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 4.1

Test Demonstrators with DPS, Safety assessment 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 25
Actual submission date:	26/02/2021
Responsible/Author:	TÜV SÜD
Dissemination level:	PU
Status:	Final

Reviewed: (yes)

Document history		
Revision	*Date*	*Description*
0.1	22/10/2020	First draft, internal
0.2-0.9	-	Intermediate drafts, internal
0.10	16/02/2021	Draft released for comments
1.0	26/02/2021	Released version

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)

Report contributors		
Name	*Beneficiary Short Name*	*Details of contribution*
Emanuele Gianoglio	TÜV SÜD	Introduction, ISA strategy, Definition of the system, Functional safety assessment report, Conclusions
Paolo Gianotti	TÜV SÜD	Introduction, ISA strategy, Definition of the system, Functional safety assessment report, Conclusions
Walter Heydt	TÜV SÜD	Running dynamics assessment report, Conclusions
Bernhard Nölte	TÜV SÜD	Introduction
Dirk Thomas	TÜV SÜD	Introduction

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)

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 [6] 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 that goal, a reliable radio communication is implemented to transfer data between the Traction units and integrated with the Distributed Power System (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

Functional safety assessment activities of TÜV SÜD follow the legal requirements and the common practice for authorization of test runs on German railway infrastructure.

Involvement of authorities (German Eisenbahnbundesamt) in test runs is only necessary if the test scope includes changes to:

1. permissible wheel set loads and vehicle weights per unit length,
2. applicable dimensions of the reference line,
3. prescribed and intended operation of train radio and train control systems,
4. defined braking distances, or
5. permissible speeds.

Otherwise authorization can be done bilaterally, by the train operator and the infrastructure operator, as long as safety is assured.

Independently of the involvement of the authorities, the procedure followed for a change like the DPS train is:

1. Implement a risk management system for the test runs - according to article 5 of regulation (EU) Nr. 402/2013 as amended.
2. Provide evidence and create a declaration that all hazards and associated risks identified for the nature and extent of the test runs planned are kept at a reasonable level - according to article 16 of regulation (EU) Nr. 402/2013 as amended.
3. Involve an independent assessment body (AsBo, UBS -unabhängige BewertungsStelle-) to assess the safety of the test runs and create a safety assessment report.

Within M2O the above procedural steps are prepared but not fully implemented. TÜV SÜD performs the independent assessment (step 3.) as far as this can be done based on the achieved results of step 1. and 2.

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 assessment scope is defined by the following questions:

/Q1/ Is a CSM process implemented?

/Q2/ Are safety measures implemented and proven to be compliant to the applicable standards?

/Q3/ Do dynamic tests (simulated) show no unsafe results and no deviations, also in degraded modes?

/Q4/ Are the simulations consistent with the assumptions/constraints of the overall safety analysis?

Responses to the above questions are reported in §6.

1.3 Structure of the document

The structure of the document is the following:

- §1 - Introduction, which provides an overview of M2O project, the purpose and scope of D4.1 and the structure of the document;
- §2 - ISA Strategy, which provides the strategy adopted by the ISA to assess the safety demonstration carried out during M2O project. It includes limitations and assumptions which consider the scope of the research project;
- §3 - Definition of the System, which provides an overview of the system under assessment, namely the DPS train.
- §4 - Functional Safety Assessment, which provides the results of the functional safety assessment performed during the project;
- §5 - Running Dynamics Assessment, which provides the results of the running dynamics assessment performed during the project;
- §6 -Overall results, which provides a summary of the results deriving from the functional safety and running dynamics assessments;
- §7 -References, which provides the documental references used in this document;

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 ISA Strategy

The main topics of the assessment are:

- Assessment of the overall Risk Analysis and Evaluation
- Functional safety aspects of the interaction between the radio system and the train
- Evaluation of the overall safety analyses at train level (simulation of longitudinal forces, etc.)

For the assessment of the overall Risk analysis, the implemented process is assessed against the requirements of EN50126. Regarding generic RAMS activities, the following references are adopted:

- "Common Safety Methods" CSM (ref. Commission Implementing Regulation Nr. 402/2013 as amended by Nr. 1136/2015), for an harmonized framework for the risk assessment process through the prescription of Hazard Identification, Risk Analysis and Risk Evaluation
- EN50126 for the definition of the overall lifecycle of the system
- EN50128/EN50129/EN50159 for the functional safety aspects (affecting the interfaces between the radio subsystem and the other on-board subsystems)

The limitations and assumptions listed in §2.1 apply.

The assessment strategy adopted in the context of M2O project has been to provide continuous feedbacks, starting from the kick-off meeting held in Frankfurt in January 2019 and continuously, during the technical meetings periodically held during the project.

