MARATHON 2 OPERATION (M2O)

General concept of trains' safety with Distributed Power Systems, general operational mitigations and procedures

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

CONTENT

- **General context** for safety analysis
- **Functional model** of DPS trains
- DPS trains **architecture and internal interfaces**
- System **lifecycle and safety activities**
- **Hazardous conditions** related to DPS train operation
- **Safety integrity levels** allocation
- **Safety requirements** specification and verification
- **Experimental test** campaign

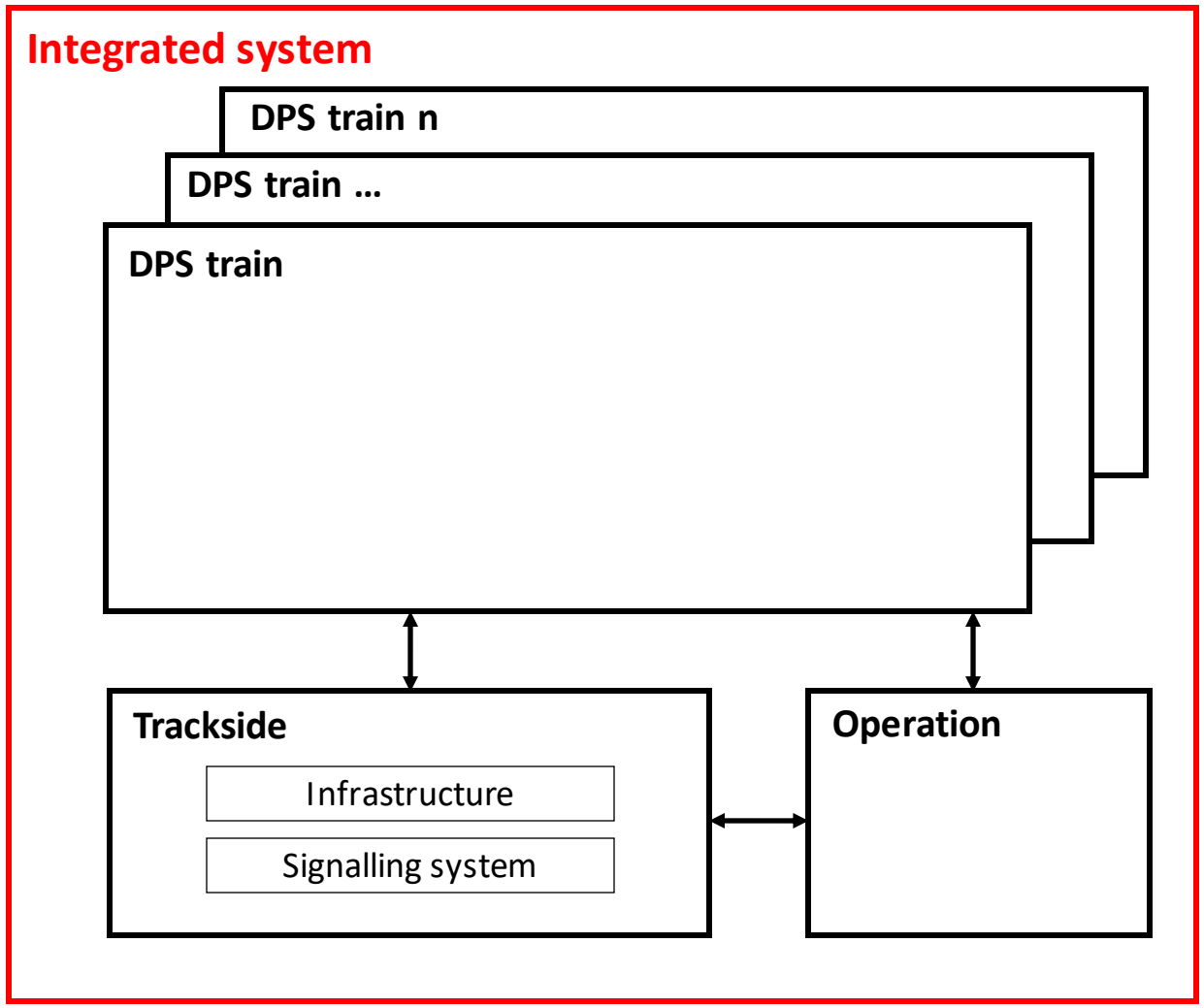
marathon 2 operation

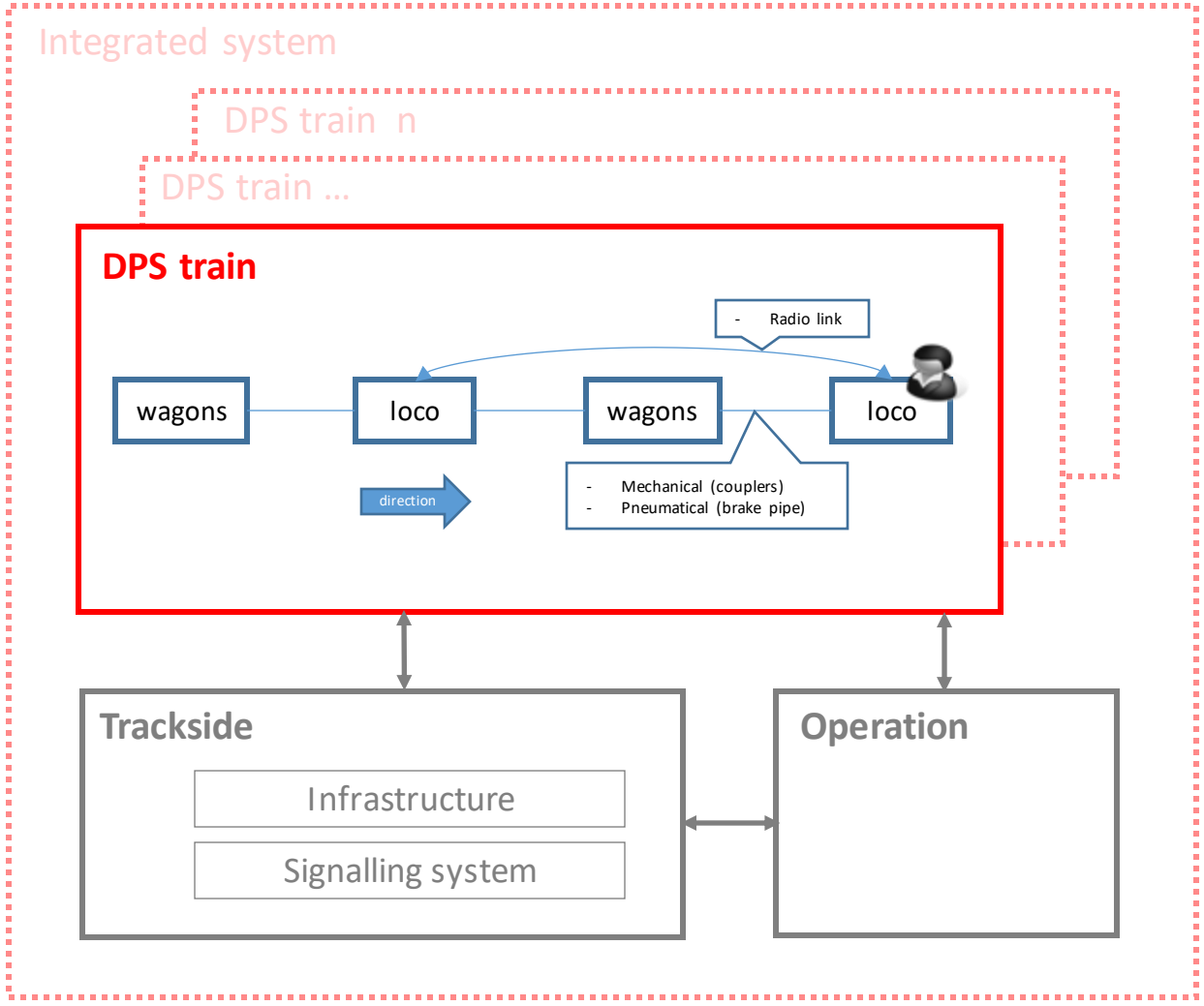
MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

