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 2.3

Integrated system, Safety report

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 21
Actual submission date:	21-01-2021
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*
0.1	24/05/2020	First draft
0.2	20/07/2020	Second draft (M2O internal review is still on-going)
0.3	22/07/2020	Third draft (M2O and FR8RAILII review is still on-going)
0.4	17/11/2020	Fourth draft after FR8RAILII review. IHA included
1.0	26/11/2020	First delivery
1.1	21/01/2021	Updating according to comments on v1.0 (27/11/2020) from the Project Officer: updating of Figure 1. Change of wording of PHA_MIT_17.

Report contributors		
Name	*Beneficiary Short Name*	*Details of contribution*
Stefano La Rovere	NIER	Definition of the methodology for the safety analyses. Development of safety analyses. Discussion of results.
Daniele Vitale	NIER	Definition of the methodology for the safety analyses. Development of safety analyses. Production of the deliverable.
Armand Toubol	NEW OPERA	Development of safety analyses. Discussion of results.
Luciano Cantone	University of Rome, Tor Vergata	Discussion of results.

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)

1 Introduction

1.1 M20 project

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. The market requirement are competitiveness, reliability, flexibility, frequency and information. The previous FP7 MARATHON project [8] demonstrators have shown the feasibility of 1500m long coupled heavy trains with distributed power of two Traction Units (TU) running safely on the French network. Building on that, M2O intends to extend the possibilities to multiple Traction units as Distributed Power System (DPS), in collaboration with FR8RAILII project. To reach this goal, a reliable radio communication is implemented to transfer data between the Traction units and integrated with DPS.

Within the above context, the safety of "DPS train" is studied in order to address the specific (new or modified) functions and their possible interaction with other elements of the operational contexts (trackside or on-board equipment) and to cope with the various operational situations.

1.2 Purpose and scope

The present deliverable concerns the safety activities performed during the M20 project and specifically during the Work-Package 2 (task 2.3), including:

- the specification of a Safety plan focused on the activities performed during the M2O project;
- the development of safety analyses focused on the Integrated system including a generic implementation of "long freight trains" based on Distributed Power System and radio communication (independently from the specific technology adopted) and trackside's elements (belonging to the Infrastructure or to Signalling systems).

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 demonstrators (WP3), through the specification of mitigations to be implemented by the DPS train or fulfilled by the operational context.

The scope of the safety analyses performed during the M20 project is defined:

- by the elements of the Integrated system listed in Table 1;
- by the DPS train functional behavior defined under the FR8RAILII project [9], [10].

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)

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.

In order to apply the results obtained by the safety analyses performed during the M20 project to a specific application of DPS train, the applicable functional specification 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.

1.3 Structure of the document

The structure of the document is the following:

- §1 - Introduction, which provides general information on the purpose, scope and content of this document;
- §2 - General information, which concerns the definition of the operational context of DPS trains and the specification of the Safety plan of the activities performed during M2O project;
- §3 - Preliminary Hazard Analysis, which provides a brief description of the adopted methodology and the results obtained by the Preliminary Hazard Analysis;
- §4 - Hazard Analysis, which describes the adopted methodology and provides the results obtained by the Hazard Analysis;
- §5 - Interface Hazard Analysis, which describes the adopted methodology and provides the results obtained by the Interface Hazard Analysis;
- §6 - Summary of results from safety analyses, which provides a summary of the main results coming from the safety analyses and specifically the list of hazards, the Safety Integrity level assigned to the functions implemented by DPS train and the reference to the Hazard Log;
- §7 - Conclusion, which provides summary considerations on the activities and results;
- §8 - Acronyms, which provides the list of acronyms used in this document;
- §9 - References, which provides the list of references used in this document.

This document also includes the following appendixes:

- Appendix A - **Preliminary Hazard Analysis table**;
- Appendix B - **Hazard Analysis table**;
- *Appendix C* - Interface Hazard Analysis*;*
- *Appendix D* - Hazard Log.

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 General information

2.1 System definition

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

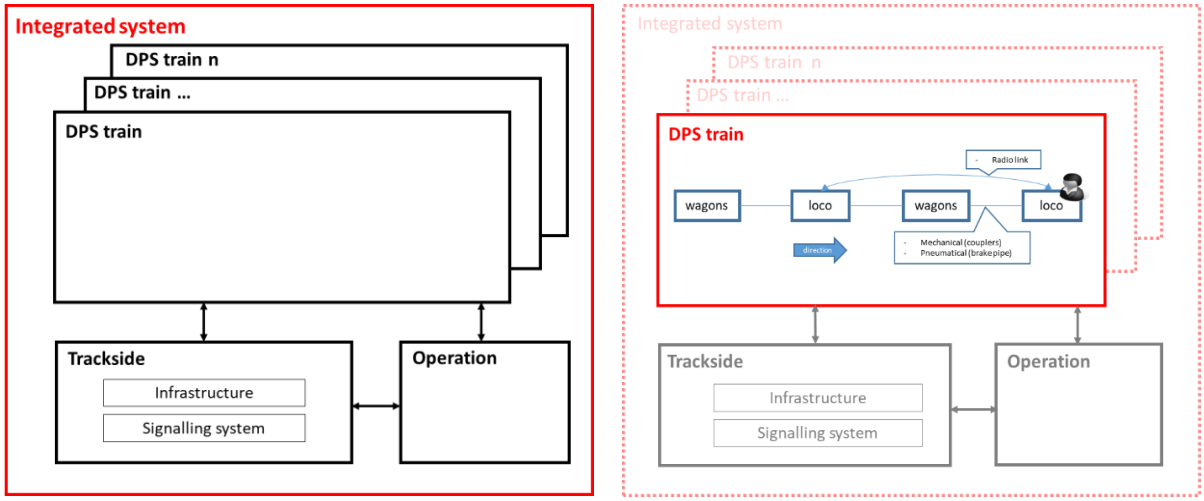

Figure 1 - General context, and "Long freight train" Integrated system (left) and DPS train (right)

The picture on the left side in Figure 1 represents the whole "Integrated system", including different "long freight trains" equipped by Radio communication and Distributed Power System (DPS trains) and the trackside elements. The Integrated system is considered in the following Preliminary Hazard Analysis (see §2.3.4). The picture on the right side focuses on a single DPS train, with its external interfaces with trackside elements and other trains. The single DPS train, including the leading traction unit (TU) and up to four guided TUs, is considered in the following Hazard Analysis (see §4).

According to §1.2, the scope of the safety analyses is defined:

- by the elements of the Integrated system, including "long freight trains" based on Distributed Power System and radio communication and trackside's elements;
- by the DPS train functional behavior defined under the FR8RAILII project [9], [10].

Table 1 provides the hierarchical list of the different elements / factors of the Integrated system. The first level includes the trackside elements (belonging to the Infrastructure or to Signalling systems), the DPS train and some operational topics. It will be used in the Preliminary Hazard Analysis to evaluate if the specific characteristics of DPS train could lead to specific hazardous conditions due to interactions with the infrastructure, signalling systems and train devices.

This list has been defined by catching the representative elements of the railway systems from the Infrastructure [1] and Rolling Stock [2] Technical Specifications for Interoperability (TSI). Anyway the completeness of this list shall be verified for each specific application of DPS train, i.e. with reference to the specific DPS train configuration and tracks.

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	-
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 and wagons) coupling and decoupling	-

Table 1 - Integrated system, relevant elements / factors

The functional behavior of DPS train, which defines the scope of the following analysis, is defined in the documents made available by the FR8RAILII project:

- System Requirements LT V6 [9];
- D5.2 - Functional and system requirements specification [10].

Based on the Functional and system requirements specification [10], the "specific" functions implemented by DPS trains in the two main phases - Train set-up and Train run - are listed and singularly described in Table 2. 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 [10]
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

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)

Phase	Main function	Description	Reference to [10]
	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

2.2 Safety goals

A first set of safety goals for DPS train is specified in the System Requirements document made available by the FR8RAILII project [9] and provided in Table 3.

System requirement - ID	System requirement – text
DB_REQ_LT_V6: 37	The operation of DPS must not compromise the operation of Traction units in other trains or yards in conventional operation.
DB_REQ_LT_V6: 38	The operation of DPS must not compromise the existing infrastructure.
DB_REQ_LT_V6: 42	The restrictions of the positions of the TU must be identified from a train dynamic perspective.
DB_REQ_LT_V6: 67	The DPS must master the longitudinal forces and tractive effort so that at least the existing safety level in the reference system is achieved with trains in conventional traction. This applies to all train configurations, speeds, inclinations, track radii and, in general, all regular operating conditions of the train. Emergency braking is a regular operating condition, too.
DB_REQ_LT_V6: 68	The allowed braking distances are always to be complied with as today.[1]
DB_REQ_LT_V6: 33	The technical system shall comply with the national and international standards and regulations set up in the agreed verification plan. [2]
DB_REQ_LT_V6: 34	The maintenance, safety and work safety aspects must be taken into account.
DB_REQ_LT_V6: 35	The execution and the verification are carried out in accordance with EN 50126 DIN EN 50128. The details are regulated by the agreed verification plan.

Table 3 - DPS Safety objectives

[1] I.e. criteria and limits stated for the braking distances of existing (i.e. authorized) trains also apply to DPS trains based on radio communication.

[2] This document provides the plan of the safety activities performed within the M2O project.

2.3 Safety plan

This section is the Safety plan developed for the activities to be performed during M2O project. Specifically, this Safety plan:

- specifies the safety activities to be performed for the system definition and operation (WP2) and for the safety demonstration of the demonstrators (WP3) and their relations with the different phases stated by the EN 50126 [3](as possible);
- specifies relations between M2O and FR8RAILII projects in the development of safety activities;
- provides insights on the management of safety requirements coming from safety analyses;
- describes the content of the Hazard log;
- 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].

2.3.1 Relationship with FR8RAIL II project

The safety activities concerning the DPS trains based on radio communication and the specific demonstrators for test runs will be performed under the M2O and FR8RAILII projects.

The safety activities performed during the M2O project are based on the input provided by the FR8RAILII project; specifically:

- the scope of the safety analyses (provided by this document), which is defined by the functional specifications made available by the FR8RAILII project [9], [10];
- the scope of the train dynamics simulations (developed during the WP3 of the M2O project), which is defined by the configuration of the DPS train demonstrators and the characteristics of the track for test runs, which will be made available by the FR8RAILII project;
- the evidences of the fulfilment of the mitigations specified by the performed safety analyses by the DPS demonstrators set for test runs will be provided by the FR8RAILII project.
- the traceability between the mitigations specified by the hazard analyses and the (safety) requirements specified for DPS train, the characteristics of the test track and the procedures for the test runs execution will be independently verified during the WP3 of the M2O project;
- the evidences of the implementation of the (safety) requirements specified for DPS train (that will be gathered during the WP3 of the M2O project, if (if any).

The content and the results of the safety analyses performed during the M2O project (provided by this document), of the train dynamics simulations and of the safety verification activities will be shared with and reviewed by the safety experts of the FR8RAILII project.

The effective verification of the implementation of the (safety) requirements specified for DPS train depends on the information that will be made available from FR8RAILII project (e.g. concerning the Generic application of the DPS train subsystems).

2.3.2 Safety activities

The safety activities to be performed during the M2O project include:

- Safety analyses, including a Preliminary Hazard Analyses (PHA), a Hazard Analysis (HA) and an Interface Hazard Analysis (IHA);
- In-train longitudinal force simulations in the most critical operational situations;
- Safety Verification and validation activities.

Safety analyses are focused on the Integrated system housing long freight trains, on the functional specifications and on the architecture implemented for DPS train, as defined by FR8RAILII project. They provide the safety requirements to be implemented by DPS trains and to be exported as Safety related Application Condition to the other elements of the Integrated system.

In-train longitudinal forces simulations will be performed (during WP3) to support the safety demonstration of the DPS train implementation, with a focus on the configuration of the DPS train demonstrators and on the specific characteristics of the operational context for test runs. A comparison among new trainsets and already running (and implicitly safe) trainsets will be developed by means of "relative approach": Trainsets already in operation (assumed to be safe) and new trainsets applying DPS technology are statistically simulated by TrainDy and new trainsets are considered "safe", with respect to the risk coming from high in-train forces, if they have a lower or equal ratio of in-train forces to admissible forces when comparing to current trainsets.. Admissible in-train compressive forces, will be computed according correlations available in UIC codes and/or ERRI reports. Admissible longitudinal compressive forces will be computed considering the minimum track radius of curvature in the area of interest. These topics are addressed in a dedicated deliverable (D3.3 during WP3).

The Safety Verification and validation activities will be performed (during WP3) and focused on the demonstrators of DPS train.

Figure 2 provides the V-cycle representation introduced by the EN50126 [3] and shows the "position" of the above safety activities.