The main safety Deliverables steered by the technical discussions are the D2.3 (Integrated system, Safety report), D3.1 and D3.2 (First and Second Demonstrator(s) Specific application Safety case) owned by NIER, in its role of safety management for the project. These Deliverables have been the main inputs for the assessment: they have been peer to peer reviewed during the project.

The assessment has been separated in two main areas:

- Functional Safety: results are reported in §3;
- Running Dynamics: results are reported in §4.

2.1 Limitations and assumptions

The applicable limitations and assumptions on which the independent safety assessment was initially based upon are:

1. The underlying project is a research project, so the organization and independence requirements deriving from EN5012x may not be entirely complied with. These lifecycle and quality/safety management aspects are therefore out of scope. TÜV will focus on the "technical" assessment.
2. The underlying "generic products" are assumed to be assessed already, including the HW interface with the train logic

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. All vehicles are presumed to be in homologated state in terms of running dynamics -> fulfilling requirements of EN 14363, EN 15839 (and EN 16235 if applicable)
4. ISA tasks are limited to Specific Application (SA) level
5. Only one SA configuration is considered (implementation with only one type of loco)
6. Assessment of TSI compliance is out of scope

The actual status is that the assumption #2 is not satisfied: the evidence of compliance to the applicable safety standards (i.e. EN50129, EN50128/EN50657, EN50159) of the underlying products is not available at this stage of the project. The implications of this are reported in the following sections.

3 Definition of the System

The system under consideration is a Distributed Power System (DPS) Train equipped with the following main subsystems (see Figure 1):

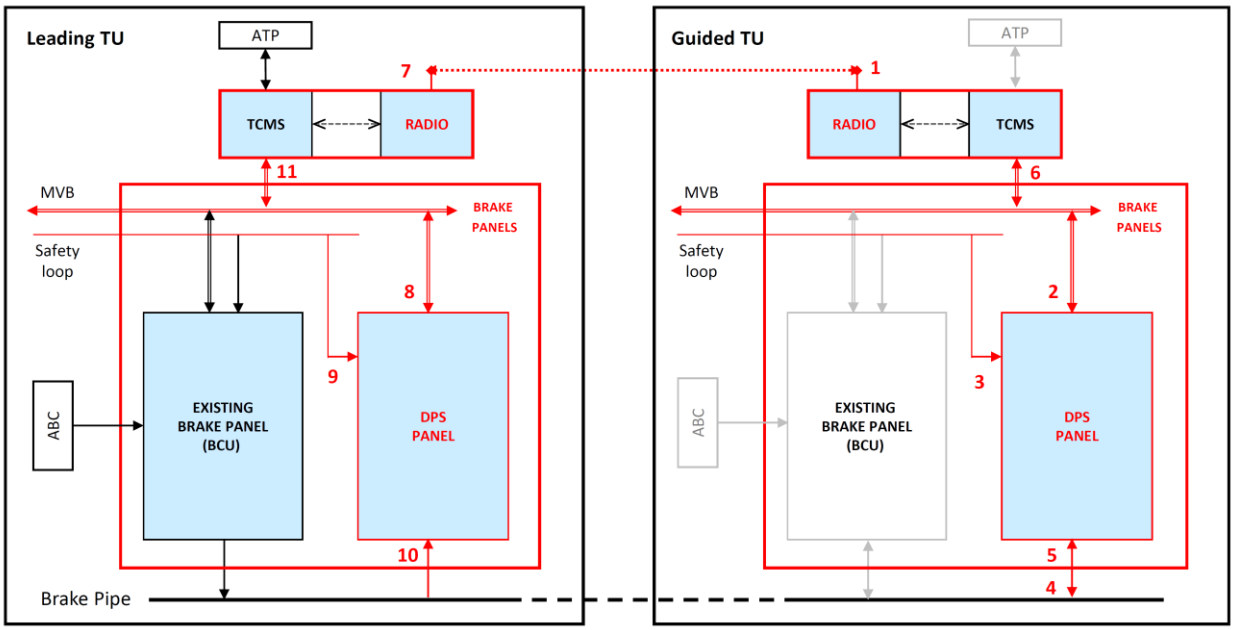


Figure 1 DPS traction units architecture

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

Emergency and Service brake), communicates with the leading TU (over a black-channel including MVB, TCMS, Radio) and monitors the Brake pipe pressure;

- Brake Pipe (unique for the leading and the guided Traction units).

In Figure 1, the existing and new interfaces related to the implementation of DPS equipment/functions are represented by red arrows. The existing interfaces, working as for conventional trains, are represented by black arrows if "active", grey otherwise.

Figure 2 provides an overview of the DPS train and its integration within the overall integrated system, made by DPS trains and trackside elements.