GENERAL CONTEXT FOR SAFETY ANALYSIS

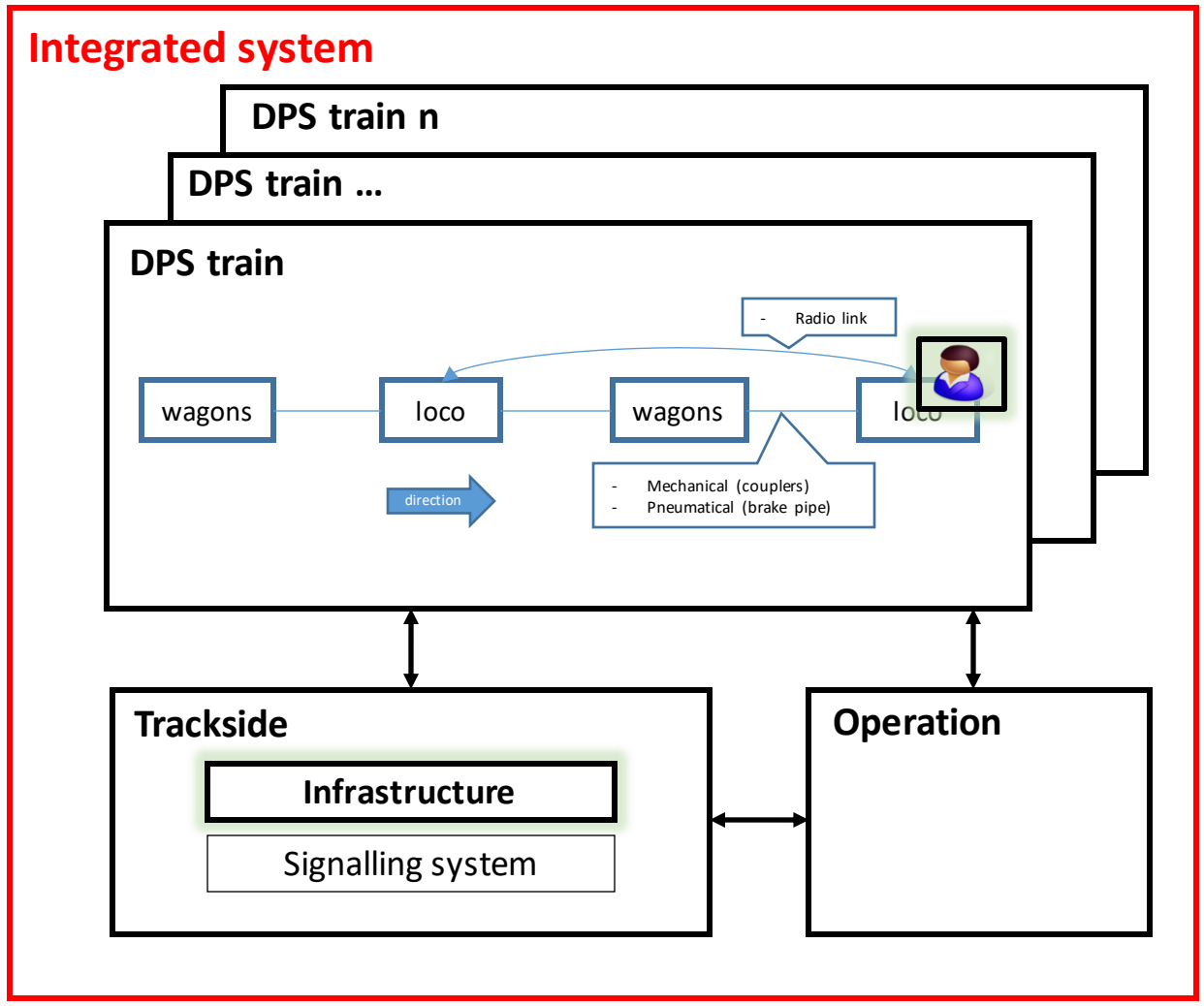




MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

GENERAL CONTEXT FOR SAFETY ANALYSIS



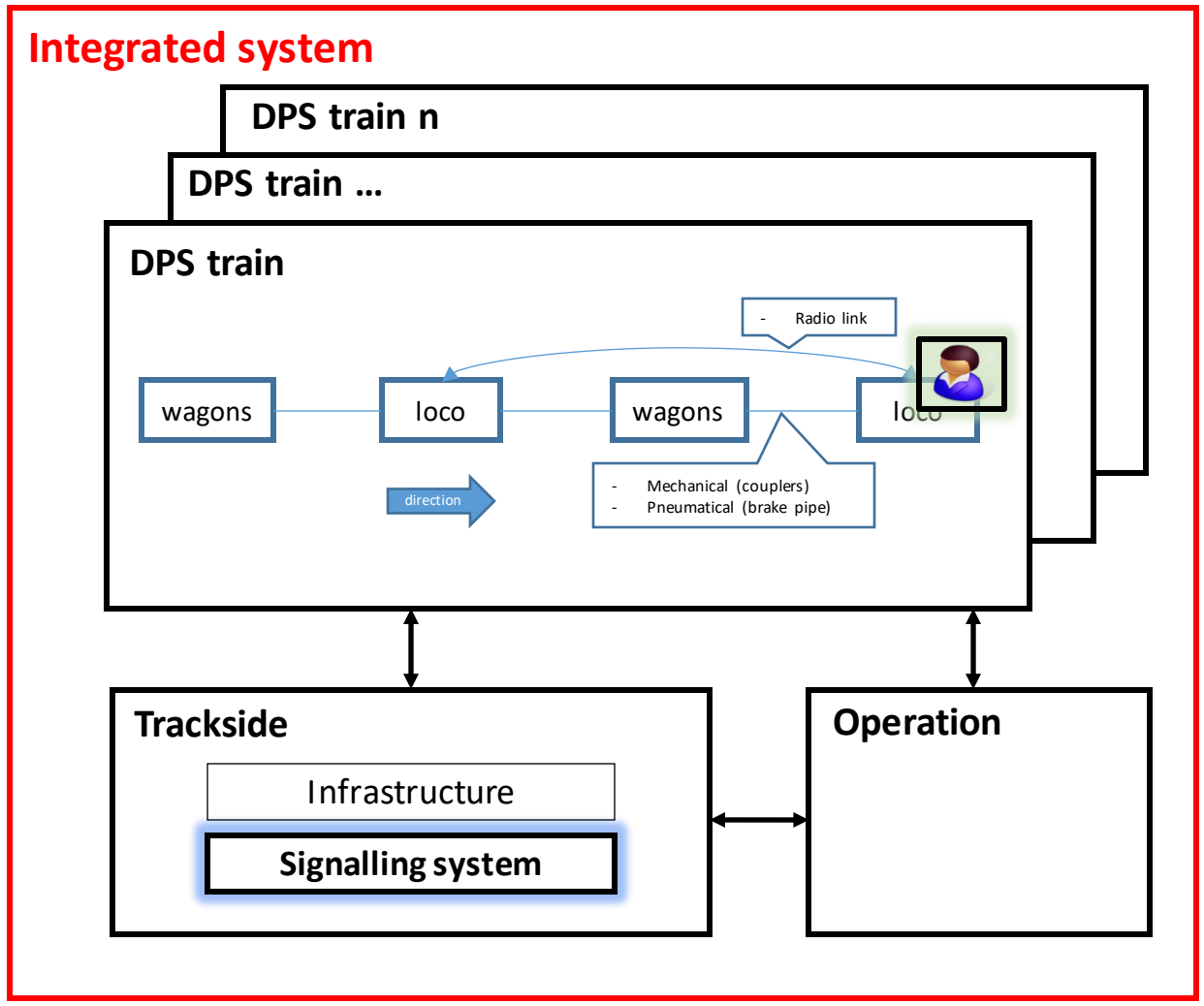
INFRASTRUCTURE

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

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

GENERAL CONTEXT FOR SAFETY ANALYSIS



SIGNALLING SYSTEM

2.1 - Interlocking (central logic)	-
2.2 - Automatic Train Protection (Trackside)	-
2.3 - Trains routing and traffic regulation	-
2.4 - Field Signalling 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