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)

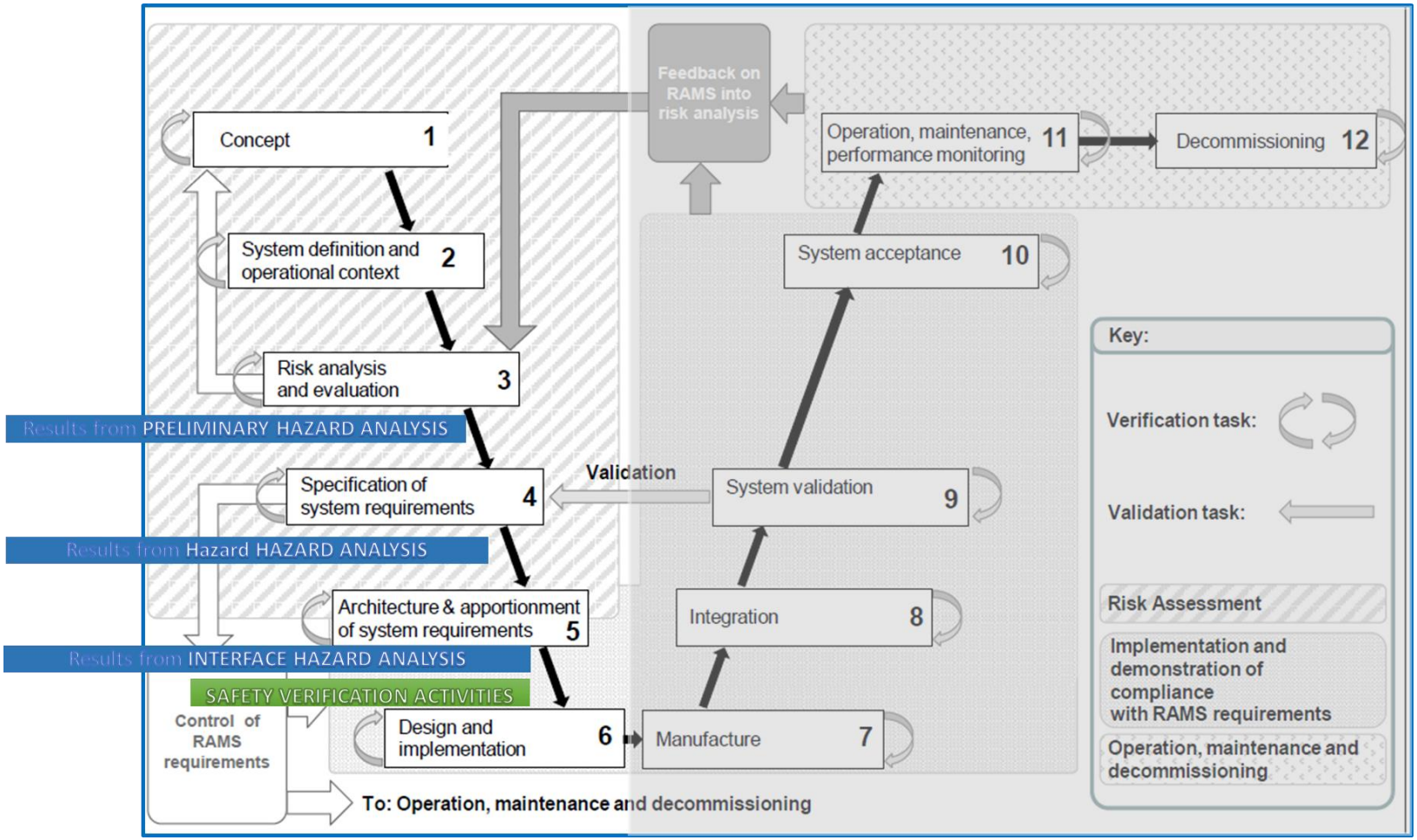

Figure 2 - V&V Cycle and Safety activities

2.3.3 Safety analysis

Three main safety analyses are developed within the M2O project:

- Preliminary Hazard analysis (PHA) developed for the entire Integrated system;
- Hazard Analysis (HA), based on the functional and system requirements of DPS trains;
- Interface Hazard Analysis, based on the specific architecture implemented for DPS train.

The above safety analyses are developed with the common objectives to identify hazardous conditions related to the operation of DPS train and to specify proper mitigations, from different perspectives and details of Input information.

Figure 3 provides details on the safety analyses developed during the M2O project.

The **Preliminary Hazard analysis** (PHA) is developed for the entire Integrated system including long freight trains in their operational context, as defined in §1.1 (see Figure 1). Specifically, the elements listed in Table 1 define the scope of the PHA. Input information comes from previous experience, i.e. previous S2R project or more generally previous demonstrators of long freight trains. The PHA has the objective to identify the elements/factors (of the infrastructure, signalling systems, 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 **Hazard Analysis** (HA) is developed for a specific implementation of DPS train (see Figure 1). The main input is the Functional and system requirements specification [7], [10] provided by FR8RAILII project. The HA has the objective to identify further mitigations, including functional, technical and contextual safety requirements, based on a set of functional requirements specifying the DPS train implementation [10].

The **Interface Hazard Analysis** (IHA) is developed for a specific implementation of DPS train. Input information concern the Functional and system requirements specification [7], [10] and a high level representation of DPS train architecture (instantiated in this document, see Figure 4). The IHA has the objective to assess the potential deviations in the data and signals exchanged between DPS train subsystems (i.e. thought its internal interfaces).

According to Figure 3, the main results coming from the above safety analyses are the:

- list of hazards (provided in §6.1);
- Safety Integrity Level allocated to the DPS train functions (provided in §6.2);
- mitigations, including Safety requirements to be implemented by DPS train and Safety-Related Application Conditions to be met for its operational context).

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)

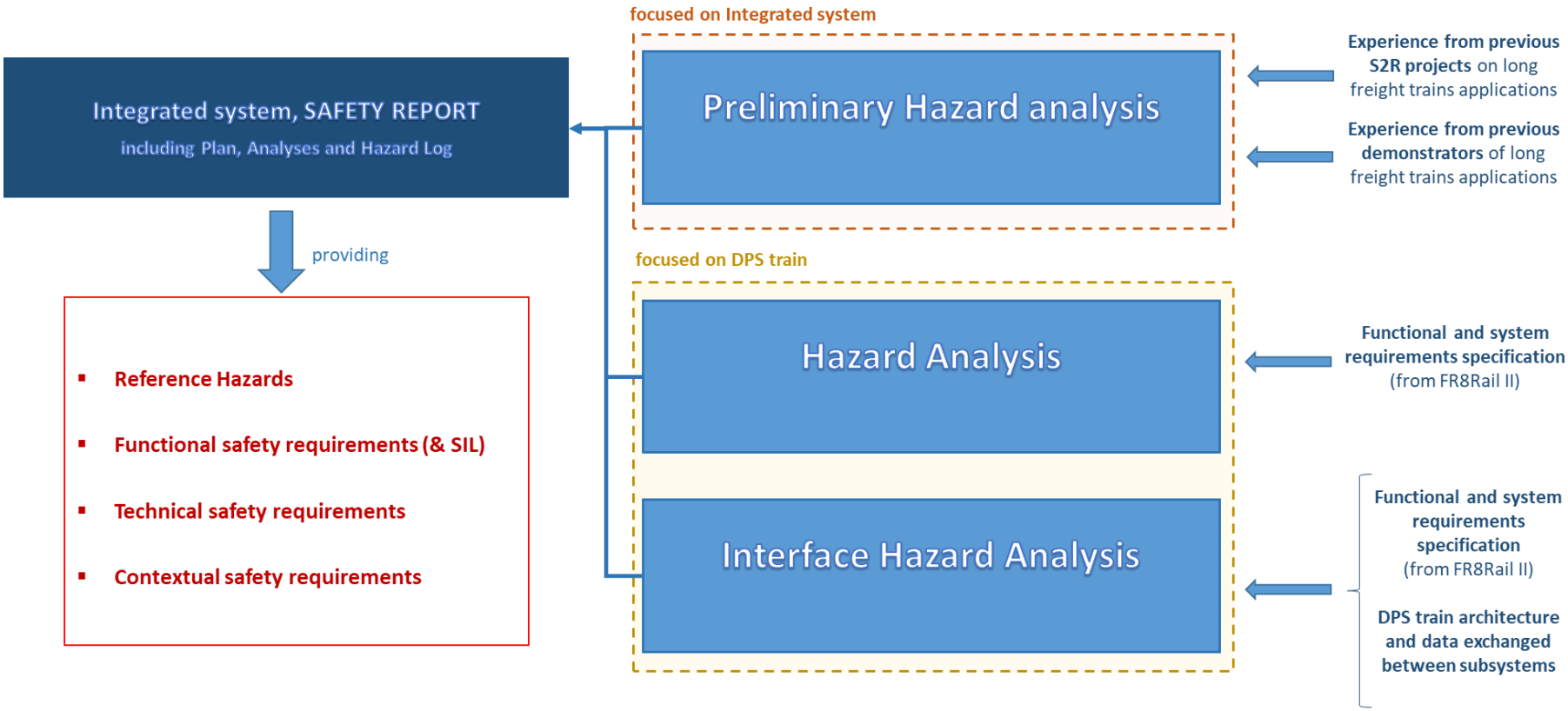

Figure 3 - Safety analysis process and activities

2.3.4 Safety requirements

The requirements to be met for the safe operation of DPS train are specified through the development of safety analysis described in §2.3.3.

The mitigations specified during these safety analyses include safety requirements to be implemented by the DPS trains and to be exported to other elements of the Integrated system (i.e. safety-related application conditions).

These mitigations are classified in:

- Functional safety requirements;
- Technical safety requirements;
- Contextual safety requirements.

These categories are defined in the EN50126 (Part2) [4], with the following definitions.

Functional safety requirements have to be implemented by the DPS train. They 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 concern constraints for the design, installation and use of the system, including the conformity to standards, regulation, and codes of practice. They include both safety requirements to be implemented by the DPS and application conditions to be exported to other elements.

Contextual safety requirements cover operational and maintenance tasks. They are application conditions to be exported to the Operators in charge of the setting of a proper operational context for DPS train. They could concern:

- specific actions expected for any category of personnel concerned (driver / staff);
- the expected operational procedures for normal and abnormal modes;

Contextual safety requirements also include the assumptions about safety-related operational restrictions, if any.

With reference to the above categorization and the safety analyses introduced in §2.3.3:

- mitigations coming from PHA are expected to be (mainly) technical and contextual safety requirements;
- mitigations coming from HA are expected to be (mainly) functional safety requirements.
- mitigations coming from IHA are expected to be (mainly) technical 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)

2.3.5 Safety Verification and Validation activities

The Safety Verification and Validation activities will be performed for the demonstrators of DPS train and focused on:

- radio communication, with focus on the implementation of a proper communication protocol[3] and on cyber-security issues in the execution of test runs;
- the evidences of the fulfillment of the mitigations specified in the safety analyses (provided by this document) by the DPS train demonstrators that will be made available by the FR8RAILII project and will be gathered in a dedicated Technical Safety Report;
- on the train dynamics simulations and specifically on the consistency of input and assumptions with the expected behaviour of DPS trains (including radio communication) and with the specific characteristic of the test runs (e.g. concerning the test track, the trainset configurations, the manoeuvres to be performed under the operational and degraded operating modes), the consistency of the conclusions derived from the numerical results with the procedural rules and the tests plan specified for the DPS train demonstrators, including constraints on the trainset configuration, speed limits and non-admitted manoeuvres, if any.

According to §2.3.1, FR8RAILII project will provide a traceability matrix between the mitigations specified by the safety analyses - and classified as Functional safety requirements - with the set of requirements specified for the development of the DPS trains demonstrators; specifically, it is expected that the functional requirements already specified (in [6] and [7] or advanced versions) covering one (or more) mitigation(s) will be classified as safety requirements; further functional safety requirements will be specified as needed and possible (accounting for the FR8RAILII scope);

FR8RAILII project will provide a traceability matrix between the remaining mitigations specified by the safety analyses with the specific characteristics of the tracks (and related trackside signalling systems) for test runs and the applicable procedures (generic ones or specifically developed for test runs).

The above traceability matrixes will be verified during the Safety Verification and Validation activities that will be performed during the WP3 of the M2O project.

Mitigations not (fully) covered shall be further assessed in order to verify that risks in the execution of test runs are still acceptable or to specify further (procedural) mitigations. This activity will be performed during WP3, based on the information made available by FR8RAILII project concerning the test runs execution.

Validation activities focused on the final implementation of DPS train demonstrators are out of scope of the M2O project.

[3] A proper "safety layer" implementing a set of defenses against communication threats (deletion; insertion; re-sequencing; corruption; delay) compliant with the EN50159 [7].

2.3.6 Potential consequences of credible accidents

Based on the system definition in §2.1, 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). For each accident, the potential consequences are defined with reference to the worst credible scenario, including the missed or ineffective protection by safety functions.

Accident (leading to one or more consequences)		**(worst) Potential consequences**
A_1	Collision between trains (rear, side, head-on)	C_1, C_2, C3, C_4
A_2	Collision of the train with / damage to infrastructure	C_1, C_2, C_3, C_4
A_3	Collision of the train with obstacle (persons, animals, road vehicles)	C_1, C_2, C_3, C_4
A_4	Derailment / Overturning of the train	C_1, C2, C_3, C_4
A_5	Cut of the train (separation)	C2, C_3, C_4
A_6	Other accidents (Electrocution, Burns, Asphyxia, Suffocation, Poisoning, Contamination, Fire, Explosion)	C_1, C_2, C_3, C_4

Table 5 - Accidental conditions

The above accidents can occur because of hazardous conditions related to the operation of DPS train, as identified during the safety analysis.

The severity of the potential (worst) consequences of hazardous conditions can be evaluated with reference to defined Severity classes, i.e. according to the EN 50126 [1]:

- Minor - possible minor injury; possible damage to systems;
- Marginal - severe or minor injury (no fatality); significant threat to the environment; minor damages to systems.
- Critical - single fatality and/or severe injury and/or significant damage to the environment; major damages to systems.
- Catastrophic - fatalities and/or multiple severe injuries and/or major damage to the environment; major damages to main systems.

2.3.7 Hazard Log

The main safety-relevant information coming from the safety analysis are recorded in the Hazard Log that will be taken as input in the Verification and validation activities (planned under WP3).

Specifically, 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.