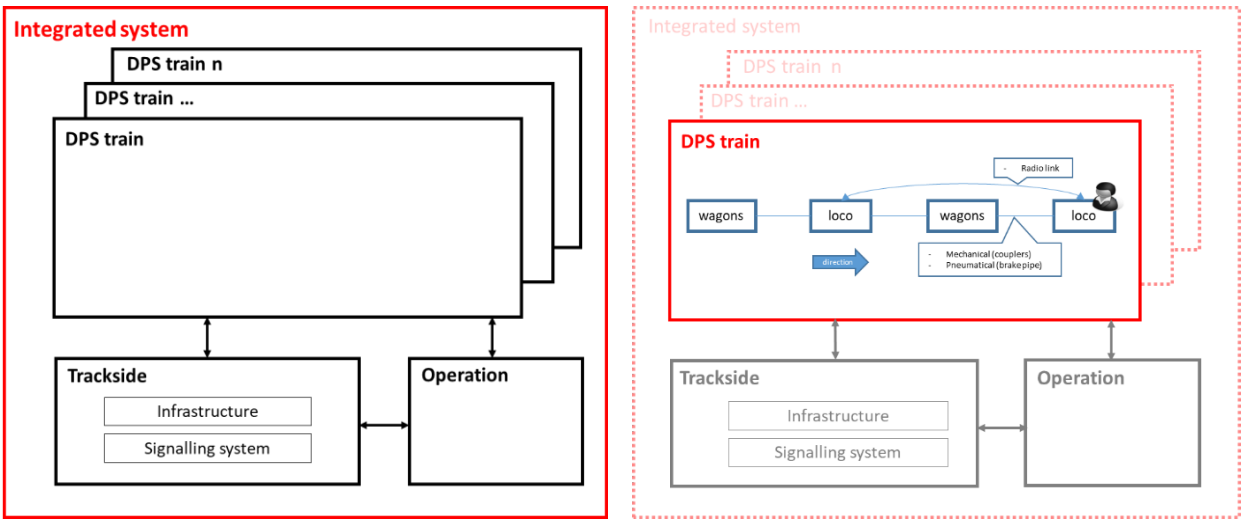


Figure 2 DPS Train

DPS trains considered for the safety analyses performed in WP2 and WP3 are the demonstrators that will be used to run on-track tests by FR8RAIL II project. They are made by up to three traction units (one leading and one/two guided) equipped with DPS: two BR 187 (TRAXX AC3) and one BR 188 (TRAXX MS3), with a total length of 660-700m.

4 Functional Safety Assessment

The following chapters describe inputs, assessment criteria, findings and appraisals of the functional safety assessment.

The "Inputs" section includes the documentation made available to the assessors during the project, which have been taken as basis for the assessment.

The "Assessment criteria" section includes the objectives of the assessment.

The "Findings" section includes the outcomes deriving from the assessment of the input documents and from the information gathered during the meeting held during the project.

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

The "Appraisal" section includes the results of the assessment, with an overall appraisal about the outcomes of the safety activities carried out during the project.

4.1 Inputs

The input documents provided by M2O Partners for the functional safety assessment are the following:

- D2.3 – Integrated system Safety report: it includes the safety plan of the project and the description and results of the performed safety analyses (Preliminary Hazard Analysis, Hazard Analysis, Interface Hazard Analysis), as well as the Hazard Log of the project.
- D3.2 – First and Second Demonstrator Specific application Safety case: it includes the safety demonstration of the DPS train demonstrators developed by FR8RAIL II for the purpose to run on-track tests, with the structure of a specific application safety case.
- D3.3 – TrainDy simulations for experimental tests system, Safety report.

4.2 Assessment criteria

The following criteria applies:

1. A suitable process for the management of the functional safety, in line with the requirements of the applicable standards, shall be adopted, considering the limitation and assumptions listed in §2.1. The assessment strategy is described in §2.
2. The adequacy of the communication system implemented between the leading and guided TUs in terms of safety shall be demonstrated, including the impact of the latencies of the different communication protocols (i.e. GSM-R, LTE).
3. The structure of the SASC shall be inspired to the requirements for a SASC according to EN50129, which shall include the following sections:
    - Definition of the system
    - Quality Management Report
    - Safety Management Report
    - Technical Safety Report
        - Assurance of correct functional operation
            - System architecture description
            - Definition of interfaces
            - Fulfilment of system requirement specification
            - Fulfilment of safety requirement specification
            - Assurance of correct HW functionality
            - Assurance of correct SW functionality
        - Effect of faults
            - Effects of single faults
            - Independence of items
            - Detection of single faults

        - Action following detection (including retention of safe state)
        - Effects of multiple faults
        - Defence against systematic faults
    - Operation with external influences
    - Safety related application conditions
    - Safety qualification test results
- Related Safety Cases
- Conclusion

4. The conclusions of the SASC shall provide adequate evidence that the residual risk to run on-track tests with the DPS train demonstrators is sufficiently low.

