				
		Nominal	Degraded	
REF	LWL	793	794	
		On	Off	Fail
DPS	LWL	768	789	794
	LWLW	766	792	794
	LWLWL	762	790	794

Table 16 - Results from simulations on stopping distance

The results on stopping distance (measured as difference between the final running distance and the position at which the depression starts in brake pipe at the first TU), show that:

- When radio is working the stopping distances are always better than the reference train. Above consideration usually stands also when radio communication is lost; when this is not true the red colour is used. When the DPS is not able to detect the air pressure drop of 0.2 bar (see Fail column), the stopping distances are the same or lower than the reference system (except for LWLWL in emergency braking after full traction).
- For reference system and train length around 650 m there is no meaningful difference between nominal and degraded condition.
- For emergency braking from full traction, looking at DPS LWLW, when DPS fails detecting the air pressure drop, the stopping distance is lower than case LWL, since the activated TU is in the middle and it detects before the air pressure drop coming from the leading TU and traction force is removed before than case LWL.
- For emergency braking from full traction, looking at DPS LWLWL, there are two sets of results:
  - For full traction: the provided traction force is higher than the REF case (since there are three TUs)
  - For 67% of maximum traction at each TU: the provided traction force is roughly the same of REF case. Results are displayed within parentheses.

  Providing the same amount of power of the reference case results in lower stopping distances also for this trainset. It is important to note that also results on Longitudinal Forces have been computed considering, for traction force, the same amount of reference case, therefore, this result does not provide a bigger constraint.

Looking at UIC 544-1 [12], for this type of train, having a percentage of braked weight around 80%, the allowed stopping distance in brake position G is around 920 m, which is higher than all simulated values.

- For emergency braking from coasting, when the radio connection in on, the stopping distances decrease from LWL to LWLWL: having closer or higher number of discharge points in brake pipe, improves the braking efficiency.
- For at emergency braking from coasting, when the radio connection in lost, the stopping distances are very similar for all positions and number of activated TU: small differences seem caused by a different internal dynamic, which has a minor effect on stopping distance.

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

Appendix B Details on Validation strategy

This appendix provides details on the strategy for the validation of the DPS train Demonstrator(s) set for the execution of the experimental test campaign introduced in §1.5, agreed with the FR8RAIL II partners.

Table 17 concerns the Safety functional requirements, while Table 18 concerns the Technical and Contextual safety requirements, specified during the safety analyses (see §2.4).

The column "Validation strategy" specifies the Verification and Validation (V&V) activities to be finalized (before the test runs) in order to gather evidence of the fulfilment of the applicable mitigations.

The column "Evidence for validation" specifies the sources of the evidence that safety-related requirements are specified, implemented and verified, to be collected before test runs (summarized in Table 7).