Each hazard, as soon as it is identified, is in an "open" status. Its status will be "closed" when evidence of the implementation of all the related mitigations will be gathered.

The Hazard Log will be updated during the WP3 of the M2O project, based on the results coming from the safety verification activities (out of scope of this document).

2.3.8 Risk Acceptance and Safety Integrity Level allocation

According to the EN 50129 [5], the "Safety integrity" relates to the ability of a safety-related system to achieve its required safety functions. It comprises two parts:

- systematic failure integrity, which is the non-quantifiable part and related to systematic HW and SW faults and human errors;
- random failure integrity, which relates to the hazardous random hardware faults, as result of the finite reliability of hardware components.

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.

While four Safety Integrity Levels are defined by the 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 EN50129 [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 during the safety analyses (see §2.3.3) are listed in Table 16. They could lead to one or more accidents listed in Table 5 and then to the consequences in Table 4.

With reference to the Severity classes previously mentioned, all these hazards could have catastrophic consequences (i.e. at least in the worst case, they produce fatalities and/or multiple severe injuries and/or major damage to the environment and/or major damages to main systems).

Two mitigation strategies are adopted in order to achieve an acceptable a risk levels for these hazardous conditions:

- "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 EN50129 [5]);
- "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 EN50129 [5]) with additional operational mitigations that should 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}, in order 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 will be re-evaluated in each specific application where implementation details are known.

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 Preliminary Hazard Analysis

3.1 PHA form

With reference to the operational context depicted in Figure 1, the PHA concerns the whole Integrated system, including all the elements belonging to the Infrastructure, Signalling systems, "long" freight train and Operation. These elements, introduced by the hierarchical list in Table 1, are singularly addressed against the characteristics of long freight trains: increase of the train length and overall mass, implementation of distributed traction and brake, radio communication between Traction units, presence and operation of multiple pantographs, presence new equipment.

The specific hazardous condition related to the given elements and one or more characteristics of DPS trains are recorded, producing a hierarchical list of hazards (See §6.1). This list is taken as reference in the subsequent activities and complemented as needed.

Specific hazards (i.e. strictly related to the DPS trains characteristics) and "conventional hazards" (i.e. generally 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.

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

Table 7 provides the form used for the development of the Preliminary Hazard Analysis.

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS		REMARK
Level 1	Level 2	Level 3	Train length and overall mass	Distributed traction and brake	Communication between Traction units	Multiple pantographs	New equipment	ID	Description	ID	Description	

Table 7 - PHA form

3.2 Results from PHA

Appendix A provides the PHA table, filled-in with the results obtained by the Preliminary Hazard Analysis of the "Long freight train" Integrated system.

Table 8 provides the list of mitigations specified during the PHA (PHA_MIT_xx). Each mitigation is classified in Functional or Technical or Contextual safety requirements, according to §2.3.4. The element(s) of the Integrated system in charge of the implementation of each given mitigation is(are) specified in the last column. No functional safety requirement is specified at this stage (and no Safety Integrity Level is assigned to the remaining mitigations).

A "specific application" of DPS trains is based on a defined functional specification (e.g. as defined by [7] and [8]) and concerns specific train(s) configurations and specific track(s) where the running authorization applies.

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.					X			1 - INFRASTRUCTURE 2 - SIGNALLING SYSTEM 3 - DPS TRAIN
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 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.					X			1 - INFRASTRUCTURE 2 - SIGNALLING SYSTEM 3 - DPS TRAIN
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.					X			1 - INFRASTRUCTURE, 1.2 - Superstructure Elements integrity, 1.2.1 - Top ballast layer integrity, 3 - DPS TRAIN, 3.1 - Running gear integrity, 3.3.1 - Wheelsets integrity
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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.					X			1 - INFRASTRUCTURE, 1.1 - Substructure elements integrity, 1.1.1 - Bridges integrity

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.					X			2 - SIGNALLING SYSTEM, 2.3 - Trains routing and traffic regulation
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.					X			2 - SIGNALLING SYSTEM, 2.4 - Field Signaling equipment
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.					X	X		1 - INFRASTRUCTURE, 1.3 - Track geometry, 1.3.12 - Loading gauge
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.					X			2 - SIGNALLING SYSTEM, 2.1 - Interlocking (central logic)
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).					X			4 - OPERATION, 4.4 - Train maneuver

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.					X			4 - OPERATION, 4.3 - Field equipment operation, 4.3.1 - Switch point operation
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.					X			4 - OPERATION, 4.3 - Field equipment operation, 4.3.2 - Level crossing operation
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.						X		2 - SIGNALLING SYSTEM, 2.2 - Automatic Train Protection (Trackside), 4 - OPERATION, 4.4 - Train maneuver
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.					X			2 - SIGNALLING SYSTEM, 2.2 - Automatic Train Protection (Trackside)

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.					X			3 - DPS TRAIN, 3.4 - Energy supply system & Pantograph
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.					X			3 - DPS TRAIN (Simulations)

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.					X			3 - DPS TRAIN (Simulations)
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).					X			3 - DPS TRAIN (Simulations)

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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).					X			3 - DPS TRAIN (Simulations)
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.					X			3 - DPS TRAIN (Simulations)
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).					X			3 - DPS TRAIN (SRAC verification)
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).					X			3 - DPS TRAIN (SRAC verification)

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.							X	3 - DPS TRAIN, 3.3 - Coupling system 4 - OPERATION
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.						X	X	4 - OPERATION, 4.2 - Train checks
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 .						X		4 - OPERATION, 4.4 - Train maneuver
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).						X	X	4 - OPERATION, 4.4 - Train maneuver

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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.						X		3 - DPS TRAIN, 3.5 - Automatic Train Protection (Trainboard) 4 - OPERATION, 4.4 - Train maneuver
PHA_MIT_27	Procedures shall be defined in order to avoid that applicable prescriptions for train running (received by trackside signaling operators) are not remembered by the driver of DPS train after a long train stop or after driver change, as for conventional trains.						X		4 - OPERATION, 4.4 - Train maneuver
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.						X		3 - DPS TRAIN, 3.6 - Driver interface 4 - OPERATION
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.						X		3 - DPS TRAIN, 3.6 - Driver interface 4 - OPERATION

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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).						X		4 - OPERATION, 4.4 - Train maneuver
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).						X		1 - INFRASTRUCTURE, 1.3 - Track geometry, 1.3.11 - Electric neutral section, 2 - SIGNALLING SYSTEM, 2.4 - Field Signaling equipment, 2.4.6 - Catenary and Power Supply 3 - DPS TRAIN, 3.4 - Energy supply system & Pantograph 4 - OPERATION
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.						X		4 - OPERATION, 4.4 - Train manoeuvre

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)

Mitigation from Preliminary Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Exported to
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	
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).						X		4 - OPERATION, 4.5 - Management of off-normal conditions
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.					X	X		4 - OPERATION, 4.1 - Loading of wagons, 4.1.1 - Load distribution
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).					X			3 - DPS TRAIN, 3.3 - Coupling system
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.					X			3 - DPS TRAIN, 3.4 - Energy supply system & Pantograph

Table 8 - Mitigations from the DPS train Preliminary Hazard Analysis

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 Hazard Analysis

4.1 HA form

With reference to the operational context depicted in Figure 1, the HA concerns a single DPS Train implementing the "specific" functions listed in Table 2, as defined in the Functional and system requirements specification [10].

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 is adopted. Specifically, the guidewords specified in Table 9 (for a generic function) are applied to each function to be assessed.

Guidewords	Deviation (description for a generic function)
No / interruption	Missed or incomplete execution of the function, which does not produce the expected outcomes
Untimely / delayed	The function is not carried out when required but too late
Anticipated	The function is not carried out when required but too early
Undue	The function is carried out when not required
Wrong / Incorrect	The function is carried out but produces incorrect outcomes

Table 9 - Guidewords and (generic) functional deviations assessed by HA

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 are described with reference to the worst possible scenario. One or more (macro and specific) hazards are traced to the deviations; the list of hazards produced by the PHA is taken as reference, and integrated as needed.

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

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 10 provides the form used for the development of the Hazard Analysis.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATION	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description

Table 10 - HA form

4.2 Results from HA

Appendix B provides the HA table, filled-in with the results obtained by the Hazard Analysis of the Integrated system.

Table 11 provides the list of mitigations specified during the HA (HA_MIT_xx). Each mitigation is classified in Functional or Technical or Contextual safety requirements, according to §2.3.4.

For each functional safety requirement, the last two columns specify the function(s) in charge of its implementation and the Safety Integrity Level (SIL) consistently assigned. Specifically, the SIL assigned in Table 17 to each function implemented by DPS train is propagated to all the related 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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Parking Brake management	High Safety Integrity level
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).	X							Train inauguration & configuration	Low Safety 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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.	X							Communication set-up & Train inauguration & configuration	Low Safety integrity level
HA_MIT_04	DPS Train shall guarantee the integrity of train configuration data and make impossible any change after a valid Start of mission.	X							Train inauguration & configuration	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.		X						Communication set-up & Communication between Traction units	Low Safety integrity 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.	X							Train initial test	Low Safety integrity level
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.		X						Train initial test	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Train operational status management	Low Safety integrity level
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.	X							Train inauguration & configuration	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Communication set-up & Communication between Traction units	Low Safety integrity level
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.	X							Communication set-up & Communication between Traction units	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.		X						Communication between Traction units	Low Safety integrity level
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).		X						Communication between Traction units	Low Safety integrity level
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 signaling (EN50129).				X				Communication between Traction units	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.		X						Communication between Traction units	Low Safety integrity level
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. DPS switching-off shall be allowed only with train speed equal to zero.	X							Train operational status management & System de-activation	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Traction management	Low Safety integrity level
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).	X							Traction management	Low Safety integrity level
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.		X						Traction management	Low Safety integrity level
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.		X						Traction management	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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).		X						Emergency brake management	High Safety Integrity level
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.	X							Emergency brake management	High Safety Integrity level
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.		X						Emergency brake management	High Safety Integrity level
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.		X						Emergency brake management	High Safety Integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Emergency brake management	High Safety Integrity level
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.		X						Service brake management	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.	X							Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level (for BP venting)
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.	X							Emergency brake management	High Safety Integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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).	X							Communication between Traction units & Emergency brake management	High Safety Integrity level (for BP venting)
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).		X						Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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).		X						Service brake management & Emergency brake management & Communication between Traction units	High Safety Integrity level
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.	X							Energy management	Low Safety integrity level
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.		X						Communication between Traction units & Emergency brake management	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.	X							Energy management	Low Safety integrity level
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.	X							Automatic Train Protection	High Safety Integrity level
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.	X							Automatic Train Protection	High Safety Integrity level
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).	X							Automatic Train Protection	High Safety Integrity level
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).		X						Diagnostic	Low Safety integrity level

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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.					X			-	-
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.		X						Diagnostic	Low Safety integrity level
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.					X			-	-
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).						X		-	-

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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	Reference function(s) (for Functional safety requirements)	Safety Integrity level (for Functional safety requirements)
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.						X		-	-
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.						X		-	-
HA_MIT_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off.						X		-	-
HA_MIT_46	The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition.	X							Parking brake	High Safety Integrity level

Table 11 - Mitigations from the DPS train Hazard Analysis

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 Interface Hazard Analysis

5.1 IHA form

The IHA has the objective to assess the potential deviations in the data and signals exchanged among the DPS Train's subsystems (i.e. thought its internal interfaces). 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 [10] and on a high level representation of DPS train architecture depicted in Figure 4 (representing just one of the guided Traction units). It is focused on the interface between the equipment involved in the DPS implementation (in red):

- the Radio equipment interfaced to the existing TCMS of the leading Traction unit and the Radio equipment interfaced to the existing TCMS of the guided Traction unit;
- 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 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);
- Brake panels of the guided Traction unit, including the Existing brake panel, which is assumed to be isolated from the Brake pipe, and the 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;
- Brake Pipe (in common between the leading and the guided Traction units).

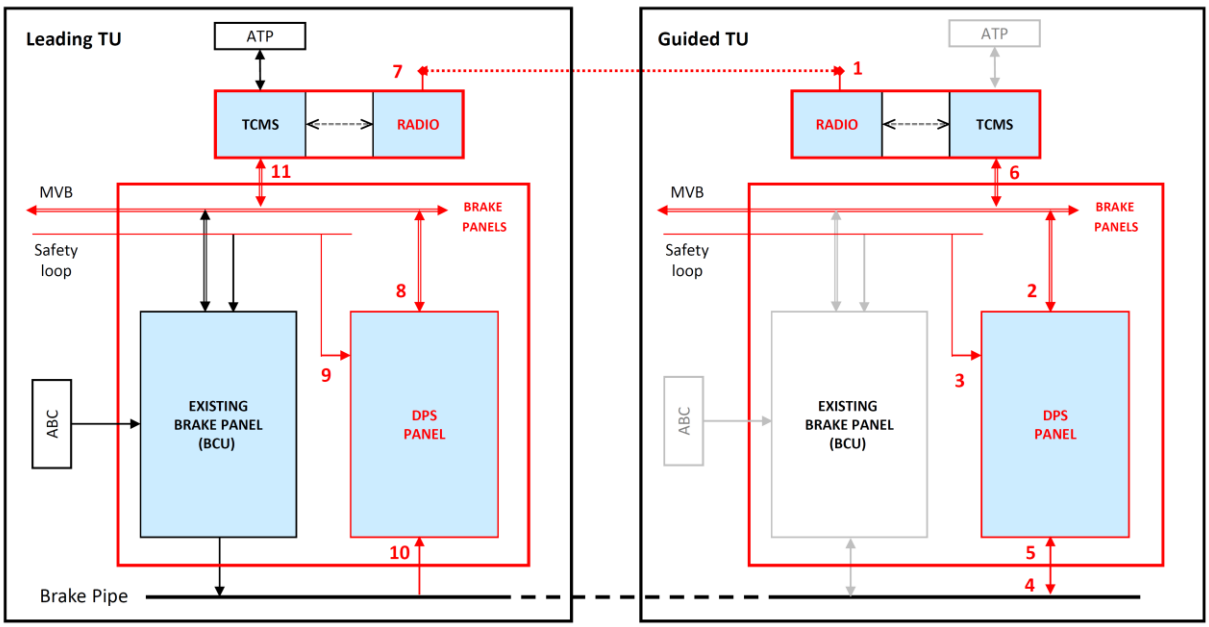

Figure 4 - DPS Train, main subsystems and internal Interface

The existing and new interfaces related to DPS implementation are represented in Figure 4 by red arrows (singularly identified and analyzed in the following). The existing interfaces working as for conventional trains are represented by black arrows if "active", grey ones otherwise.