4.3 Findings

The safety activities performed during the M2O project include:

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

The PHA is developed for the Integrated system including long freight trains in their operational context.

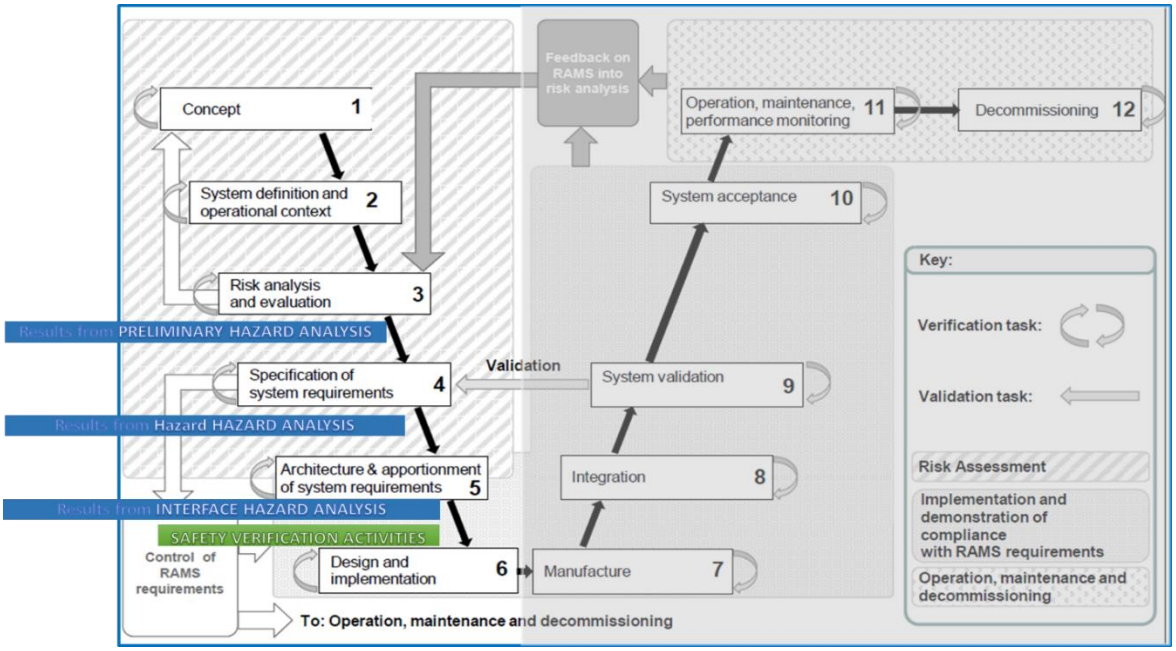
The HA is developed for a specific DPS train implementation based on the functional and system requirements specification provided by FR8RAILII project.

The IHA is developed for a specific DPS train based on the architecture implemented by the DPS train provided by FR8RAILII project.

The longitudinal dynamics simulations are used to support the safety demonstration of the system, for both the in-train longitudinal forces and the stopping distance of the DPS train. The assessment of this activity is reported in §5.

The lifecycle phases covered by the safety activities performed in the scope of this project are limited to the upper left part (design) of the Vcycle set by the EN50126.

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 safety analyses coordinated and performed by NIER (WP2) include the following steps:

- identification of a set of accidents, the corresponding consequences and their severity;
- identification of the list of the hazardous conditions related to the specific characteristics of the DPS train (PHA) and to the functions implemented by the DPS train (HA).
- definition of the mitigation strategies, depending on the consequences of each hazard.

The hazardous conditions have been derived from the functional specification of the system provided by FR8RAILII in the Deliverable D5.2.

The result of the analysis is that each hazardous condition may lead to the worst-case severity accident. Consequently, two mitigation strategies have been identified:

- "high safety integrity" → the frequency of occurrence of hazardous failures shall be less than 10-8 event/h (limit stated for SIL4 function by the EN50129);
- "low safety integrity" →the frequency of occurrence of hazardous failures shall be less than 10-6 event/h (limit stated for SIL2 function by the EN50129) 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 failure of occurrence related to catastrophic consequences).

The safety integrity levels have been apportioned to the identified countermeasures that shall be implemented in the DPS train demonstrator.