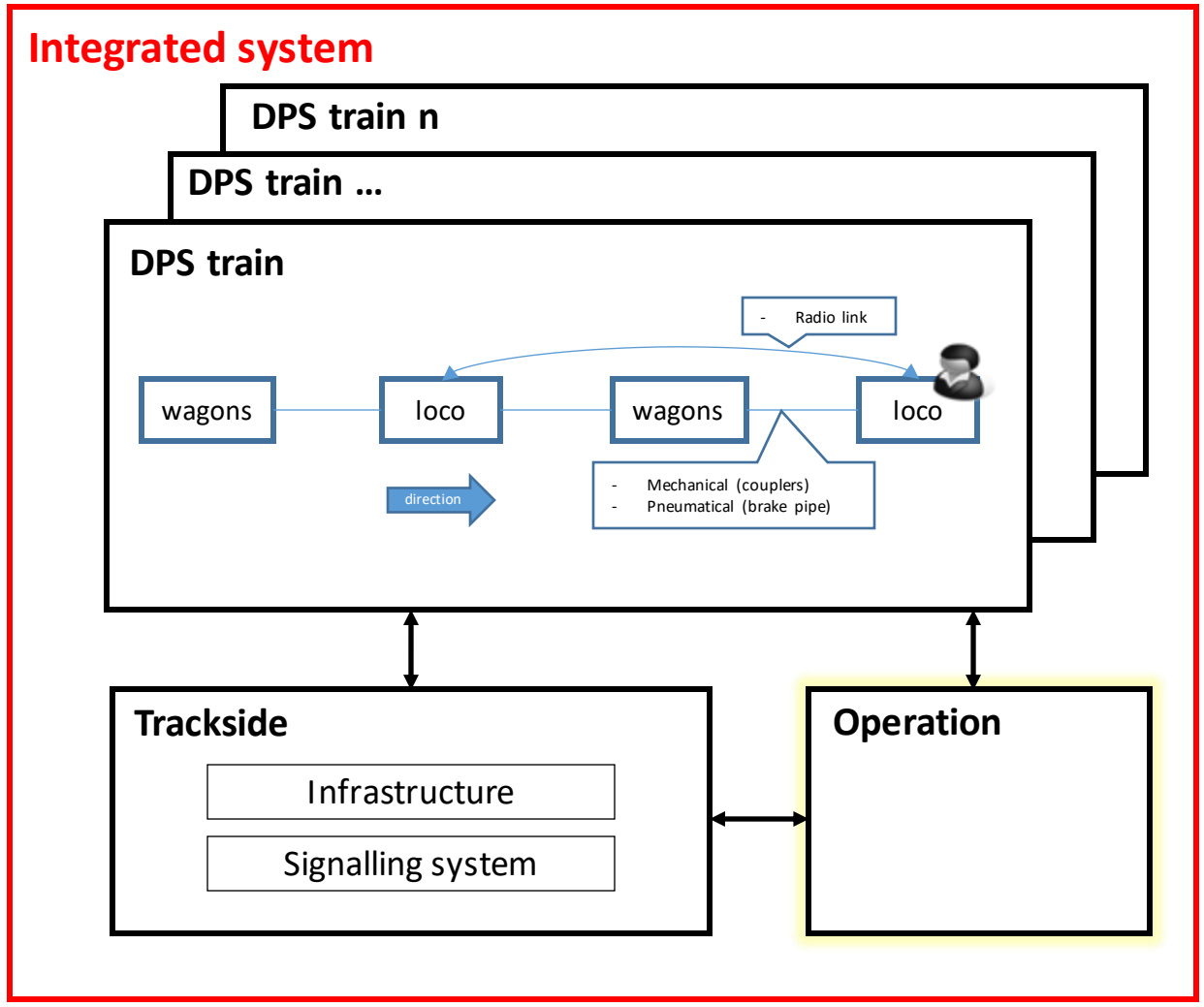
marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

GENERAL CONTEXT FOR SAFETY ANALYSIS



OPERATION

4.1 - Loading of wagons	4.1.1 - Load distribution
	4.1.2 - Load fastening
4.2 - Train checks	-
4.3 - Field equipment operation	4.3.1 - Switch point operation
	4.3.2 - Level crossing operation
4.4 - Train manoeuvre	-
4.5 - Management of off-normal conditions	-
4.6 – System's elements (Traction units, wagons) coupling and decoupling	-