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 12 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 4). Main data/signals exchanged are specified in Table 12 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 for cut the traction current
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 12 - Mitigations from the DPS train Hazard Analysis

In order to be systematic in the definition of the functional deviations to be singularly assessed, a HAZOP-like approach is adopted. Specifically, the guidewords in in Table 13 are applied to each interface and exchanged data/signal.

Guidewords	Deviation assessed by IHA (description for a generic interface)
No / loss	Missed or incomplete exchanged of data/signal
Incorrect	Incorrect data/signal are exchanged through the interface
Undue	Data/signal are exchanged through the interface when not required

Table 13 - Guidewords and (generic) deviations assessed by IHA

The effects of each deviation in the exchange of data and signals through the internal interfaces is described with reference to the worst possible scenario, without considering the implementation of any mitigation (Effect pre-mitigation). One or more hazards are traced to the deviations; the list of hazards produced by the previous analyses (PHA and HA) is taken as reference, and integrated as needed.

One or more mitigations are specified to reduce the risk related to the hazard, by reducing the probability of occurrence of potential accidents or their consequences. The mitigations already defined in the previous analyses (HA mainly) are taken as reference, and integrated as needed.

Table 14 provides the form used for the development of the Interface Hazard Analysis.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	HAZ_ID	HAZ_Description	MIT_ID	MIT_Description

Table 14 - IHA form

5.2 Results from IHA

Table 14 provides the list of mitigations specified during the IHA (IHA_MIT_xx). Each mitigation is classified in Functional or Technical or Contextual safety requirements, according to §2.3.4.

For each functional safety requirement, the last two columns specify the function(s) in charge of its implementation and the Safety Integrity Level (SIL) consistently assigned. Specifically, the SIL assigned in Table 17 to each function implemented by DPS train is propagated to all the related 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)

Mitigation from Hazard Analysis		Functional safety requirements			Technical safety requirements		Contextual safety requirements		Safety Integrity level	
ID	Description	Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/installation/use	Expected actions by the driver	Expected operational procedure	**Reference function(s)** (for Functional safety requirements)	**Safety Integrity level** (for Functional safety requirements)
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 detected during operation and shall trigger an action to stop the operation of the train.		X						Emergency brake management	High Safety Integrity level
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).		X						Emergency brake management	High Safety Integrity level

Table 15 - Mitigations from the DPS train Interface Hazard Analysis

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)

6 Summary of results from safety analyses

6.1 List of Hazards

One of the main results coming from the previous safety analyses is the list of the hazardous conditions related to the specific characteristics of DPS train (as defined for the PHA in §3) and to the functions implemented by DPS train (as defined for the HA in §4).

Table 16 provides the hierarchical list of hazards specified during the previous safety analyses, 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 and the source (PHA/HA) of each Specific hazard.

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard		Source
H_1	**Impaired (or lost) train running stability**	A_4	Derailment / Overturning of the train	-
H_1_1	**Increase of vehicle axle load**			PHA
H_1_2	**Long bridges with excessive cross winds**			PHA
H_1_3	**Long bridges with hazardous dynamic behavior** (i.e. natural frequencies coupled with vibrations induced by trains)			PHA
H_1_4	**Excessive overall mass of DPS train brake with respect to the infrastructure**			PHA
H_1_5	**Excessive longitudinal forces transmitted to the infrastructure** due to the brake application by DPS train.			PHA
H_2	**Interference between train and loading gauge due to changes in train shape**	A_2	Collision of the train with / damage to infrastructure	PHA
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)			PHA / HA
H_3_2	**Excessive stretch length** after stopping of the train due to distributed traction/braking			PHA
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**			PHA / HA
H_4_2	Excessive in-train longitudinal forces **due to specific track characteristics**			PHA
H_4_3	Excessive in-train longitudinal forces **due to specific maneuver**			PHA

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		Source
H_4_4	Excessive in-train longitudinal forces **due to specific distribution of loads over wagons**			PHA
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**			PHA
H_5_2	Excessive train braking distances or speed **due to an excessive timing of reaction for braking application**			PHA
H_5_3	Excessive train braking distances or speed **due to distributed traction and braking performance**			PHA / HA
H_5_4	Excessive train speed **due to an undue release of brakes**			PHA
H_5_5	**Temporary speed restriction not fulfilled with the whole length of the train**			PHA
H_5_6	**Missed / ineffective reduction of the train speed by the driver** (acting on traction and brake).			PHA
H_6	**Undue train braking or train unduly immobilized**	A_6	Other accidents (Electrocution, Burns, Asphyxia, Suffocation, Poisoning, Contamination, Fire, Explosion)	PHA
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**			PHA / HA
H_7_2	Undue train movement due to a **shunting operation made by the driver**			PHA
H_7_3	Undue train movement **in an area where shunting is not allowed**			PHA / HA
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)**			PHA / HA
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			PHA / HA

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard		Source
	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**			PHA
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)			PHA
H_10	**Hazardous operation of train/maintenance staff**	All accident		-
H_10_1	**Incorrect (unsafe) train composition or configuration due to staff error**			PHA / HA
H_10_2	**Intendent change of train configuration data by staff during operation**			PHA / HA
H_10_3	Unsafe maneuver of the train, due to a **wrong orientation**			PHA
H_10_4	**Unsafe maneuver of the driver**, which does not remember the received prescriptions after a long train stop or after driver change			PHA
H_10_5	**Unsafe management of train equipment in the crossing of neutral section due to staff error**			PHA
H_10_6	**Improper use of compressor to restore the minimum pressure in the main air reservoir**			PHA
H_10_7	**Unsafe condition of the train after end-of mission due to staff error**			PHA
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.**			PHA
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)			PHA
H_11_3	The **braking distance is too long to stop the train at the first main signal after a Hotbox-detector**.			PHA
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**			PHA
H_11_5	**Level crossing unduly switched on** before the full passage of the end of the train			PHA
H_11_6	**Switch point unduly maneuvered or released or** before the full passage of the end of the train.			PHA

(Macro and Specific) Hazard		Consequent accident(s) for Macro hazard		Source
H_12	**Train misrouted on a wrong (non-adequate) line**	All accident		PHA
H_13	**Ineffective DPS train initial tests**	All accident		-
H_13_1	**Missed or incomplete execution** of DPS train initial tests			PHA
H_13_2	**Incorrect execution** of DPS train initial tests			PHA
H_14	**Other hazardous conditions on train**	A_4	Derailment / Overturning of the train	-
H_14_1	**Fire on-board** during train run			PHA / HA
H_14_2	**Operational relevant failures and disturbances** during train run			PHA / HA

Table 16 - List of Hazards

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 due to an incapacitated driver (not detected).

6.2 Safety integrity of DPS Train functions

Table 17 provides the list of functions implemented by DPS train and for each function:

- a qualitative description of the consequent (worst-case) scenario and potential accident;
- the safety integrity level allocated to the function, according to the criteria stated in §2.3.8;
- further mitigations to be implemented in order to achieve a tolerable risk level (specifically for low safety integrity functions).

Based on Table 17, a further set of mitigations (SIL_MIT_xx) is specified, concerning the Safety Integrity required to each function implemented by DPS train; they are listed in Table 18, together with the mitigated hazards.

The SIL assigned in Table 17 to each function is propagated to all the related mitigations (functional safety requirements) listed in Table 11 (from HA) and in Table 14 (from IHA)[4].

[4] No functional safety requirement is specified by the PHA.

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)

Phase	Main function	Worst scenario from	Safety integrity level		Further mitigations	
A - Start of mission	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).	No safety function	-	Train inauguration & configuration. Operational procedure for DPS train composition.	PHA_MIT_22, HA_MIT_03
	Communication set-up	**Incomplete exchange of data between DPS train Traction units 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	-	Train inauguration & configuration. Driver acknowledgment of configuration data exchanged between Traction units.	HA_MIT_03, HA_MIT_43, HA_MIT_08
	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	SIL_MIT_07	Driver acknowledgment of configuration data exchanged between Traction units.	PHA_MIT_25, HA_MIT_03, HA_MIT_08
	Train operational status management	**Missed or undue remote controls from the leading Traction unit 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	SIL_MIT_09	Driver acknowledgment and procedure specifying driver responsibility in the setting of train orientation	PHA_MIT_25, HA_MIT_08

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)

Phase	Main function	Worst scenario from	Safety integrity level		Further mitigations	
	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	SIL_MIT_08	Operational procedure for the execution of train initial tests. Driver acknowledgment and procedure specifying driver responsibility in the execution of train initial tests.	PHA_MIT_23, PHA_MIT_32, HA_MIT_42
B - Train run	Communication between Traction units	**Missed or incorrect exchange of remote controls between the DPS train Traction units** ,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	SIL_MIT_01	Brake pipe pressure monitoring for the application of pneumatic brake.	HA_MIT_30, HA_MIT_15, HA_MIT_44, HA_MIT_08
	Traction management	**DPS train speed beyond the actual limit due to an ineffective management of traction** and/or excessive in-train longitudinal forces (and potential DPS train separation and/or derailment).	Low Safety integrity level	SIL_MIT_06	Brake pipe pressure monitoring for the application of traction cut-off	PHA_MIT_28, PHA_MIT_29, HA_MIT_08, HA_MIT_19
	Service brake management	**Ineffective application of (pneumatically controlled) 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	SIL_MIT_10	Emergency (pneumatic) brake.	HA_MIT_27
	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	SIL_MIT_11	-	PHA_MIT_30
	Parking Brake management	**Ineffective permanent immobilization and undue train movement**, with potential collision of DPS train (with other trains, infrastructure or obstacle)	High Safety Integrity level	SIL_MIT_12	-	PHA_MIT_32

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)

Phase	Main function	Worst scenario from	Safety integrity level		Further mitigations	
	Energy management	**Potential damage to the infrastructure** (catenary overhead) **and/or to the DPS train** (on-board power supply system).	Low Safety integrity level	SIL_MIT_03	Procedure specifying driver actions and responsibility in the selection of pantographs and crossing of neutral sections	PHA_MIT_31
	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	SIL_MIT_02	Train (brake) initial test or procedure specifying driver responsibility	PHA_MIT_30, HA_MIT_06
	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	SIL_MIT_13	-	(PHA_MIT_26)
	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	SIL_MIT_04	Train (brake) initial test and Procedure specifying driver responsibility	PHA_MIT_33, HA_MIT_06, HA_MIT_08
C - End of mission	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	SIL_MIT_05	Procedure specifying driver responsibility on DPS disconnection	HA_MIT_45, HA_MIT_08

Table 17 - Safety integrity level allocation to DPS Train functions and further mitigations

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)

Safety Integrity requirements for DPS train		Mitigated hazard	Functional safety requirements			Technical safety requirements		Contextual safety requirements	
ID	Description		Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/ installation/ use	Expected actions by the driver	Expected operational procedure
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 (EN50129), on software for railway control and protection systems (EN50128) and on safety-related communication in transmission systems (EN50159).	H_4_1, H_5_3			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_5_3			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_8_1, H_8_2			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_14_1, H_14_2			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_5_3			X				

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)

Safety Integrity requirements for DPS train		Mitigated hazard	Functional safety requirements			Technical safety requirements		Contextual safety requirements	
ID	Description		Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/ installation/ use	Expected actions by the driver	Expected operational procedure
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_5_3			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_5_3, H_10_1			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_13			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_10_2			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_5_3			X				

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)

Safety Integrity requirements for DPS train		Mitigated hazard	Functional safety requirements			Technical safety requirements		Contextual safety requirements	
ID	Description		Functional behavior	Failures detection & Safe state enforcement and retention	Safety Integrity	Compliance to regulation and standard	Technical constraints for design/ installation/ use	Expected actions by the driver	Expected operational procedure
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_5_3			X				
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 (EN50129) and on software for railway control and protection systems (EN50128).	H_4_1, H_7_1			X				
SIL_MIT_13	The Automatic Train Protection 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 (EN50129) and on software for railway control and protection systems (EN50128).	H_5_3			X				

Table 18 - Safety Integrity requirements for 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)

6.3 Hazard Log

Appendix C provides the Hazard Log recording the safety-relevant information coming from the performed safety analysis.

It is based on the list of hazards provided in Table 16 and the information recorded in the PHA and HA tables. Specifically, it provides the list of mitigations to be implemented for each specific hazard (i.e. to reduce the related risk to a tolerable level).

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)

7 Conclusion

This deliverable concerns a subset of the safety activities performed during the Work-Package 2 (task 2.3) of the M20 project. Specifically, it provides: the Safety plan of the activities performed during the whole M2O project, and the results obtained by the safety analyses performed on the Integrated system including a generic implementation of "long freight trains" based on Distributed Power System (DPS) and radio communication (independently from the specific technology adopted) and trackside's elements (belonging to the Infrastructure or to Signalling systems).