Low safety integrity functions are functions required for the DPS train set-up (i.e. train inauguration and

configuration and train initial tests), to the energy management and Diagnostics, and to the remote control of traction and service brake at the guided Traction units. They are allocated to SIL1/SIL2 train's equipment (as for conventional train) and to the radio communication between the leading traction unit and each guided traction unit, involving the (SIL2) TCMS and the non-trusted communication system (radio equipment and LTE-network) as a black channel (with a safety layer – SDTv2 has been selected - implemented on the top of it).

High safety integrity functions are allocated to SIL3/4 train's equipment (as for conventional train), involving:

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

The latency in the radio communication between Traction units has potential impact on train behaviour, when brake application is required during train run. Specifically, the time required for radio communication introduces delay between the venting of the train brake pipe at the leading Traction unit and the venting of the brake pipe at each guided Traction unit; excessive latency could reduce the effectiveness of the braking action, with increase of the train stopping distances, and/or increase longitudinal forces between units.
Latency between Train Controller Unit and Radio Controller (RCDPS) for both TU's (end-to-end with radio communication) is estimated by laboratory test to be 390 ms (+/- 15%). Laboratory performance test made on GSM-R was validated by the test run (during 2019), resulting in an additional 0.5 s. The same value has been used for LTE in a conservative way. In the modelling of DPS trains family based on LTE technology, 0.9 s +/- 15% (first contribution rounded up) has been used to characterize the delay between the command at the leading TU and its actuation at guided TU.

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

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

Considering the scope of M2O and FR8RAIL II projects, no formal Verification and Validation process has been performed (nor planned) for the DPS development and integration within the traction units: the focus of the safety V&V activities has been on the proper identification of validation activities required for the safe execution of the experimental test campaign (e.g. information deriving from test track and train documentation, test instructions). In addition to this, the results from the simulations have been used to demonstrate that also in degraded modes (without communication and without supporting the venting of the brake pipe based on the pressure sensors), the behavior of DPS trains is not worse with respect to the reference system. Therefore, concerning brake application, no specific action is required to personnel attending the guided TUs during tests.

The safety V&V activities have the final goal to demonstrate that the mitigations identified by the safety

analysis for DPS trains are implemented by the Demonstrator(s) developed by FR8RAIL II for the experimental campaign. Results have been collected in the form of a Specific Application Safety Case (SASC) in D3.2.
Due to the limitations of the research project, only some of the sections foreseen by the EN50129 could be filled. In particular, the structure of the SASC delivered by WP3 is the following:

- Definition of the system: it includes a definition of the DPS system and its sub-systems, and a description of the context in which the DPS trains have been studied, with a focus on the characteristics of the demonstrators developed by FR8RAIL II for the test runs to be performed in order to validate the requirements set out by the two projects.
- Safety management report: it describes the lifecycle adopted to carry out the safety activities, the performed safety analyses, the organisation (including the relationship with FR8RAIL II project) and the longitudinal dynamics studies.
- Technical safety report: it includes the results deriving from the safety analyses, the safety concept of the DPS train, based on the countermeasures defined according to the established risk acceptance criteria.
  Countermeasures have been defined according to the categories defined by EN50126: requirements have been divided into functional safety requirements, technical safety requirements and contextual safety requirements (including the SRACs exported to the operation of the DPS train).
  The behaviour of the DPS train is described, both in nominal mode and degraded mode, with focus on longitudinal dynamic aspects and braking distances.
  Evidences of fulfilment of safety requirements and operation with external influences are missing. This section covers the information related to: assurance of correct functional operation, effect of faults, detection of single faults, action following detection, operation with external influences, safety related application conditions.
- Related safety cases: this section shall include the reference to the underlying safety cases, which the Specific Application rely on (i.e. Generic Product/Application Safety Cases), related to the systems composing the DPS train (e.g. DPS brake panel).
  Considering the limitation of the scope of the project, such evidences were not available, thus no claim could be made about the compliance of the DPS train to the applicable safety standards.
- Conclusion: it includes a summary of the safety activities performed during M2O project and the corresponding conclusions: a detailed sets of safety validation activities to be executed before the test runs and of the related evidence to be provided by FR8RAIL II have been specified; they include:
  - evidence closing the design stage, i.e. traceability between the safety functional requirements (specified by the safety analyses) and the (last version of) functional requirements stated by FR8RAIL II projects and/or the related functional tests;
  - evidence about the proper implementation of the safety functional requirements (by functional tests);

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

Concerning the experimental test campaign, considering the lack of evidence of the correct implementation of the safety functional requirements, specific operational procedures (i.e. additional application conditions with respect to the contextual safety requirements deriving from the safety analyses) have been identified by WP3. They are reported in Table 1, together with their expected validation strategy and the corresponding evidence required for fulfilment.

Table 1 Test runs ACs

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

As a result, because of the lack of evidences from safety validation, each guided Loco is required to be manned, and specific instructions shall be provided to the on-board staff, about checks/actions to be performed and confirmations to be provided to the driver of the leading Traction unit during the execution of the test runs.