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_01	DPS Train shall guarantee the Parking brake application (assuring the standstill condition), specifically during the Train initial test, as for conventional trains.	Parking Brake management	High Safety Integrity level	Functional tests to be performed. Specific procedure concerning the application of the parking brake (manual check if the parking brake is not implemented with high safety integrity level) will be documented in the test specification (including driver instructions).	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation Test specification providing instruction to staff (on handling of the parking brake)
HA_MIT_02	Each Traction unit of DPS train shall be identified during the train inauguration and configuration through a unique identifier (e.g. UIC-train number).	Train inauguration & configuration	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_03	After DPS train inauguration, the train run shall be possible only in case of: _ complete set of valid configuration data, acknowledged by the Driver AND _ positive results from checks of diagnostic function(s) AND _ positive results from valid Train Initial tests, acknowledged by the Driver; _ consistent train orientation at different Traction units, acknowledged by the Driver Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.	Communication set-up & Train inauguration & configuration	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_04	DPS Train shall guarantee the integrity of train configuration data and make impossible any change after a valid Start of mission.	Train inauguration & configuration	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_05	The leading and guided Traction units of DPS train shall monitor the radio communication by a continuous exchange of messages, once established.	Communication set-up & Communication between Traction units	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_06	The DPS Train initial tests shall validate the train configuration and verify the braking capability through the following checks: _ availability of (pneumatic / electric) energy source, according to the inexhaustibility requirement; _ brake pipe integrity (leak); _ brake pipe continuity (extended on DPS train, based on radio communication between Traction units); _ capability to apply the Emergency brake requested by the driver, and through the safety loop and protection systems in the leading and guided Traction units; _ capability to monitor the brake pipe pressure and react to a pressure drop (i.e. to assist the pressure reduction up to the vent of the brake pipe) initiated by the leading Traction unit and by each guided Traction unit.	Train initial test	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_07	The guided Traction units of DPS train shall communicate to the leading Traction unit - by radio - the correct execution of the brake test.	Train initial test	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_08	Driver shall be aware (i.e. informed) on the status of DPS, on the status of the radio communication between the Traction units, on the Parking brake state, on the capability to apply traction and (dynamic and pneumatic) brake forces at every Traction units, and on the active alarms at every Traction units.	Train operational status management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_09	Before the DPS train departure, the leading Traction unit shall communicate (by radio) to all the guided Traction units the orientation set by the driver (at the first set and at any change). Each guided Traction unit shall communicate (by radio) to the leading Traction unit the set train orientation, for the Driver acknowledgment. Otherwise (if the acknowledgment process is not implemented or not possible, e.g. in case of permanent loss of radio communication), a specific test shall be performed before the train departure in order to verify that all the Traction units have a coherent orientation (at the first set and at any change), e.g. by staff verifying the orientation set at the different Traction unit or by operating a small movement of the train.	Train inauguration & configuration	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_10	The leading Traction unit of DPS train shall send commands to all the connected guided Traction units by means of cyclic process data. Non-exhaustive examples of commands are: set point for traction/braking forces, pneumatic brake commands (from driver's controller or protection systems), independent brake (from driver's controller), information for the selection of pantograph (power supply system and voltage), request to raise or lower the pantograph, travel direction, sanding command.	Communication set-up & Communication between Traction units	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations)Report of functional test of functional test before track tests
HA_MIT_11	The radio communication between the leading and guided Traction units of DPS train shall comply with the standards on safety-related communication in open transmission system (EN 50159) and be protected against masqueraded messages, unauthorized access, intentional takeover of the control through unauthorized third parties. and intentional disturbances of radio signals (jamming), e.g. establishing the connection by a secure exchange of pairing keys based on the UIC vehicle numbers.	Communication set-up & Communication between Traction units	Low Safety integrity level	Participating locomotives and data server build up a VPN. LTE security service	M2O deliverables on Radio communication (D2.1)
HA_MIT_12	The leading and guided Traction units of DPS train shall monitor the radio communication and detect a communication interruption if: _the communication channel is terminated abruptly; _OR messages are received with frozen life sign; _OR no valid message is received.	Communication between Traction units	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_13	The leading and guided Traction units of DPS train shall exchange a life sign through radio communication (i.e. to detect interruption, since process data are send periodically).	Communication between Traction units	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations)Report of functional test of functional test before track tests
HA_MIT_15	Each (guided and leading) Traction unit of DPS Train shall apply the traction cut off, with a defined ramp down, in case of interruption of the radio communication with the (leading and guided respectively) Traction units (i.e. if a defined time-out expires). In case of re-establishment of the radio communication, the traction/brake is managed according to the first valid message. In case of long unavailability (I.e. if a second time-out expires), pantographs shall be lowered at each Traction unit and a new train inauguration shall be performed.	Communication between Traction units	Low Safety integrity level	According to the results from LTD simulations (D3.3), there is no benefit in removing traction even if there is a radio communication loss: it is necessary to do so when (and if) the pressure at guided TU reduces by 0.2 bar. HA_MIT_15 will be not implemented.	M2O deliverables on LTD (M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_16	The DPS switch-off and the unavailability of power supply for train equipment shall lead to a safe state by the: _ reset the train inauguration (new train inauguration shall be performed in case of DPS switch-on); _ inhibition of the remote (i.e. by radio) control through the termination of radio communication between the Traction units; _ the brake application in order to maintain or to put the train at standstill condition.	Train operational status management & System de-activation	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_17	After that a traction cut-off command is received from the leading Traction unit of DPS Train, each guided Traction unit shall maintain the traction cut-off until the release command is received from the leading Traction unit.	Traction management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_18	Each Traction unit of DPS Train shall limit the traction and dynamic brake forces to the maximum values specified for the specific application (if applicable).	Traction management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_19	Each Traction unit of DPS Train shall apply the traction cut off if the brake pipe pressure is below a defined limit, independently from the status of the radio connection and received information, with a defined ramp down.	Traction management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_20	The guided Traction units of a DPS Train shall report by radio communication its capability of applying traction and dynamic and pneumatic brake forces to the leading Traction unit.	Traction management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_21	Each Traction units of DSP Train shall monitor the availability of air pressure in the main reservoir detect if no sufficient air pressure is available in its main air reservoir, and trigger an appropriate action (e.g. traction interlock and/or message to driver as for conventional train) inhibiting the train running if the inexhaustibility of the brake is not guaranteed for the entire DPS train. Brake inexhaustibility requirement: without any source of energy for brake actuation (pressure and air flow / electric energy), the Brake system shall guarantee the application of the minimum (Emergency) brake force for at least 2 times (i.e. brake cannot be released if it cannot be applied again).	Emergency brake management	High Safety Integrity level	Test train length, mass, number of axles and axle load will not exceed the allowable limits for the test track. Thus, the supervision of main reservoir pressure of the leading locomotive (including the actions taken when thresholds of the pressure are crossed) is sufficient to guarantee a safe management of this hazard. Inexhaustibility of car brakes is guaranteed by design of the UIC pneumatic brake system. The participating locomotives supply energy from for the brake applications from "Reservebehälter", which guarantees inexhaustibility by their dimensioning.	Test specification providing instruction to staff (reference to the existing procedures / norms on unavailability of air in the main reservoirs)
HA_MIT_22	The guided Traction units of DPS train shall vent the brake pipe when the emergency brake command is received via radio communication from the leading Traction unit.	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_23	Each guided Traction unit of DPS train shall complete any on-going brake application (i.e. assistance to the brake pipe pressure reduction) if the radio communication with the leading Traction unit is interrupted.	Emergency brake management	High Safety Integrity level	Functional tests to be performed.Test train length will not exceed the allowable limits for the test track. Thus, brake pipe venting by leading loco only will still lead to safe stopping.	Functional and system requirement specification (Traceability matrix with mitigations)Report on Functional tests (before test runs)(DPS/TCMS) Software and software test documentation