The performed safety analyses include the Preliminary Hazard analysis (PHA) developed for the entire Integrated system (i.e. including all the elements belonging to the infrastructure, signalling systems, "long" freight train and operation, see Figure 1), the Hazard Analysis (HA) developed for a single DPS train based on related functional and system requirements [10], and the Interface Hazard Analysis (IHA) also based on a high level representation of DPS train architecture (instantiated in this document, see Figure 4).

The main results obtained by the performed safety analyses are the list hazardous conditions related to the operation of DPS trains and the list of mitigations to be implemented, classified in Functional safety requirements, Technical safety requirements and Contextual safety requirements (see §2.3.4).

The content and results of the above safety analyses have been shared and reviewed by FR8RAILII experts, considering their wide applicability as reference in the development of DPS train demonstrators during the FR8RAILII project as well as in future specific applications.

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)

8 Acronyms

ATP	Automatic Train Protection
ABC	Actuator Brake Control (existing brake handle)
BP	Brake Pipe
DPS	Distributed Power System
HA	Hazard Analysis
IHA	Interface Hazard Analysis
MIT	MITigation
MVB	Multifunction Vehicle Bus
PHA	Preliminary Hazard Analysis
SIL	Safety Integrity Level
TCMS	Train Control and Management System
TU	Traction Unit
TSI	Technical Specifications for Interoperability

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)

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

[9] FR8RAILII project, 20190827 (DB) Requirements LT V6.

[10] FR8RAILII project, D5.2 - Functional and system requirements specification. (BT_dbl2.0).

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 Preliminary Hazard Analysis table

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS	
Level 1	Level 2	Level 3	Train length and mass	Distributed traction and brake	Communication between Locos	Multiple pantographs	New equipment	ID	Description	ID	Description
1 - INFRASTRUCTURE	1.1 - Substructure elements	1.1.1 - Bridges integrity	x					H_1_2	Long bridges with excessive cross winds	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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.
								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.		
		1.1.2 - Tunnels integrity						No difference from conventional applications			
	1.2 - Superstructure Elements	1.2.1 - Top ballast layer integrity		x				H_1_5	Excessive longitudinal forces transmitted to the infrastructure due to the brake application by DPS train.	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.
		1.2.2 - Sleepers integrity	x								
		1.2.3 - Rail fastenings integrity	x								
		1.2.4 - Running rails integrity	x								
		1.2.5 - Points and crossings integrity	x								
	1.3 - Rails and Track	1.3.1 - Rails profile						No difference from conventional applications			
		1.3.2 - Track width						No difference from conventional applications			
		1.3.3 - Track height						No difference from conventional applications			
		1.3.4 - Track twist						No difference from conventional applications			
		1.3.5 - Track Curve						No difference from conventional applications			
		1.3.6 - Track Gradient	x					H_4_2	Excessive in-train longitudinal forces due to specific track characteristics	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.
										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.
		1.3.7 - Track Cant						No difference f+J20rom conventional applications			
		1.3.8 - Track Crest and trough						No difference from conventional applications			
		1.3.9 - Track load carrying capacity						No difference from conventional applications			
		1.3.10 - Direction of running						No difference from conventional applications			
		1.3.11 - Electric neutral section				x				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).
		1.3.12 - Loading gauge					X	H_2	Interference between train and loading gauge due to changes in train shape	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.

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS	
Level 1	Level 2	Level 3	Train length and mass	Distributed traction and brake	Communication between Locos	Multiple pantographs	New equipment	ID	Description	ID	Description
2 - SIGNALLING SYSTEM	2.1 - Interlocking (central logic)	-	X					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	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).
										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.
	2.2 - Automatic Train Protection (Trackside)	-	X					H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application	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).
								H_5_5	Temporary speed restriction not fulfilled with the whole length of the train	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.
								H_6	Undue train braking or train unduly immobilized	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.
	2.3 - Trains routing and traffic regulation	-	X					H_12	Train misrouted on a wrong (non-adequate) line	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.
	2.4 - Field Signalling equipment	2.4.1 - Train detection by track circuit	X					H_9_1	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)	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).
		2.4.2 - Train detection by axles counter	X					H_9_2	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	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).
		2.4.3 - Signals	X					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.	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.
		2.4.4 - Switch point	X					H_11_6	Switch point unduly manoeuvred or released or before the full passage of the end of the train.	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.
		2.4.5 - Level crossing	X					H_11_5	Level crossing unduly switched on before the full passage of the end of the train	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.
		2.4.6 - Catenary and Power Supply	X	X		X		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)	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).
		2.4.7 - Hot box detector	X					H_11_3	The braking distance is too long to stop the train at the first main signal after a Hotbox-detector.	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.

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS	
Level 1	Level 2	Level 3	Train length and mass	Distributed traction and brake	Communication between Locos	Multiple pantographs	New equipment	ID	Description	ID	Description
3 - DPS TRAIN	3.1 - Running gear	3.3.1 - Wheelsets integrity	X	X				H_1_1	Increase of vehicle axle load	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.
		3.3.2 - Suspension integrity						No difference from conventional applications			
		3.3.3 - Bogie structure integrity						No difference from conventional applications			
	3.2 - Wagon	3.4.1 - Load carrying units integrity						No difference from conventional applications			
		3.4.2 - Frame integrity						No difference from conventional applications			
	3.3 - Coupling system	-	X	X		x		H_3_1	Loss of integrity of coupling between units (Traction units or wagons)	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.
								H_3_2	Excessive stretch length after stopping of the train due to distributed traction/braking	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).
	3.4 - Energy supply system & Pantograph	-		X	X			H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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).
								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))	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.
										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.
	3.5 - Automatic Train Protection (Trainboard)	-		X	X			H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application	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;
								H_5_5	Temporary speed restriction not fulfilled with the whole length of the train	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.
	3.6 - Driver interface	-		X	X			H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application	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.
	3.7 - Train Control & Management System	-		X	X			H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
								H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application	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.

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS	
Level 1	Level 2	Level 3	Train length and mass	Distributed traction and brake	Communication between Locos	Multiple pantographs	New equipment	ID	Description	ID	Description
	3.8 - Braking and traction equipment	-		X	X			H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
								H_5_1	Excessive train braking distances or speed due to an impaired (or lost) braking capability	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.
								H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application	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;
								H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
								H_5_4	Excessive train speed due to an undue release of brakes	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.
								H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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.
4 - OPERATION	4.1 - Loading of wagons	4.1.1 - Load distribution	X	X				H_4_4	Excessive in-train longitudinal forces due to specific distribution of loads over wagons	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.
										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.
		4.1.2 - Load fastening	X					H_4_4	Excessive in-train longitudinal forces due to specific distribution of loads over wagons	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.
	4.2 - Train checks	-		X	X	X		H_13_1	Missed or incomplete execution of DPS train initial tests	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.
								H_13_2	Incorrect execuition of DPS train initial tests	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.
	4.3 - Field equipment operation	4.3.1 - Switch point operation	X					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.	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.
		4.3.2 - Level crossing operation	X					H_11_6	Switch point unduly manoeuvred or released or before the full passage of the end of the train.	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.

ELEMENTS / FACTORS			LONG TRAIN CHARACTERISTICS					HAZARD		MITIGATIONS	
Level 1	Level 2	Level 3	Train length and mass	Distributed traction and brake	Communication between Locos	Multiple pantographs	New equipment	ID	Description	ID	Description
	4.4 - Train manoeuvre	-	X	X	X	X		H_4_3	Excessive in-train longitudinal forces due to specific manoeuvre	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.
								H_5_6	Missed / ineffective reduction of the train speed by the driver (acting on traction and dynamic brake).	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.
								H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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.
								H_7_2	Undue train movement due to a shunting operation made by the driver	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 .
								H_7_3	Undue train movement in an area where shunting is not allowed	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).
								H_10_4	Unsafe manoeuvre of the driver, which does not remember the received prescriptions after a long train stop or after driver change	PHA_MIT_27	Procedures shall be defined in order to avoid that applicable prescriptions for train running (received by trackside signaling operators) are not remembered by the driver of DPS train after a long train stop or after driver change, as for conventional trains.
								H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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.
								H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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).
								H_10_5	Unsafe management of train equipment in the crossing of neutral section due to staff error	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).
								H_10_6	Improper use of compressor to restore the minimum pressure in the main air reservoir	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).
	4.5 - Management of off-normal conditions	-	x		x	x	x	H_14_1	Fire on-board during train run	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).
								H_14_2	Operational relevant failures and disturbances during train run	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).
	4.6 - System's elements (locomotives and wagons) coupling and decoupling	-	X					H_13_2	Incorrect execuition of DPS train initial tests	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.
								H_10_7	Unsafe condition of the train after end-of mission due to staff error		

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 Hazard Analysis table

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
Train composition Forming the train according to the established composition, by coupling wagons and traction units.	No / interruption	Missed coupling of all the wagons and traction units.	Coupling of locomotives and wagons	Inconsistency between the train physical composition and configuration data.	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
	Untimely / delayed	Delay in the coupling of all the wagons and traction units.	Coupling of locomotives and wagons	Delayed in the train start of mission.	No hazardous effect.				
	Wrong / Incorrect	Wrong coupling of wagons and traction units with respect to the established composition	Coupling of locomotives and wagons	Inconsistency between the train physical composition and configuration data.	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
	Undue / anticipated	-	-	-	-	-	-	-	-

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
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.	No / interruption	Missed connection to the radio network of one or more locomotive.	Start of mission	The train Start of mission is finalized without all locomotive connected to the radio network	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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.
								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 Changing the train orientation shall be allowed only with train speed equal to zero. 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.
	Untimely / delayed	Delayed connection to the radio network of one or more locomotive.	Start of mission	Delayed finalization of the train Start of mission.	No hazardous effect.	-	-	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.
	Wrong / Incorrect	Undue connection to the radio network of external subject	Start of mission	Potential manipulation of train configuration data	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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.
								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.
	Undue / anticipated	Connection of locomotives to different radio network	Start of mission	The train Start of mission is finalized without all locomotive connected to the radio network	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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.
								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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
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.	No / interruption	The train inauguration and configuration processes are not finalized.	Start of mission	The train Start of mission is finalized without all validated configuration data.	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
								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).
		Incomplete set of configuration data introduced by the driver	Start of mission	Wrong configuration data are used by locomotives	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
Untimely / delayed	Delay in the finalization of the train inauguration and configuration	Start of mission	Delayed finalization of the train Start of mission.	No hazardous effect.	-	-	-	-	
Wrong / Incorrect	Incorrect inauguration data (train number, UIC locomotive number, static properties) exchanged by leading and guided locomotives.	Start of mission	Wrong configuration data are used by locomotives	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
	Wrong train orientation (with respect to the one set by the driver)	Start of mission / Train run	Different orientation established for a guided locomotives (with respect to the orientation set for the remaining locomotives)	Undue movement of the train in the opposite direction, due to an incorrect setting of train orientation.	H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
	Undue / anticipated	Undue finalization of the configuration process (e.g. when not all configuration data are introduced and shared between locomotives)	Start of mission	Wrong configuration data are used by locomotives	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
		Undue train movement before that the start of mission is finalized	Start of mission	Train movement without automatic protection and driver supervision	Potential collision with other trains or infrastructure or obstacles.	H_7_3	Undue train movement in an area where shunting is not allowed	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.
		Intendent change of train configuration data by staff	After Start of mission	Wrong configuration data are used by locomotives	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_10_2	Intendent change of train configuration data by staff during operation	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 operational status management Management of the operational status of DPS train	No / interruption /Untimely / delayed	Missed or delayed switch off of DPS when required	Start of mission / Train run	DPS could be in service retention mode, with established radio communication and valid configuration data.	Undue remote controls leading to an hazardous management of distributed traction and brake. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
	Wrong / Incorrect / Undue / anticipated	Undue train run with DPS in Switch off mode	Start of mission	DPS train remote controls cannot be implemented because of lack of radio communication and valid configuration data.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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. DPS switching-off shall be allowed only with train speed equal to zero.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
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	No	Missed execution of train initial test	Start of mission	Latent failures may remain undetected, with potential incapability to apply brake when required. Incorrect configuration data may remain undetected, i.e. leading to an hazardous management of distributed traction and brake.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_13_1	Missed or incomplete execution of DPS train initial 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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
	Interruption	Execution of an incomplete set of train initial tests.	Start of mission	Latent failures may remain undetected, with potential incapability to apply brake when required. Incorrect configuration data may remain undetected, i.e. leading to an hazardous management of distributed traction and brake.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_13_1	Missed or incomplete execution of DPS train initial 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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
	Wrong / Incorrect	Incorrect execution of the train initial test	Start of mission	Latent failures may remain undetected, with potential incapability to apply brake when required. Incorrect configuration data may remain undetected, i.e. leading to an hazardous management of distributed traction and brake.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_13_2	Incorrect execuition of DPS train initial 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.
	Undue / anticipated	Ineffective execution of the train initial test (i.e. not able to identify latent failures affecting braking capability)	Start of mission	Latent failures may remain undetected, with potential incapability to apply brake when required. Incorrect configuration data may remain undetected, i.e. leading to an hazardous management of distributed traction and brake.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_13_2	Incorrect execuition of DPS train initial tests	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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
Communication between Traction units Communication between Traction units	No / interruption / delayed	Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train run.	Leading and guided locomotive may operate improperly by their traction and brake.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
								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.
								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).
								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.
								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.
		Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train run and on-going pneumatic (service or emergency) brake application	Guided locomotives may release the on-going brake	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
		Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train run and on-going pneumatic (service or emergency) brake application	Guided locomotives may stop the on-going brake release while the leading the loco release the brake and activate the traction.	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
		Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train run and emergency brake command to be sent by the leading loco.	Guided locomotives do not receive the Emergency brake command from the Leading loco.	Train is not stopped within the predefine distance. Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
		Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train run and emergency brake request to be sent by the guided locos.	Leading locomotive does not receive the Emergency brake request from the Guided loco.	Train is not stopped within the predefine distance. Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	HA_MIT_29	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	HA_MIT_31	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).
								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.
		Loss of communication between the leading locomotives and one or more guided locomotives, due to radio link unavailability or msg deletion	Train running through a neutral section	Leading and trailing pantographs are both connected to catenary on different charged sections. Electrical stress due to undue harmonics, phase crash, surges, ….	Potential damage to the infrastructure and / or trainborne power supply system.	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))	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.
	Wrong / Incorrect	No valid communication between the leading locomotives and one or more guided locomotives due to data corruption, msg repetition, resequencing, insertion	Train run. See above for specific scenario.	Leading and/or guided locomotive may operate improperly by their traction and brake	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
	Undue	Masquerade messages in the communication between the leading locomotives	Train run. See above for specific scenario.	Leading and/or guided locomotive may operate improperly by their traction and brake	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
Traction management Management of traction according to set point (including traction cut-off as required).	No / interruption / partial	Missed or partial (not at all the locomotives) traction when required (by driver)	Train run	The whole traction effort could be not enough for train running at the required speed.	In-train longitudinal forces are still acceptable. No hazardous effect.	-	-		
		Missed or partial (not at all the locomotives) traction cut-off when required (e.g. for brake application)	Train run	Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). Increase of in-train longitudinal force.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
								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).
								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).
								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_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.
	Untimely / delayed / Undue / anticipated	Untimely application of traction (in one or more locomotives) with respect to the driver command	Train run	The whole traction effort could be not enough for train running at the required speed.	No hazardous effect.	-	-	-	-
		Undue removal of Traction cut-off	Train run and on-going pneumatic (service or emergency) brake application	Undue application of traction reducing the effectiveness of the on-going braking action.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
	Wrong / Incorrect	Incorrect application of traction (in one or more locomotives) with respect to the set level	Train run	Different levels of traction are applied by the different locomotives	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
								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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
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.	No / interruption / partial	Missed or partial (not at all the locomotives) application of the service (dynamic and pneumatic) brake when required (e.g. for brake application)	Train run	Service (dynamic and pneumatic) brake is not applied by all the locomotives at the set level. Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). Increase of in-train longitudinal force.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
								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.
	Untimely / delayed / Undue / anticipated	Untimely application of the service (dynamic and pneumatic) brake (in one or more locomotives) with respect to the driver command	Train run	Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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_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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
	Wrong / Incorrect	Incorrect application of service (dynamic and pneumatic) brake (in one or more locomotives) or incorrect set levels	Train run	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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_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.
Emergency 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 maximum (reliable) brake force.	No / delayed	Missed or delayed application of emergency brake by the leading locomotive, when required	Train run and emergency brake command sent from leading to guided locomotives	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
		Missed or delayed application of emergency brake by a guided locomotive, when required	Train run and emergency brake command sent from leading to guided locomotives	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
		Missed or delayed command of emergency brake sent by the leading locomotive to the guided locomotives	Train run and emergency brake request sent from a guided locomotive to the leading vehicle.	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
		Missed or delayed request of emergency brake sent by a guided locomotive to the leading locomotive	Train run and emergency brake request sent from a guided locomotive to the leading vehicle.	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Increase of the stopping distance in case of EB request sent from a Guided Traction unit (due to the detection of any condition requiring the train stop, i.e. under which conventional train apply EB up to train standstill). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
								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.
								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).
		Missed or delayed brake pipe venting in case of train separation	Train separation during running	Ineffective braking of train sections	Increase of consequence of a train separation event.	H_3_1	Loss of integrity of coupling between units (Traction units or wagons)	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).
								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).