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)

4.4 Appraisal

The safety analyses performed during the project provide a suitable set of countermeasures. The process adopted by NIER to carry out these safety analyses is in line with the requirements of EN50126.

Currently:

- the safety functions implemented by the products integrated in the DPS traction units lack a corresponding safety demonstration (to prove compliance to the applicable safety standards e.g. EN50129, EN50128 / EN50657, EN50159);
- the results of the V&V activities showing the fulfilment of the requirements associated to each of the identified countermeasures are not available.

Regarding the analysis of a suitable radio communication protocol to support the operation of a DPS train, the result is that, in terms of safety, no differences are found between GSM-R and LTE, provided that the compliance of the safety layer to the requirements of EN50159 will be demonstrated.
The results of the simulations showed that also in absence of radio communication the DPS train still behaves safely in terms of longitudinal forces and stopping distances. So, also in terms of latency there is no difference in the usage of GSM-R or LTE for what concerns the safe behavior of the system during tests. This shall be confirmed for each specific application.

Regarding the safety demonstration of the brake functionality, it relies on the fact that, in the event of a loss of radio communication or failure in the control system, the required safety integrity is ensured by sensing the pressure drops in the brake pipe: when brakes - SB or EB – are applied from the leading loco, the guided loco will brake based on the pressure drop. This is supported by the results of the simulations, performed to evaluate the generated in-train longitudinal forces. The simulations show that braking distances are not exceeded even if the guided locos fail to sense the pressure drop and the braking effort is achieved in a traditional way, i.e. based on the decrease of pressure along the brake pipe (without the boost capabilities of the guided locos). This is essential, as functional safety is not demonstrated yet.

Considering that the evidences gathered during the project are limited to the design phase and that the assumptions and limitations stated in §2.1 are not fulfilled, a positive evaluation about the correct implementation of the "functional safety" countermeasures on the DPS demonstrator for the purpose of the test runs cannot be stated.
The SASC (D3.2) provides a good starting point for the safety demonstration of future DPS trains, it includes the results of the activities carried out during the project, focused on the demonstrators that will be used by FR8RAIL II to run on-track tests. The structure of the SASC is inspired to the requirements of EN50129: information are gathered to the extent of what is applicable to a research project.
For the purpose to run on-track tests with the DPS demonstrator(s), the SRACs defined by WP2-WP3, as collected in the SASC (D3.2) shall be respected.

In general, in order to exploit the results obtained by the safety analyses performed during the M20 project to a specific application of DPS train:

1) the applicable functional specification (for this SA) shall be compared with the ones taken as reference for the safety analyses.
2) The implementation of the safety countermeasures shall be demonstrated.

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 Running Dynamics Assessment

The assessment on the running dynamic behavior in terms of longitudinal dynamic behavior of the studied train consists is based on the input with respect to simulation results within the project M2O. These are:

D3.1 LTD simulation report
D3.3 TrainDy simulations for experimental tests
D2.3 First and Second Demonstrator(s), specific application safety case.

The assessment considers general simulation topics and the proceeding from investigating the general longitudinal dynamics performed in D3.1 for a high number of different freight train families with respect to the critical parameters identified in Deliverable D2.2, the simulations targeting the conditions and failure modes during the planned on-track tests with the demonstrator, towards the specific safety case for the demonstrator train.

5.1 General simulation and modelling topics

The simulations of longitudinal train dynamics were carried out using the simulation tool TrainDy, which is a tool approved by UIC for the calculation of longitudinal internal dynamics of freight trains for speeds up to 120 km/h. The software uses models of existing vehicles including modelling of the components relevant for the purpose. This implies that the vehicle models used within the simulations consider vehicles with existing homologation. This means the vehicles are compliant with requirements of TSI LOC&PAS (for locos) and TSI WAG (for freight wagons), which also includes compliance with EN 14363 or EN 15839, respectively, regarding safety against derailment under longitudinal compressive forces. The only exception from that in the performed simulations is the new loco BR188, of which one vehicle will be used in the demonstrator train. However, since this loco is already in the final stages of its homologation and its characteristics are known, it is not considered as critical. As no automatic couplers will be present in the demonstrator train, requirements resulting from UIC 530-2 with respect to this type of couplers are not considered.

Derailment risks with respect to longitudinal forces result from the combination of longitudinal compressive forces and curves of small radii, in particular two consecutive curves with a opposite sign of curvature, so called S-curves, as well as the radius of the wagons buffer plates. A general limit for permissible longitudinal compressive forces is set to 400 kN by UIC 421, considering different curve radii and buffer plate radii. The simulations performed within M2O consider curve radii down to 190 m, which is a typical radius for a switch, and the buffer plate radii for the used wagons. This is covered by the limit of 400 kN for longitudinal compressive forces stated by UIC 421, and this limit is used within the simulations as acceptance criteria.