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_24	Each guided Traction unit of DPS train shall cancel any on-going brake release (i.e. brake pipe refilling shall be inhibited) if the radio communication with the leading Traction unit is interrupted.	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_25	Each Traction unit of DPS train shall guarantee that traction is cut off when brake is applied or brake application is commanded.	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_26	The guided Traction units of DPS train shall report the actual status of the local pneumatic brake (applied/released) and the local measured brake pipe pressure to the leading Traction unit. The leading Traction unit of DPS train shall assure safe condition (no train run, train stop) in case of critical failures (no/ineffective brake or no/incorrect measure of brake pipe pressure) at any (Leading or Guided) Traction unit.	Service brake management	Low Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_27	The Leading Traction unit of a DPS train shall send an emergency brake command to all the guided Traction units (to guarantee the continuity of the brake) and vent the brake pipe (i.e. actuate an Emergency brake) in case of request generated by the driver, OR by the safety loop and protection systems in the leading Traction unit, OR by a EB request coming from a guided Traction unit.	Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level (for BP venting)	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_28	The Leading Traction unit of a DPS train shall apply the Emergency brake (when required) by venting the brake pipe independently from the status of radio communication and from the generation of the command to the guided Traction units.	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_29	The guided Traction units of DPS train, in case of detection of any condition requiring the train stop (i.e. under which conventional train apply EB up to train standstill), shall cut off the traction, vent the brake pipe and communicate the Emergency brake request to the leading Traction unit).	Communication between Traction units & Emergency brake management	High Safety Integrity level (for BP venting)	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_30	The guided Traction units of DPS train, in case of reduction of the brake pipe pressure shall apply the traction cut off with a defined ramp down and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train).	Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))
HA_MIT_31	The leading Traction units of DPS train, in case of reduction of the brake pipe pressure, shall cut off the traction with a defined ramp down, and vent or assist the venting of the brake pipe (by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train). The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train).	Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report of functional test of functional test before track tests
HA_MIT_32	The leading Traction unit of DPS train shall send to the guided Traction units the information on the network system and voltage introduced by the driver and used for the selection of its pantograph and shall verify the consistency of the pantograph selected by the guided Traction unit.	Energy management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations)Report on Functional tests (before test runs)(DPS/TCMS) Software and software test documentation