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
	Undue / untimely	Undue emergency brake applied by the leading locomotive, without the command sent to the guided locomotives	Train run.	Only the leading locomotive vents the brake pipe, with increase of in-train longitudinal force	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
		Undue emergency brake applied by a guided locomotive, when not commanded by the leading Loco	Train run.	Only a guided locomotive vents the brake pipe, with increase of in-train longitudinal force	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
								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).
	Wrong / Incorrect	-							
Parking Brake Application of braking force ensuring the permanent immobilization of the train.	No / Interruption / delayed	Missed or delayed or partial application of the braking force in order to immobilize permanently the train	Train at standstill	Ineffective immobilization and undue movement of the train.	Potential collision with other trains, or infrastructure or obstacles.	H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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.
	No / Interruption / delayed	Missed or delayed orrelease of the braking force (when not required / with trainshall be permanently at standstill condition)	Train run	Possible undue parking brake application by Guided Loco in run time with damages to the calipers	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	HA_MIT_46	The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition.
	Wrong / Incorrect / Undue / Untimely / Anticipated	Undue release of the braking force (when not required / with trainshall be permanently at standstill condition)	Train at standstill	Ineffective immobilization and undue movement of the train.	Potential collision with other trains, or infrastructure or obstacles.	H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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.
								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.

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
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.	No / interruption / delayed	Missed or delayed transmission of driver's request to raise the pantograph to the guided vehicle (over the radio connection)	Start of mission or change of pantographs	No connection to the catenary and no power supply for traction.	No hazardous effect.				
		Missed or delayed disconnection from the catenary (by opening of the main circuit breaker and lowering of pantograph(s)) when require	Train running through a neutral section	Leading and trailing pantographs are both connected to catenary on different charged sections. Electrical stress due to undue harmonics, phase crash, surges, ….	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	H_8_2	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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.
								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.
	Wrong / Incorrect / Untimely / Undue / anticipated	Incorrect selection of the pantograph to be used by a guided locomotive	Change of pantographs	Use of an improper pantograph with respect to the network and voltage system	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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.
								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.
Air management Management of the main air reservoir (use of compressor)	No / interruption	Unavailability of sufficient air pressure in the main reservoir to properly operate		Missed or partial supply of energy for brake force generation	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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_21	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.
	Untimely / delayed / Wrong / Incorrect / Undue / anticipated	N/A							
Automatic Train Protection Management of the status of ATP System (active / sleeping mode) on (leading / guided) Traction units.	No / interruption / Untimely / delayed	Missed or delayed ATP in active mode when required	Train run	The leading locomotive provides remote controls to the guided locomotives without accounting for space and speed limits coming from ATP trackside.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
								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.
	Wrong / Incorrect / Undue / anticipated	Undue train run with ATP System in sleeping mode		The leading locomotive provides remote controls to the guided locomotives without accounting for space and speed limits coming from ATP trackside.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).

FUNCTIONAL FAILURE MODE				FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Function	Guide-word	Deviation	Scenario	Local effect	Final effect	ID	Description	ID	Description
Diagnostic	No / interruption / delayed	Missed or delayed notification of fire in a guided locomotive.	Train run & fire in guided loco	Missed activation of fire fighting unit in a guided vehicle.	Development of fire in the guided locomotives	H_14_1	Fire on-board during train run	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).
								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).
		Missed or delayed notification of operational relevant failures and disturbances.	Train run	Missed reaction (automatic or by the driver) to operational relevant failures and disturbances.	Hazardous condition due to the missed or delayed reaction to operational relevant failures and disturbances.	H_14_2	Operational relevant failures and disturbances during train run	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).
								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.
								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.
								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.
	Untimely / Wrong / Incorrect /Undue / anticipated	Undue notification to the driver of fire in a guided locomotive (when it is not the case).	Train run	Undue activation of fire fighting unit in a guided vehicle	-	-	-		
		Undue notification to the driver of operational relevant failures and disturbances (when it is not the case).	Train run	Undue reaction o operational relevant failures and disturbances:	-	-	-		
System de-activation	No / interruption	N/A							
Management of system de-activation and the related communication between the Traction units about the status of train.	Untimely / delayed / Wrong / Incorrect	N/A							
	Undue / anticipated	Undue de-activation of the system (when not required)	Train run	Incorrect management of distributed traction and brake during train run	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
						H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	HA_MIT_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off.

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 C Interface Hazard Analysis