Longitudinal tensile forces can if too high tear apart a coupler and by that divide a train consist. The simulations consider a maximum tensile force of 550 kN as limit value, which is based on experience by the French operator SNCF. This value does not disrupt the train consist if reached but will lead to fatigue issues if exceeded often. This is deemed as reasonable approach.

The braking performance in the simulations is considered on vehicle base and follows the approach of EN 14531 or UIC 544-1.

A selection of measured in-train forces measured during on-track tests in 2019 within the project EU-project Future Freight Loco four Europe (FFL4E) have been used for validation of the simulation results by the tool TrainDy. The results are presented in Deliverable D3.1 and show a good agreement between the measurement results and the corresponding simulation results, which besides the approval by UIC increases the base of confidence in the simulation results.

The general approach in the simulations is a comparison between train consists with application of DPS – either functional or in different kind of failure modes – with a reference system that represents a train consist without DPS that is today approved and possible to run in normal operational traffic. The comparison is based on a virtual probability of derailment or disruption of a train consist. The DPS based train consist is in both nominal and failure mode considered safer if the virtual probability of derailment or disruption is lower than for the already possible reference case without DPS.

5.2 Simulations of longitudinal dynamics towards the demonstrator

The simulation studies towards the application of the M2O demonstrator consists of several steps.

Deliverable 3.1 studies the influence of the most relevant parameters with impact on the longitudinal dynamics of train consists, identified in Deliverable D2.2. The identified most relevant parameters are

- Communication delay between the traction units
- Time to fill the brake cylinders up to 95%
- Braking efficiency
- Pressure in the brake cylinders at the beginning of the filling.

Those parameters always showed the by far most significant impact on the resulting longitudinal compression forces - both positively and negatively, depending on the variation of the parameters – for different kinds of train families. The potential deterioration of the longitudinal compression forces resulted in up to more than 10% when compared to a reference train family. Except for the impact of the slope of the track – which is taken into account during the simulations performed in D3.3 – all other studied influence parameters of Deliverable D2.2 resulted in a much less impact of the longitudinal train dynamics, which motivates the necessity to include these identified four impact parameters named above in the following analyses.

The analysis of D3.1 Is performed by means of a parameter study with a large number of train families, based on existing train families taken from a database by Deutsche Bahn. Additionally, different braking regimes were considered. The simulated cases are based on a number of maneuvers that have been identified as the most critical ones in previous projects, such as emergency braking and emergency braking from full traction with and without communication loss. The study is performed on flat track only, without any influence of track gradients due to topographic characteristics. This is reasonable at this stage of the investigation for the identification of train consists that can be run safely with DPS. The influence of track gradients is considered later within the work of Deliverable D3.3. The study also takes different types of communication for the DPS-system, namely GSM-R and LTE, as well as an ideal communication without interruption representing 5G. The Deliverable identifies a number of train families that can be run safely with DPS under GSM-R. The number can be even increased using LTE communication.

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 D3.3 takes both the results from Deliverable D2.2 and D3.1 and presents the results for a number of train consists performing different maneuvers, and studies the influence of communication loss in the DPS system. The study presented in D3.3 also takes topographic characteristics of the intended test track into account and applies a number of DPS failure cases that are important in combination with track gradients. The considered maneuvers are extended compared to Deliverable D3.1, and contain operations usual for normal operation, such as

- Acceleration to coasting
- Service braking from coasting
- Emergency braking from coasting
- Acceleration up to coasting speed with immediate emergency braking

For the latter operations, the simulations also compare the influence of cast iron brake shoes and LL brake shoes, considering the ongoing change to LL shoes in conjunction with the implementation of quieter routes.

Degraded modes, i.e. a communication loss between the traction, are additionally considered with the following maneuvers

- Accelerations to coasting, followed by period of communication loss and breaking of leading traction unit (reaction of DPS on guided traction unit after re-installed communication)
- Braking from coasting, followed by a communication loss and even harder braking of leading traction unit (reaction of DPS on guided traction unit after re-installed communication)
- Braking from coasting, followed by communications loss and service or emergency brake at the same time (reaction of DPS on guided traction unit when detection of pressure drop in brake pipe of 0.2 bar)
- Acceleration to coasting followed by immediate emergency brake of leading traction unit with communication loss at the same time (reaction of DPS on guided traction unit when detection of pressure drop in brake pipe of 0.2 bar)
- Emergency braking from coasting together with communication loss

For the maneuvers including communication loss, the topography of the test track for the M2O demonstrator is considered, which is reasonable as these maneuvers potentially increase longitudinal compressive or tensile forces.