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_33	The (leading and guided) Traction units of DPS train shall complete the on-going procedure for the lowering of pantographs if the communication between the Traction units is interrupted.	Communication between Traction units & Emergency brake management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_34	The guided Traction units of DPS train shall select the pantograph to be used according to the applicable network and voltage system and shall communicate to the leading Traction unit the selected pantograph.	Energy management	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_35	The leading Traction units shall guarantee the consistency between the information (movement authority, speed restriction, emergency brake) acquired from the trackside signaling (ATP) system and the remote controls provided to the guided Traction units to implement a distributed traction and braking.	Automatic Train Protection	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_36	The On-board ATP of each guided Traction unit in DPS train shall be in an operating mode (e.g. ERTM/ETCS Sleeping mode) guarantying that no train movement supervision is performed.	Automatic Train Protection	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_37	The radio communication between the Traction units of DPS train shall not influence and not be influenced by the radio communication between the on-board and track-side ATP equipment (if used).	Automatic Train Protection	High Safety Integrity level	Antennae have been positioned in such a way that DPS radio signals do not influence GSM-R.	Report on antennae interference
HA_MIT_38	The leading Traction unit of DPS train shall continuously monitor and inform the driver about the status of the guided Traction units, (including traction / brake / alarm).	Diagnostic	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Reference function(s)	Safety Integrity level	Validation strategy	Evidence for validation
HA_MIT_40	The alarms in a guided Traction unit requiring a reaction at DPS train level (e.g. train speed reduction, train stop, activation of protective unit) shall be communicated to the leading Traction unit.	Diagnostic	Low Safety integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
HA_MIT_46	The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition.	Parking brake	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
IHA_MIT_01	The leading and guided Traction units of DPS train equipment shall monitor the pressure in the brake pipe by redundant transducers. In case of low pressure in the brake pipe detected by one transducer the brake is applied. The unavailability / malfunction of one pressure transducer shall be a safety-critical failure and lead to safe condition (train stop and management of brake degradation).	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations) Report on Functional tests (before test runs) (DPS/TCMS) Software and software test documentation
IHA_MIT_02	Each Traction units of DPS train shall implement redundant safety loops for the emergency brake application.In case of one Safety Loop is open (signal = 0) the emergency brake is applied.Inconsistency between the two Safety Loops shall be a safety-critical failure and lead to safe condition (train stop and management of brake degradation).	Emergency brake management	High Safety Integrity level	Functional tests to be performed.	Functional and system requirement specification (Traceability matrix with mitigations)Report on Functional tests (before test runs)(DPS/TCMS) Software and software test documentation