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
1	TCMS L→ TCMS G	LG - Radio connection Status	No / loss of	No / loss of LG - Radio connection Status	The Guided Traction unit does not consider available the radio communication with the leading Traction unit. It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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.
									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.
									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.
									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).
			Incorrect / undue	Incorrect LG - Radio connection Status	The Guided Traction unit unduly considers available the radio communication with the leading Traction unit. It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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 signaling (EN50129).
									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.
									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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
		LG - Number / position of traction units	No / loss of	No / loss of LG - Number / position of traction units	Unknown number and/or position of traction units and possible incorrect train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
			Incorrect	Incorrect LG - Number / position of traction units	Incorrect umber and/or position of traction units used during train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
			Undue	Undue LG - Number / position of traction units	N.A.	N.A.	N.A.	N.A.	N.A.	
		LG - Distributed power switched on	No / loss of	No / loss of LG - Distributed power switched on	Incorrect management of distributed traction and brake during train run	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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. DPS switching-off shall be allowed only with train speed equal to zero.
			Incorrect	Incorrect LG - Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
			Undue	Undue LG - Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
		LG - Traction unit orientation	No / loss of	No / loss of LG - Traction unit orientation	Missed set of train orientation at one or more guided Traction units (with respect to the orientation set by the driver for the leading Traction unit)	Undue movement of the train in wrong direction (with respect to the orientation set by the driver for the leading Traction unit)	H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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.
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
			Incorrect	Incorrect LG - Traction unit orientation	Different orientation established for one or more guided Traction units (with respect to the orientation set by the driver for the leading Traction unit)	Undue movement of the train in wrong direction (with respect to the orientation set by the driver for the leading Traction unit)	H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
			Undue	Undue LG - Traction unit orientation	N.A.	N.A.	N.A.	N.A.	N.A.	
		LG - Traction request to set level	No / loss of	No / loss of LG - Traction request to set level	The traction set point is not communicated to the Guided Traction units (by the Leading Traction unit). The driver can not control the traction forces of all vehicles.	Traction force performance degradation	N.A.	No hazardous effect.	No hazardous effect.	
			Incorrect	Incorrect LG - Traction request to set level	An incorrect traction set point is communicated to the Guided Traction units (by the Leading Traction unit). The driver can not control the traction forces of all vehicles. Different levels of traction or dynamic braking are applied by the different Traction units.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment)	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Undue	Undue LG - Traction request to set level	N.A.	N.A.	N.A.	N.A.	N.A.	
		LG - Service brake request to set level	No / loss of	No / loss of LG - Dynamic brake request to set level	The Service brake set point is not communicated to the Guided Traction units (by the Leading Traction unit). Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). The driver can not control the traction / brake forces of all vehicles.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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.
									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).
			Incorrect	Incorrect LG - Dynamic brake request to set level	An incorrect Dynamic brake set point is communicated to the Guided Traction units (by the Leading Traction unit). Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). The driver can not control the Dynamic brake forces of all vehicles. Different levels of traction or dynamic braking are applied by the different Traction units, with potential increase of in-train longitudinal force.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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.
			Undue	Undue LG - Dynamic brake request to set level	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
		LG - Traction cut off command	No / loss of	No / loss of LG - Traction cut off command	The Traction cut off command is not communicated to the Guided Traction units (by the Leading Traction unit). The driver can not control the traction / brake forces of all vehicles.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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).
			Incorrect / Undue	Incorrect LG - Traction cut off command	The Traction cut off command is communicated to the Guided Traction units (by the Leading Traction unit, when not required).	Undue reduction of train speed	-	No hazardous effect.	No hazardous effect.	
		LG - Emergency brake command	No / loss of	No / loss of LG - Emergency brake command	The Emergency brake command is not communicated to the Guided Traction units (by the Leading Traction unit, via radio).	Missed or delayed application of emergency brake(i.e. missed traction cut-off and assistance to brake application) by one or more guided Traction unit, when required.	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
									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.
			Incorrect / undue	Incorrect LG - Emergency brake command	The Emergency brake command is unduly communicated to the Guided Traction units (by the Leading Traction unit, via radio, when not required).	Application of emergency brake at the Guided Traction unit(s), while it is not applied at the Traction unit. Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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 signaling (EN50129).
									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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
0	0	**LG - Brake release command**	No / loss of	No / loss of LG - Brake release command	The Brake release command is not communicated to the Guided Traction units (by the Leading Traction unit).	Missed release of brake at the guided Traction unit (while the Leading Traction unit releases the brake and activates the traction)	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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.
			Incorrect	Incorrect LG - Brake release command	N.A.	N.A.	N.A.	N.A.	N.A.	
			Undue	Undue LG - Brake release command	Undue brake release command from Leading Traction unit to Guided Traction unit.	Guided Traction unit(s) unduly release she brake	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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_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 signaling (EN50129).
									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.
0	0	**LG - Parking brake command**	No / loss of	No / loss of LG - Parking brake command	The Parking brake command is not communicated to the Guided Traction units (by the Leading Traction unit).	Ineffective immobilization and undue movement of the train. Potential collision with other trains, or infrastructure or obstacles	H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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.
			Incorrect	Incorrect LG - Parking brake command	Missed or delayed or release of the braking force (when not required / with train shall be permanently at standstill condition)	Ineffective immobilization and undue movement of the train. Potential collision with other trains, or infrastructure or obstacles	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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.
			Undue	Undue LG - Parking brake command	Possible undue parking brake application by Guided Traction unit in run time with damages to the calipers	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	HA_MIT_46	The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
0	0	**LG - Selection of the network voltage / pantograph**	No / loss of	No / loss of LG - Selection of the network voltage	The information for the selection of the pantograph to be operated is not communicated to the Guided Traction units (by the Leading Traction unit).	The Guided Traction may select a wrong pantograph, damaging Damage the overhead contact line (catenary) and/or trainborne power supply equipment.	H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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.
									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.
			Incorrect	Incorrect LG - Selection of the network voltage	Incorrect information for the selection of the pantograph to be operated is communicated to the Guided Traction units (by the Leading Traction unit).	The Guided Traction selects a wrong pantograph, damaging Damage the overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
									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.
			Undue	Undue LG - Selection of the network voltage	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**LG - Emergency pantograph fall down / opening of the circuit breaker for cut the traction current**	No / loss of	No / loss of LG - Emergency pantograph fall down and opening of the circuit breaker for cut the traction current	Potential incorrect management of connections to catenary, e.g. Leading and trailing pantographs are both connected to catenary on different charged sections.	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	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))	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.
									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.
			Undue / Incorrect	Undue LG - Emergency pantograph fall down and opening of the circuit breaker for cut the traction current	Undue request by the Leading Traction unit to Guided Traction unit to fall down the pantograph and open the circuit breaker.	Undue traction cut off by the Guided Traction unit	-	No hazardous effect.	No hazardous effect.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
2	TCMS G→ BRAKE PANELS G	**Distributed power switched on**	No / loss of	No / loss of Distributed power switched on	Incorrect management of distributed traction and brake during train run	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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. DPS switching-off shall be allowed only with train speed equal to zero.
			Incorrect	Incorrect Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
			Undue	Undue Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**Communication ok**	No / loss of	No / loss of Communication ok	The Guided Traction unit does not consider available the radio communication with the Leading Traction unit. It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Undue	Undue / Incorrect Communication ok	The Guided Traction unit unduly considers available the radio communication with the leading Traction unit. It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
0	0	**Number / position of traction units**	No / loss of	No / loss of LG - Number / position of traction units	Unknown number and/or position of traction units and possible incorrect train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
			Incorrect	Incorrect LG - Number / position of traction units	Incorrect umber and/or position of traction units used during train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
			Undue	Undue LG - Number / position of traction units	N.A.	N.A.	N.A.	N.A.	N.A.	
		Brake pipe vent command	No / loss of	No / loss of Brake pipe vent command	Guided Traction unit does not receive and apply the Brake pipe vent command sent by the Leading Traction unit. Missed traction cut-off and assistance to brake application at the Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
			Incorrect	Incorrect Brake pipe vent command	Guided Traction unit does not apply the Brake pipe vent command sent by the Leading Traction unit. Missed traction cut-off and assistance to brake application at the Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment)	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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 signaling (EN50129).
							H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
			Undue	Undue Brake pipe vent command	Guided Traction unit unduly apply the Brake pipe vent command (not sent by the Leading Traction unit). Undue traction cut-off and assistance to brake application at the Guided Traction unit	Undue brake application at the Guided Traction unit. Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
3	SAFETY LOOP G → BRAKE PANELS G	Traction unit Safety loop1 / Safety loop2	No / loss of	No / loss of Traction unit Safety loop1 / Safety loop2	Undue closing of a (single) safety loop (when should be open) in the Guided Traction unit or its closing is unduly detected by the Brake panel. Emergency brake is not commanded in the Guided Traction unit and not communicated to the Leading Traction units (by the DPS panel of the Guided Traction, via MOB, TCMS, radio) and then to the other Guided Traction unit(s)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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).
			Incorrect	Incorrect Traction unit Safety loop1 / Safety loop2	Undue closing status of both safety loops (when should be open) in the Guided Traction unit or their closing is unduly detected by the Brake panel. Emergency brake is not commanded in the Guided Traction unit and not communicated to the Leading Traction units (by the DPS panel of the Guided Traction, via MVB, TCMS, radio) and then to the other Guided Traction unit(s).	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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).
									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.
			Undue	Undue Traction unit Safety loop1 / Safety loop2	Undue opening of (one or both) the safety loops (when should be open) in the Guided Traction unit. Emergency brake is unduly commanded in the Guided Traction unit and communicated to the Leading Traction unit (by the DPS panel of the Guided Traction, via MVB, TCMS, radio) and then to the other Guided Traction unit(s).	Undue train stop.		No hazardous effect.	No hazardous effect.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
4	**BRAKE PANELS G → BRAKE PIPE**	**BP pressure setting / venting**	No / loss of	No / incomplete Brake pipe venting at the Guided Traction unit	Reduction of brake effectiveness and increase of stopping distance. Increase of in-train longitudinal force	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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).
			Incorrect	Incorrect setting of Brake pipe pressure at the Guided Traction unit	Service (dynamic and pneumatic) brake is not applied by all the locomotives at the set level. Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). Increase of in-train longitudinal force.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
			Undue	Undue Brake pipe venting at the Guided Traction unit	Only the guided locomotive vents the brake pipe.	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
5	BRAKE PIPE → BRAKE PANELS G	Brake pipe pressure from transducer#1 / transducer#2	No / loss of	No / loss of Brake pipe pressure from transducer#1 / transducer#2	Pressure transducer #1 or #2 in the Guided Traction unit does not measure pressure in the BP. Wrong monitoring of BP pressure and possible _ undue brake application on Guided Traction unit _missed traction cut-off and assistance to brake application on Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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 detected during operation and shall trigger an action to stop the operation of the train.
			Incorrect	Incorrect Brake pipe pressure from transducer#1 / transducer#2	Pressure transducer #1 and #2 in the Guided Traction unit provide different measures of pressure on the BP. Wrong monitoring of BP pressure and possible _ undue brake application on Guided Traction unit _missed traction cut-off and assistance to brake application on Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
							H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 detected during operation and shall trigger an action to stop the operation of the train.
									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).
			Undue	Undue Brake pipe pressure from transducer#1 / transducer#2	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
6	BRAKE PANELS G → TCMS G	**Unexpected brake pipe pressure reduction**	No / loss of	No / loss of DPS Unexpected brake pipe pressure reduction (DBC_VSDBCOk used as state)	The leading Traction unit is not informed on the detection of a reduction of the brake pipe pressure and does not command the brake application to the remaining Guided Traction unit(s).	Increase of the stopping distance in case of EB request sent from a Guided Traction unit (due to the detection of any condition requiring the train stop, i.e. under which conventional train apply EB up to train standstill). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Undue	Undue DPS Unexpected brake pipe pressure reduction (DBC_VSDBCOk used as state)	The leading Traction unit is unduly informed on the detection of a reduction of the brake pipe pressure (when it is not the case) and commands the brake application to the remaining Guided Traction unit(s).	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
		Emergency brake request	No / loss of	No / loss of Emergency brake request	The Emergency brake request is not communicated to the Leading Traction units (by a Guided Traction unit). Missed or delayed application of emergency brake by the other (leading and guided) Traction units, when required.	Increase of the stopping distance in case of EB request sent from a Guided Traction unit (due to the detection of any condition requiring the train stop, i.e. under which conventional train apply EB up to train standstill). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
									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).
			Incorrect / Undue	Undue Emergency brake request	Undue Emergency brake request communicated to the Leading Traction units ((i.e. without traction cut-off and brake application) by a Guided Traction unit. Undue application of emergency brake by the other (leading and guided) Traction units.	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
		DPS Brake status / Brake pipe pressure	No / loss of	No Brake status / Brake pipe pressure	Guided Traction unit can not notify the BP pressure status to the TCMS and to the Leading Traction unit by mean radio.	_No effect, diagnostic function. The Leading Traction unit apply the brake application anyway in case of brake pipe pressure reduction.	H_5_3	Excessive train stopping distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
									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).
			Incorrect	Incorrect Brake status / Brake pipe pressure	Incorrect communication of the BP pressure status to the TCMS and to the Leading Traction unit by mean radio.	_No effect, diagnostic function.	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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).
									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).
			Undue	Undue Brake status / Brake pipe pressure	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
7	TCMS G→ TCMS L	**GL - Traction unit orientation**	No / loss of	No / loss of GL - Traction unit orientation	Missed set of train orientation at one or more guided Traction units (with respect to the orientation set by the driver for the leading Traction unit)	Undue movement of the train in wrong direction (with respect to the orientation set by the driver for the leading Traction unit)	H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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.
			Incorrect	Incorrect GL - Traction unit orientation	Different orientation established for one or more guided Traction units (with respect to the orientation set by the driver for the leading Traction unit)	Undue movement of the train in wrong direction (with respect to the orientation set by the driver for the leading Traction unit)	H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
			Undue	Undue GL - Traction unit orientation	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**GL - Radio connection Status**	No / loss of	No / loss of GL - Radio connection Status	The Leading Traction unit does not consider available the radio communication with the Guided Traction unit. It could occur when an emergency request or critical information (e.g. alarm) has to be sent by the Guided Traction unit.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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.
									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.
									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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
			Incorrect	Incorrect GL - Radio connection Status	The Leading Traction unit unduly considers available the radio communication with the Guided Traction unit. It could occur when an emergency request or critical information (e.g. alarm) has to be sent by the Guided Traction unit.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
									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 signaling (EN50129).
									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.
									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).
			Undue	Undue GL - Radio connection Status	N.A.	N.A.	N.A.	N.A.	N.A.	
		GL - Emergency brake request	No / loss of	No / loss of GL - Emergency brake request	The Emergency brake request is not communicated to the Leading Traction units (by a Guided Traction unit). Missed or delayed application of emergency brake by the other (leading and guided) Traction units, when required.	Increase of the stopping distance in case of EB request sent from a Guided Traction unit (due to the detection of any condition requiring the train stop, i.e. under which conventional train apply EB up to train standstill). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
									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).
			Incorrect / Undue	Undue GL - Emergency brake request	Undue Emergency brake request communicated to the Leading Traction units ((i.e. without traction cut-off and brake application) by a Guided Traction unit. Undue application of emergency brake by the other (leading and guided) Traction units.	Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
		GL - Traction apply report	No / loss of	No / loss of GL - Traction apply report	The Leading Traction unit has not information on the traction effort applied by the Guided Traction unit. The driver has not complete control of the train traction.	Performance degradation	-	No hazardous effect.	No hazardous effect.	
			Incorrect	Incorrect GL - Traction apply report	The Leading Traction unit has incorrect information on the traction effort applied by the Guided Traction unit. The driver has not complete control of the train traction.	Performance degradation	-	No hazardous effect.	No hazardous effect.	
			Undue	Undue GL - Traction apply report	N.A.	N.A.	N.A.	N.A.	N.A.	
		GL - Brake status / Brake pipe pressure reports	No / loss of	No / loss of GL - Brake status / Brake pipe pressure reports	The Lading Traction unit has not information on the status of (local, pneumatic) brake applied by the Guided Traction unit(s) and/or on Brake pipe pressure. Potential incorrect / unsafe management of brake. Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance).	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train stopping distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
									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).
			Incorrect	Incorrect GL - Brake status / Brake pipe pressure reports	The Lading Traction unit has incorrect information on the status of (local, pneumatic) brake applied by the Guided Traction unit(s) and/or on Brake pipe pressure. Potential incorrect / unsafe management of brake. Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance).	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
									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).
									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).
			Undue	Undue GL - Brake status / Brake pipe pressure reports	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**GL - Air flow / Main reservoir pressure reports**	No / loss of	No / loss of GL - Air flow / Main reservoir pressure reports	The Lading Traction unit has not information on the Air flow / Main reservoir pressure.	Missed or partial supply of energy for brake force generation. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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_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.
									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).
			Incorrect	Incorrect GL - Air flow / Main reservoir pressure reports	The Lading Traction unit has incorrect information on the Air flow / Main reservoir pressure.	Missed or partial supply of energy for brake force generation. Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
									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_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.
									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).
			Undue	Undue GL - Air flow / Main reservoir pressure reports	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
0	0	**GL - Alarms (e.g. Fire, Motor temperature)**	No / loss of	No / loss of GL - Allarm (e.g. Fire, Motor temperature)	The Driver at the Leading Traction unit has not information on the detection of fire / high traction motor temperature.	Missed reaction by the driver (e.g. stop of the train, fire fighting unit activation) in case of operational relevant failure or incident on Traction unit	H_14_2	Operational relevant failures and disturbances during train run	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).
									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.
									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).
									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.
			Incorrect / Undue	Undue GL - Allarm (e.g. Fire, Motor temperature)	The Driver at the Leading Traction unit has undue information on the detection of fire / high traction motor temperature (when not occurred)	Undue reaction by the driver (e.g. stop of the train, fire fighting unit activation) without any operational relevant failure or incident on Traction unit	-	No hazardous effect.	No hazardous effect.	
0	0	**GL - Selected network voltage / pantograph**	No / loss of	No / loss of GL - Correspondance of network voltage	The Leading Traction unit has not information on the selected network voltage / pantograph from a Guided Traction unit. Potential use of an improper pantograph with respect to the network and voltage system	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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).
			Incorrect	Incorrect GL - Correspondance of network voltage	The Leading Traction unit has incorrect information on the selected network voltage / pantograph from a Guided Traction unit. Potential use of an improper pantograph with respect to the network and voltage system	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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).
			Undue	Undue GL - Correspondance of network voltage	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**GL - Pantograph / Main circuit status report**	No / loss of	No / loss of GL - Panthograph status report	The Leading Traction unit has not information on the status of pantograph and main circuit breaker from a Guided Traction unit. Potential incorrect management of connections to catenary, e.g. Leading and trailing pantographs are both connected to catenary on different charged sections.	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	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))	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.
									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.
			Incorrect	Incorrect GL - Panthograph status report	The Leading Traction unit has incorrect information on the status of pantograph and main circuit breaker from a Guided Traction unit. Potential incorrect management of connections to catenary, e.g. Leading and trailing pantographs are both connected to catenary on different charged sections.	Potential damage to the infrastructure (catenary overhead) and / or train (on-board power supply system).	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))	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.
									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.
			Undue	Undue GL - Panthograph status report	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
8	TCMS L→ BRAKE PANELS L	**Distributed power switched on**	No / loss of	No / loss of Distributed power switched on	Incorrect management of distributed traction and brake during train run	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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. DPS switching-off shall be allowed only with train speed equal to zero.
			Incorrect	Incorrect Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
			Undue	Undue Distributed power switched on	N.A.	N.A.	N.A.	N.A.	N.A.	
0	0	**Communication ok**	No / loss of	No / loss of Communication ok	The Leading Traction unit does not consider available the radio communication with the Guided Traction unit. It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Undue	Undue / Incorrect Communication ok	The Leading Traction unit unduly considers available the radio communication with the Guided Traction unit(s). It could occur when commands for the control of the train run (traction / brake) have to be sent by the leading Traction unit (worst case: emergency brake)	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance		
0	0	**Number / position of traction units**	No / loss of	No / loss of LG - Number / position of traction units	Unknown number and/or position of traction units and possible incorrect train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
			Incorrect	Incorrect LG - Number / position of traction units	Incorrect umber and/or position of traction units used during train configuration	Potentially unsafe set of configuration data, i.e. leading to an hazardous management of distributed traction and brake.	H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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).
									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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
									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 signaling (EN50129).
			Undue	Undue LG - Number / position of traction units	N.A.	N.A.	N.A.	N.A.	N.A.	
9	**SAFETY LOOP L → BRAKE PANELS L**	**Traction unit Safety loop1 / Safety loop2**	No / loss of	No / loss of Traction unit Safety loop1 or Safety loop2	Undue closing of a (single) safety loop (when should be open) in the Leading Traction unit or its closing status is unduly detected by the Brake panel. Emergency brake may be not commanded in the Leading Traction unit (by the existing Brake panel) and not communicated to the Guided Traction units (by the DPS panel, via MVB, TCMS, radio).	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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).
			Incorrect	Incorrect Traction unit Safety loop1 / Safety loop2	Undue closing of both the safety loops (when should be open) in the Leading Traction unit or their closing status is unduly detected by the Brake panel. Emergency brake is not commanded in the Leading Traction unit (by the existing Brake panel) and not communicated to the Guided Traction units (by the DPS panel, via MVB, TCMS, radio).	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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).
									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.
			Undue	Undue Traction unit Safety loop1 / Safety loop2	Undue opening of (one or both) the safety loops (when should be open) in the Leading Traction unit. Emergency brake is unduly not commanded in the Leading Traction unit (by the existing Brake panel) and communicated to the Guided Traction units (by the DPS panel, via MVB, TCMS, radio)	Undue train stop.		No hazardous effect.	No hazardous effect.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
10	**BRAKE PIPE → BRAKE PANELS L**	**Brake pipe pressure from transducer#1 / transducer#2**	No / loss of	No / loss of Brake pipe pressure from transducer#1 / transducer#2	Pressure transducer #1 or #2 in the Leading Traction unit does not measure pressure in the BP. Wrong monitoring of BP pressure and possible _ undue brake application on Guided Traction unit _missed traction cut-off and assistance to brake application on Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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 detected during operation and shall trigger an action to stop the operation of the train.
			Incorrect	Incorrect Brake pipe pressure from transducer#1 / transducer#2	Pressure transducer #1 and #2 in the Leading Traction unit provide different measures of pressure on the BP. Wrong monitoring of BP pressure and possible _ undue brake application on Guided Traction unit _missed traction cut-off and assistance to brake application on Guided Traction unit	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
							H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 detected during operation and shall trigger an action to stop the operation of the train.
									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).
			Undue	Undue Brake pipe pressure from transducer#1 / transducer#2	N.A.	N.A.	N.A.	N.A.	N.A.	