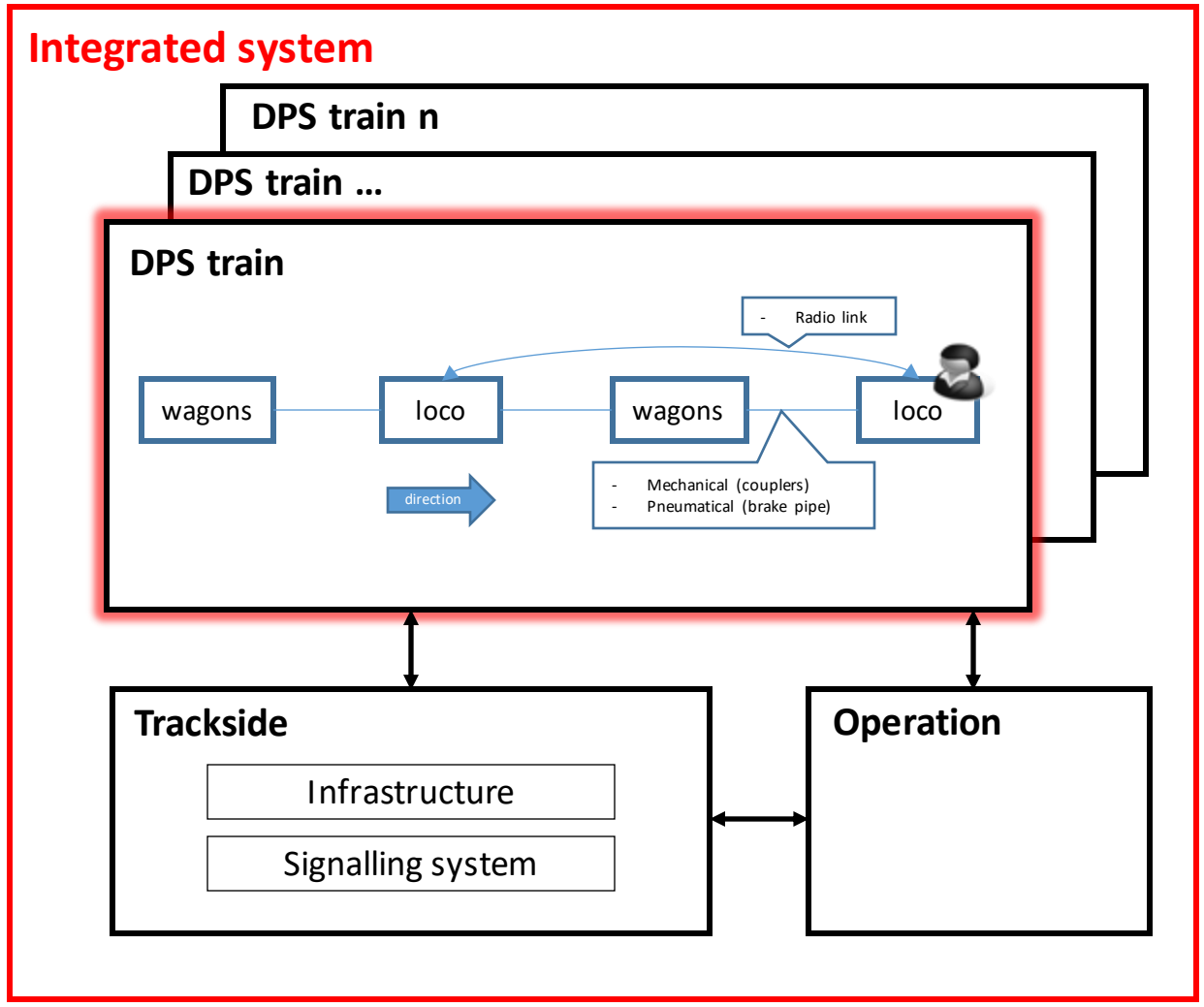
marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

GENERAL CONTEXT FOR SAFETY ANALYSIS



DPS TRAIN

3.1 - Running gear	3.3.1 - Wheelsets integrity
	3.3.2 - Suspension integrity
	3.3.3 - Bogie structure integrity
3.2 - Wagon	3.4.1 - Load carrying units integrity
	3.4.2 - Frame integrity
3.3 - Coupling system	-
3.4 - Energy supply system & Pantograph	-
3.5 - Automatic Train Protection (Trainboard)	-
3.6 - Driver interface	-
3.7 - Train Control & Management System	-
3.8 - Braking and traction equipment	-
3.9 - Distributed Power System (including Radio equipment)	-

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

FUNCTIONAL MODEL OF DPS TRAINS

Phase	Main function	Description
Train set-up	**Train composition**	Forming the train according to the established composition, by coupling wagons and traction units.
	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.
	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.
	Train operational status management	Management of the operational status of DPS train
	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
	Traction management	Management of traction according to set point (including traction cut-off as required).
	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.
	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.
	Parking Brake management	Application of braking force ensuring the permanent immobilization of the train.
	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.
	Air management	Management of the main air reservoir (use of compressor)
	Automatic Train Protection management	Management of the status of ATP System (active / sleeping mode) on (leading / guided) Traction units.
	Diagnostic	Management of alarms related to operational relevant failures and disturbances and incidental scenario (i.e. fire).
	System de-activation	Management of system de-activation and the related communication between the Traction units about the status of train.