Table 17 - Safety functional requirements and validation strategy and evidence

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
PHA_MIT_01	For each specific application, the compliance of DPS train and track(s) authorized for running to the Technical specifications for interoperability relating to the 'infrastructure' subsystem [1] and to the rolling stock [2] shall be verified.	Test train will only consist of homologated locomotive (one locomotive is not yet fully homologated but permitted for test runs) and wagons. The admission of the test runs will be given by the German rail infrastructure, where TIS-conformance is checked.	Admission for tests
PHA_MIT_02	For each specific application, in order to apply the results obtained by the safety analyses performed during the M20 project, the applicable functional specification and the main data/signals exchanged through the internal interfaces of DPS train shall be (compared and) consistent with the analyzed ones [9], [10] and the elements of the system shall be (compared and) included in the elements of the Integrated system analyzed under the M2O project.	Actual functional specifications will be checked against the version used in safety analyses (M2O deliverable D2.3)	Functional and system requirement specification (Traceability matrix with mitigations)
PHA_MIT_03	For each specific application, the compliance of DPS train with potential restrictions on maximum axle load shall be verified, as for conventional trains.	Test train will only consist of homologated locomotive (one locomotive is not yet fully homologated but permitted for test runs) and wagons. Axle load compliance for locomotives directly follows from being homologated. Axle load compliance can be verified by the wagon list, which includes type, number of axles and gross weight of cars.	Vehicle list Test track (characteristic / limits)
PHA_MIT_04	For each specific application, the presence of (long) bridges shall be addressed with respect to the overall DPS train mass, to the potential cross winds, to the hazardous bridges dynamic behaviour due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.	Test train mass will not exceed the allowable limit for the test track. Test train will not apply any excess brake force over conventional trains with comparable parameters (longitudinal forces). Test train will only consist of homologated locomotive (one locomotive is not yet fully homologated but permitted for test runs) and wagons, with standard geometry (cross winds).	Vehicle list Test track (characteristic / limits)
PHA_MIT_05	For each specific application, the possibility that DPS train is misrouted on a wrong (non-adequate) line shall be addressed and technical and/or procedural mitigations shall be applied if the event is possible.	Test train length, mass and number of axles for test track will not exceed the allowable limits for the test track (as for the Reference system). DPS can be switched off if train is misrouted on track where DPS operation is forbidden	Vehicle list Test track (characteristic / limits)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
PHA_MIT_06	For each specific application, the distance between each main signal and any critical points (e.g. switch point, level crossing, hotbox-detector, balises providing protective messages e.g. stop if in ERTMS Shunting mode) shall be enough to host DPS train.	Test train length will not exceed the allowable limits for the test track.	Vehicle list Test track (characteristic / limits)
PHA_MIT_08	For each specific application, new switch points introduced to allow shunting movement and stop of DPS train (if any) shall be taken into account by the interlocking central logic.	Test train length, mass and number of axles for test track will not exceed the allowable limits for the test track (as for the Reference system).	Vehicle list Test track (characteristic / limits)
PHA_MIT_09	For each specific application, suitable area(s) for coupling of wagons and Traction units, for the execution of Train initial tests and for shunting movement shall be identified (considering the train/units length and needs of manoeuvres).	Test train length will not exceed existing limits (as for the Reference system), for which shunting areas are designed.	Vehicle list Test track (characteristic / limits)
PHA_MIT_10	For each specific application, the manoeuvre of switch point or its release (and blocking for a different route of a different train) shall be possible only after the full passage of the end of DPS train.	Test train number of axles and length will not exceed existing limits (as for the Reference system), for which signalling equipment is designed.	Vehicle list Test track (signalling equipment and verification against vehicle characteristics)
PHA_MIT_11	For each specific application, the switch-on of a level crossing shall be possible only after the full passage of the end of DPS train. The use of timers shall be avoided or specifically verified against the length of trains and related travel time.	Test train number of axles and length will not exceed existing limits (as for the Reference system), for which signalling equipment is designed.	Vehicle list Test track (signalling equipment and verification against vehicle characteristics)
PHA_MIT_12	For each specific application, non-stopping areas (if any) shall be identified, managed by ATP, and known by the driver of DPS train, as for conventional trains.	There are no non-stopping areas in the test track.	Test track (evidence of no non-stopping area)