The results show that trains with applied DPS in most cases perform better than the respective reference trains without DPS. For failure modes of the DPS that occur on track gradients the resulting longitudinal dynamic behavior can however be worse than the corresponding reference system, but then still respects the admissible values for LCF.

For some train families with a consist of one loco both in the front and at the end of the train, the maximum admissible LCF of 400 kN is not always respected when a communication loss appears. This behavior is coupled to the gradient of stepwise traction reduction in the second loco when the pressure drop of 0.2 bar is recognized, and can be controlled by adjusting this gradient. For the demonstrator it thus needs to be made sure that the traction reduction is performed in such way that the admissible LCF values

are respected.

With specific respect to the M2O Demonstrator and the not yet fully implemented functional safety, the last two maneuvers considering the communication loss were also studied for the case that the emergency braking is not commanded by the leading traction unit, but by the or one of the guiding units. This would lead to high longitudinal tensile forces that potentially can interrupt a train consist. Only for a train consist with three traction units and an emergency braking during acceleration phase initiated by the last traction unit in running direction together with a communication loss at the same time, a train disrupt may potentially occur. The DPS systems however performs in any case at least equally or better than the reference train consist. Even though the probability of occurrence for such an event is considerably low, measures have to be taken into account for the demonstrator runs to avoid this, such as the presence of a driver in all traction units with communication among each other.
Longitudinal compressive forces are for these cases of no concern.

Additionally, a failure of a DPS unit is simulated on one traction unit for the next to last maneuvers with communication loss (acceleration followed by immediate emergency brake), when the DPS unit does not recognize the pressure drop, and the braking command is initiated by the driver on the respective loco. The resulting compressive forces for train consists using DPS us in this case usually lower than for the reference train consist, but can exceed the value of 400 kN. The test of this case is thus to be performed using a train consist that respects the value of 400 kN for the longitudinal compressive forces

The safety case for the Demonstrator, presented in Deliverable D2.3, also considers the maneuver of acceleration followed by immediate emergency braking for the specific wagons for the M2O demonstrator, both with and without communication loss, for both running direction, for G and LL brake regime, and for both running directions. The resulting compressive forces are lower for the trains using DPS than for the reference trains. For some simulated train consists, the admissible compressive forces are exceeded. In such case, a train consist hat to be chosen that respects the admissible compressive forces. The longitudinal tensile forces can partly be higher for trains with DPS compared to the reference trains, but their magnitude is of no concern.

The safety case of Deliverable D2.3 also considers the braking distance both for nominal working DPS and failure modes for different train consists. It is shown that for almost all cases, the DPS system both in nominal and in failure mode – including the failure of recognizing the pressure drop of 0.2 bar – leads to shorter braking distances than for the reference train. Only in case of three active traction units and the application of full traction for all of those, the braking distance may can be higher than for the reference train with only two traction units. If the maximum traction for the DPS train with three traction units is reduced to approx. 67%, the braking distance is about the same as the reference train. The amount of traction reduction is however not within the scope of the project. For all cases, the maximum braking distances required by UIC 544-1, are respected.

The simulations have shown that a safe operation of the M2O demonstrator with respect to longitudinal compressive and longitudinal tensile forces is possible, taking into account the constraints named above with respect the choice of the specific train consist and the presence of drivers with communication among each other in all traction units.

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

6 Overall results

The following "answers" are related to the "questions" defined in §1.2.

/R1/ A CSM process was implemented:

1. Hazards were identified through the safety analyses (PHA, HA, IHA) performed in WP2.
2. Safety countermeasures were defined, as a result of point 1.
3. The relevant stakeholders were involved in the process (partners of FR8RAIL II project).
4. The CSM is satisfactorily implemented, and safety measures were exported, as necessary.

/R2/ Evidence of implementation of the safety measures is incomplete.

/R3/ Simulations of dynamic tests show no unsafe results and no deviations, also in degraded modes (e.g. of loss of communication, misbehaviour of the brake system's DPS panel)

/R4/ Running Dynamics results are consistent with Functional Safety results.

The lack of safety demonstration regarding the communication system, the train logic and their interfaces is not relevant for tests taking into account the results of the simulations and the countermeasures to be implemented.

The ISA has no objections and does support the authorisation to run dynamic tests, provided that the provisions resulting from the safety analyses are observed by the operators while running tests.

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

7 References

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

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

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

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

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

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

[7] "Common Safety Methods" CSM (ref. Commission Implementing Regulation Nr. 402/2013 as amended by Nr. 1136/2015

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

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

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

[11] M2O project, Deliverable D 3.2 - First and Second Demonstrator(s), Specific application Safety case

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