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
11	BRAKE PANELS L → TCMS L	**Traction interlock request**	No / loss of	No / loss of DPS traction interlock request vehicle	TCMS (of the leading TU) does not receive the request of traction cut off from DPS in case of brake application	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Incorrect / Undue	Undue DPS traction interlock request vehicle	Undue cut off the traction effort (when not required)	The whole traction effort could be not enough for train running at the required speed. In-train longitudinal forces are still acceptable. No hazardous effect.	-	No hazardous effect.	No hazardous effect.	
		Emergency brake command	No / loss of	No / loss of Emergency brake command	The Emergency brake command is not communicated to TCMS (via MVB) and then to the Guided Traction units (via radio).	Missed or delayed application of emergency brake(i.e. missed traction cut-off and assistance to brake application) by one or more guided Traction unit. when required.	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
			Incorrect / undue	Incorrect Emergency brake command	The Emergency brake command is unduly communicated to TCMS (via MVB) and then to the Guided Traction units (via radio, when not required).	Application of emergency brake at the Guided Traction unit(s), while it is not applied at the Traction unit. Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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 signaling (EN50129).
									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).

DEVIATION AT THE INTERFACE					FAILURE EFFECTS (worst case)		HAZARD		MITIGATIONS	
Int	Interface	Main data / signal	Guide-words	Deviation	Local effect	Final effect	ID	Description	ID	Description
		Service brake request to set level	No / loss of	No / loss of Dynamic brake request to set level	The Service brake set point is not communicated to TCMS (via MVB) and then to the Guided Traction units (via radio). Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). The driver can not control the traction / brake forces of all vehicles.	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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.
									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.
			Incorrect	Incorrect Dynamic brake request to set level	An incorrect Dynamic brake set point is communicated TCMS (via MVB) and then to the Guided Traction units (via radio). Reduction of brake effectiveness, mitigated by the Emergency brake application (if required by ATP to met the stopping distance). The driver can not control the Dynamic brake forces of all vehicles. Different levels of traction or dynamic braking are applied by the different Traction units, with potential increase of in-	Train is not stopped within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle). Excessive in-train longitudinal forces (and potential train separation and/or derailment).	H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance	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 signaling (EN50129).
							H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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.
			Undue	Undue Dynamic brake request to set level	N.A.	N.A.	N.A.	N.A.	N.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)

Appendix D Hazard Log

HAZARD		MITIGATION	
ID	Description	ID	Description
H_1_1	Increase of vehicle axle load	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.
H_1_2	Long bridges with excessive cross winds	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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.
H_1_3	Long bridges with hazardous dynamic behaviour (i.e. natural frequencies coupled with vibrations induced by trains)	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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.
H_1_4	Excessive overall mass of DPS train brake with respect to the infrastructure	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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.
H_1_5	Excessive longitudinal forces transmitted to the infrastructure due to the brake application by DPS train.	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 behavior due to (natural frequencies coupled with the vibrations induced by trains), to the total longitudinal forces due to the brake application.
		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.
H_2	Interference between train and loading gauge due to changes in train shape	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.
H_3_1	Loss of integrity of coupling between units	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_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).
		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).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_3_2	Excessive stretch length after stopping of the train due to distributed traction/braking	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).
H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance	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).
		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.
		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).
		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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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.
		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.
		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.

HAZARD		MITIGATION	
ID	Description	ID	Description
		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.
		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.
		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).
		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 signaling (EN50129).
		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.
		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. DPS switching-off shall be allowed only with train speed equal to zero.
		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).
		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.
		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.
		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.
		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.
		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.

HAZARD		MITIGATION	
ID	Description	ID	Description
		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.
		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.
		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.
		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).
		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).
		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_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off.
		HA_MIT_46	The (leading and guided) Traction units shall disabled the parking brake application when the train is in not at standstill condition.
		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 (EN50129), on software for railway control and protection systems (EN50128) and on safety-related communication in transmission systems (EN50159).
		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 (EN50129) and on software for railway control and protection systems (EN50128).

HAZARD		MITIGATION	
ID	Description	ID	Description
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
H_4_2	Excessive in-train longitudinal forces due to specific track characteristics	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.
		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.
H_4_3	Excessive in-train longitudinal forces due to specific manoeuvre	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.
H_4_4	Excessive in-train longitudinal forces due to severe loads distribution over wagons	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.
		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.
H_5_1	Excessive train stopping distances or speed due to an impaired (or lost) braking capability	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.

HAZARD		MITIGATION	
ID	Description	ID	Description
H_5_2	Excessive train stopping distances or speed due to an excessive timing of reaction for braking application	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.
		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);
		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).
		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.
H_5_3	Excessive train stopping distances or speed due to distributed traction and braking performance	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.
		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).
		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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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.
		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.

HAZARD		MITIGATION	
ID	Description	ID	Description
		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_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.
		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.
		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.
		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).
		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 signaling (EN50129).
		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.
		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. DPS switching-off shall be allowed only with train speed equal to zero.
		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.
		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.

HAZARD		MITIGATION	
ID	Description	ID	Description
		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.
		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).
		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.
		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.
		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.
		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.
		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.
		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).
		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).
		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).

HAZARD		MITIGATION	
ID	Description	ID	Description
		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.
		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).
		HA_MIT_45	Procedures shall be defined specifying the actions and the responsibility of the driver for train running with DPS switched-off.
		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 (EN50129), on software for railway control and protection systems (EN50128) 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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
		SIL_MIT_13	The Automatic Train Protection 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 (EN50129) and on software for railway control and protection systems (EN50128).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_5_4	Excessive train speed due to an undue release of brakes	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.
H_5_5	Temporary speed restriction not fulfilled with the whole length of the train	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.
		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.
H_5_6	Missed / ineffective reduction of the train speed by the driver (acting on traction and dynamic brake).	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.
H_6	Undue train braking or train unduly immobilized	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.
H_7_1	Undue train movement due to a failure / undue release of parking or holding brake	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_01	DPS Train shall guarantee the Parking brake application (assuring the standstill condition), specifically during the Train initial test, as for conventional trains.
		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 (EN50129) and on software for railway control and protection systems (EN50128).
H_7_2	Undue train movement due to a failure / undue release of parking or holding brake	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 .
H_7_3	Undue train movement due to a shunting operation made by the driver	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).
		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.

HAZARD		MITIGATION	
ID	Description	ID	Description
H_8_1	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to incorrect selection of pantograph(s)	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).
		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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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 signaling (EN50129).
		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.
		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.
		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).
		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 (EN50129) and on software for railway control and protection systems (EN50128).

HAZARD		MITIGATION	
ID	Description	ID	Description
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. disconnection / connection to the catenary, by the opening and closing of main circuit breaker, and the lowering and arising of pantograph(s))	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.
		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.
		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.
		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 (EN50129) and on software for railway control and protection systems (EN50128).
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	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).
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)	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).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_10_1	Incorrect (unsafe) train composition or configuration due to staff error	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_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).
		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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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.
		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.
		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 signaling (EN50129).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
H_10_2	Intendent change of train configuration data by staff during operation	HA_MIT_04	DPS Train shall guarantee the integrity of train configuration data and make impossible any change after a valid Start of mission.
		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 (EN50129) and on software for railway control and protection systems (EN50128).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_10_3	Unsafe manoeuvre of the driver, due to a wrong train orientation	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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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.
		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 signaling (EN50129).
H_10_4	Unsafe manoeuvre of the driver, which does not remember the received prescriptions after a long train stop or after driver change	PHA_MIT_27	Procedures shall be defined in order to avoid that applicable prescriptions for train running (received by trackside signaling operators) are not remembered by the driver of DPS train after a long train stop or after driver change, as for conventional trains.
H_10_5	Unsafe management of train equipment in the crossing of neutral section due to staff error	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).
H_10_6	Improper use of compressor to restore the minimum pressure in the main air reservoir	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).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_10_7	Unsafe condition of the train after end-of mission due to staff error	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.
H_11_1	The distance before a main signal and a previous danger point is too short to host the train.	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.
		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.
H_11_2	A main signal stop the train with the pantograph of the guided locomotive(s) under a neutral section of the catenary (avoiding contribution to traction)	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).
H_11_3	Stopping distance after a Hotbox-detector is too short to operate properly (i.e. to stop the train at the first main signal)	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.
H_11_4	New (e.g. middle) switch points (e.g. introduced for stabling tracks) are not taken into account by the interlocking central logic	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).
		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.
H_11_5	Level crossing unduly switched on before the full passage of the end of the train	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.
H_11_6	Switch point unduly manoeuvred or released or before the full passage of the end of the train.	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.
		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.
H_12	Train misrouted on a wrong (non-adequate) line	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.

HAZARD		MITIGATION	
ID	Description	ID	Description
H_13_1	Missed or incomplete execution of DPS train initial tests	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.
		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 Changing the train orientation shall be allowed only with train speed equal to zero. Allowable shunting movement of the train allowable without any of these conditions shall be defined for each application condition.
		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 (EN50129) and on software for railway control and protection systems (EN50128).
H_13_2	Incorrect execuition of DPS train initial tests	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.
		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.
		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_07	The guided Traction units of DPS train shall communicate to the leading Traction unit - by radio - the correct execution of the brake test.
		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 (EN50129) and on software for railway control and protection systems (EN50128).

HAZARD		MITIGATION	
ID	Description	ID	Description
H_14_1	Fire on-board during train run	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_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).
		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 (EN50129) and on software for railway control and protection systems (EN50128).
H_14_2	Operational relevant failures and disturbances during train run	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_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).
		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).
		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.
		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.
		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.
		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.
		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 (EN50129) and on software for railway control and protection systems (EN50128).