PHA_MIT_13	For each specific application, the trackside signalling systems (IXL, ATP) shall be able / configured to operate DPS train, considering its total length in the assignment of movement authority and temporary speed restriction.	Test train number of axles and length will not exceed existing limits (as for the Reference system), for which signalling equipment is designed.	Vehicle list Test track (signalling equipment and verification against vehicle characteristics)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
PHA_MIT_14	For each specific application that includes a neutral section between high-voltage power supply systems or involving AC/DC transition, the coherency between the status of pantographs on different Traction units (connection/disconnection from the catenary) shall be guaranteed (by proper interlocks), in order to avoid that concurrent contacts occur with different power supply system. The timing for disconnection and consequent reconnection shall be defined accounting for track characteristics, DPS train configurations (i.e. the position of Traction units) and approaching train speed.	There are no neutral sections in the test track.	Test track (evidence on absence on neutral section)
PHA_MIT_15	For each class of specific applications, it shall be verified that the in-train longitudinal forces in DPS train are acceptable (compared to absolute limits or to a Reference train configuration already authorized for operation) in all the conditions defined by the train configuration (position of Traction units and loaded wagons), credible degraded operating modes (interruption of radio communication), train manoeuvres (traction, brake, particular operations), and track characteristics (e.g. maximum track gradient). Unsafe Train configurations (i.e. distribution of loaded wagons) shall be identified (if any) by simulations of in-train longitudinal forces and braking distance of DPS trains.	LTD simulations are performed on family of trains having length between 720 and 740 m (TU included) and hauled mass between 1800 and 1850 ton (generated according to UIC Leaflet 421) and on the specific configuration defined for Demonstrator(s). The relative approach envisaged by UIC Leaflet 421 is followed. The Longitudinal Compressive Forces (LCF) and Longitudinal Tensile Forces (LTF) are evaluated under different operative conditions (i.e. different train operations or man oeuvres and different track positions) and compared. DPS trains have not higher Longitudinal. LTD simulations are mainly focused on in-train longitudinal forces. Indeed, stopping distance of DPS trains is always less than the stopping distance of Reference trains. Additional studies have been performed, confirming that the stopping distance of DPS train at high speed is always less than for the Reference trains. Train operations is simulated at the positions with the maximum gradient along the track between Kronach and Probstzella (maximum slope equal 27‰), in order to emphasize the effects on longitudinal train dynamics, for different degraded operating modes and manoeuvres.	M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
PHA_MIT_16	For each class of specific application, train equipment (braking system in each Traction unit) shall guarantee the application of brake forces consistently with the operational status and the commands received. The acceptability of degraded conditions (due to failures leading to a reduction of the braking effort), if defined, shall be verified by simulations of in-train longitudinal forces and braking distance.	Maximum brake force of train is not affected by DPS implementation. Brake built-up time is either significantly less ("nominal mode - radio on"), slightly less ("radio off") or the same (DPS off) as in the Reference system. Reduced braking effort means reduced longitudinal force (no systematic increase of longitudinal force). No specific LTD simulation is performed in case of hazardous failure of brakes, having the same risk (related to an increase of braking distance) than in the Reference system.	Loco safety documentation M2O deliverables on LTD (D3.3 on DPS train family & D3.2 on DPS train Demonstrator(s))
PHA_MIT_17	For each class of specific applications, it shall be verified that in-train longitudinal forces and braking distance of DPS trains are acceptable (compared to absolute limits or to a reference train configuration already authorized for operation), accounting for: the (worst case) time required for EB application, when a command generated by the control system is received by the brake system; the time needed to generate this command: a. worst case with radio on (includes performance of the control system and uncertainty on radio communication latency); b. worst case with radio off (includes performance of the control system, with the pressure sensors on the brake pipe).	Waiting for experimental data on LTE technology, coming from the FR8RAIL II experimental tests, the delay between the command at the leading TU and the filling/venting of brake pipe at guided TU is modelled (in the LTD studies) by a Gaussian random variable, with a time interval 0.9 s +/- 15%. This "system wide latency (driver at leading TU → … → brake pipe valve of guided TU)" is based on the latency between Train Controller Unit and Radio Controller (RCDPS) for both TU's (end-to-end with radio communication) valued by laboratory test and validated by experimental test runs (by adding 0.5 s), both based on GSM-R [18]. Anyway, concerning the DPS Train Demonstrators, the time required for EB application is no longer than that in the Reference system, where the second driver actuate the brake after 5 s (mean value, with coefficient of variation equal to 0.1) or when the pressure in the brake pipe is equal or lower to 3.5 bar (when, for short train as for DPS Demonstrators, the brake is already effective, as verified by the specific LTD simulations).	M2O deliverables on LTD (D3.3 on DPS train family & D3.2 on DPS train Demonstrator(s))

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
PHA_MIT_18	For each class of specific applications, if the effective brake (sum of dynamic and pneumatic braking contributions) could decrease in case of loss of the radio communication between the Traction units of DPS train, simulations shall demonstrate that (because of potential train acceleration) braking distance degradation and in-train longitudinal forces are still acceptable. The contribution of dynamic brake shall not be considered for the fulfilment of braking distance (if/as applicable).	LTD simulations are performed considering ED removal when the train is in a slope section under degraded operation condition due to the loss of radio communication between TUs.	M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))
PHA_MIT_19	For each class of specific applications, the maximum traction effort and dynamic braking forces shall be specified for each Traction unit, for each DPS train configuration. The acceptability of in-train longitudinal forces in case of different traction levels applied in different Traction units shall be verified by simulations of in-train longitudinal forces and braking distance.	Longitudinal forces experienced by Demonstrator(s), with their limits of traction force, are assessed (and verified against the Reference system) by LTD simulations. LTD simulations are performed by applying the maximum braking force by all wagons and the maximum traction forces force is applied by all TUs. If the traction or braking forces are lower than their maximum values, the LTD is less enhanced. Specific study is performed for train-consist LWLWL, assuming different traction forces applied by TUs.	M2O deliverables on LTD (D2.2 and D3.1 on preliminary and general DPS Train simulations, D3.3 on DPS Train Demonstrator(s) family, D3.2 on DPS Train Demonstrator(s))
PHA_MIT_20	For each specific application, the fulfilment of the Safety-Related Application Conditions exported to DPS train and related operation by the signalling systems (trackside and on-board Automatic Train Protection, Interlocking) shall be verified (with focus on the maximum length of DPS train).	Test train number of axles and length will not exceed existing limits (as for the Reference system), for which signalling equipment is designed.	Vehicle list Test track (signalling equipment and verification against vehicle characteristics)
PHA_MIT_21	For each specific application, the fulfilment of the Safety-Related Application Conditions exported to DPS train and related operation by the Train detection system (track circuit OR axles counter) shall be verified (with focus on the potential impact of a high number of axles OR of block sections simultaneously occupied).	Test train number of axles and length will not exceed existing limits (as for the Reference system), for which signalling equipment is designed.	Vehicle list Test track (characteristic / limits)
PHA_MIT_35	For each specific application, the position of the main signals shall be verified considering the extension of the train at standstill condition (based on the type and length of the DPS train).	Train does not exceed length limit of conventional trains on the test track.	Vehicle list Test track (characteristic / limits)
PHA_MIT_36	For each specific application, the need to isolate the Traction units from the power supply system when the train is at standstill condition shall be addressed, according to the applicable rules for conventional trains.	Isolation of traction units in standstill will be documented in the test specification (including driver instructions).	Test specification providing instruction to staff (on Isolation of traction units in standstill)

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement no. 826087 (M2O)

ID	Description	Validation strategy	Evidence for validation
HA_MIT_14	The radio communication between the leading and guided Traction units of DPS train shall comply with the standard for safety-related communication in open transmission system (EN 50159) and based on a Safety Layer providing measures against communication threats (messages corruption, resequencing, repetition, insertion), managed by devices compliant with the standard for safety-related electronic systems for signalling (EN 50129).	Use of Safety layer for SIL2 railway application	Specification of Safety layer for TUS radio communication
HA_MIT_39	The alarms in a guided Traction unit requiring a reaction at DPS train level (e.g. Wheel slide protection defective, Battery charger malfunction, Traction motor temperature alarm, Status interference current monitoring tripped) shall be identified.	Identification of alarms in each guided locomotive is part of its TCMS/Diagnostic system, which is in operation during test runs. Safety relevant alarms are communicated to leading locomotive.	(DPS/TCMS) Software and software test documentation

Table 18 - Technical and Contextual safety requirements and validation strategy and evidence