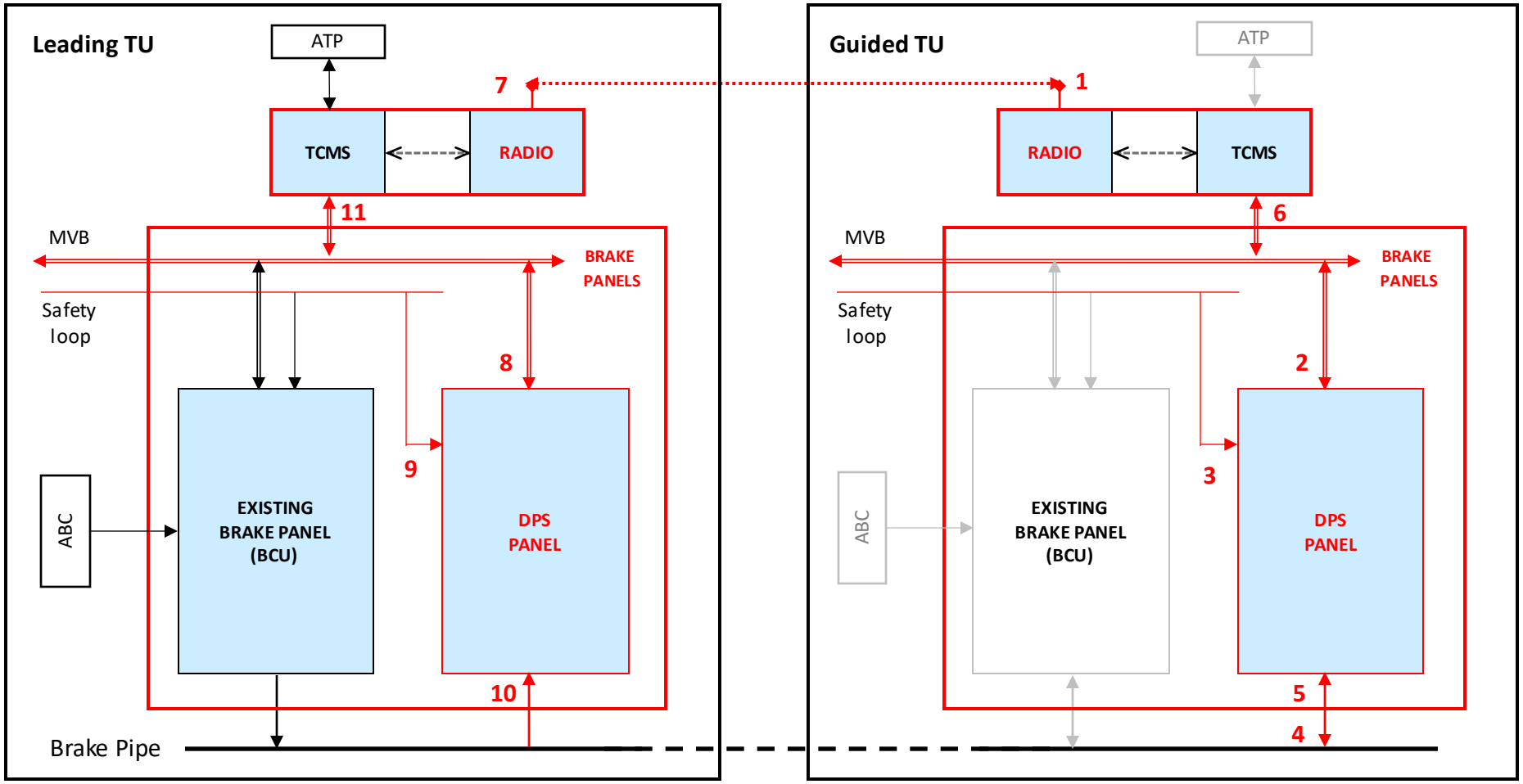
marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

DPS TRAINS ARCHITECTURE AND INTERNAL INTERFACES



New Radio equipment (RCDPS and LTE-antenna for each Traction unit) interfaced to **TCMS (adapted for DPS)**

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

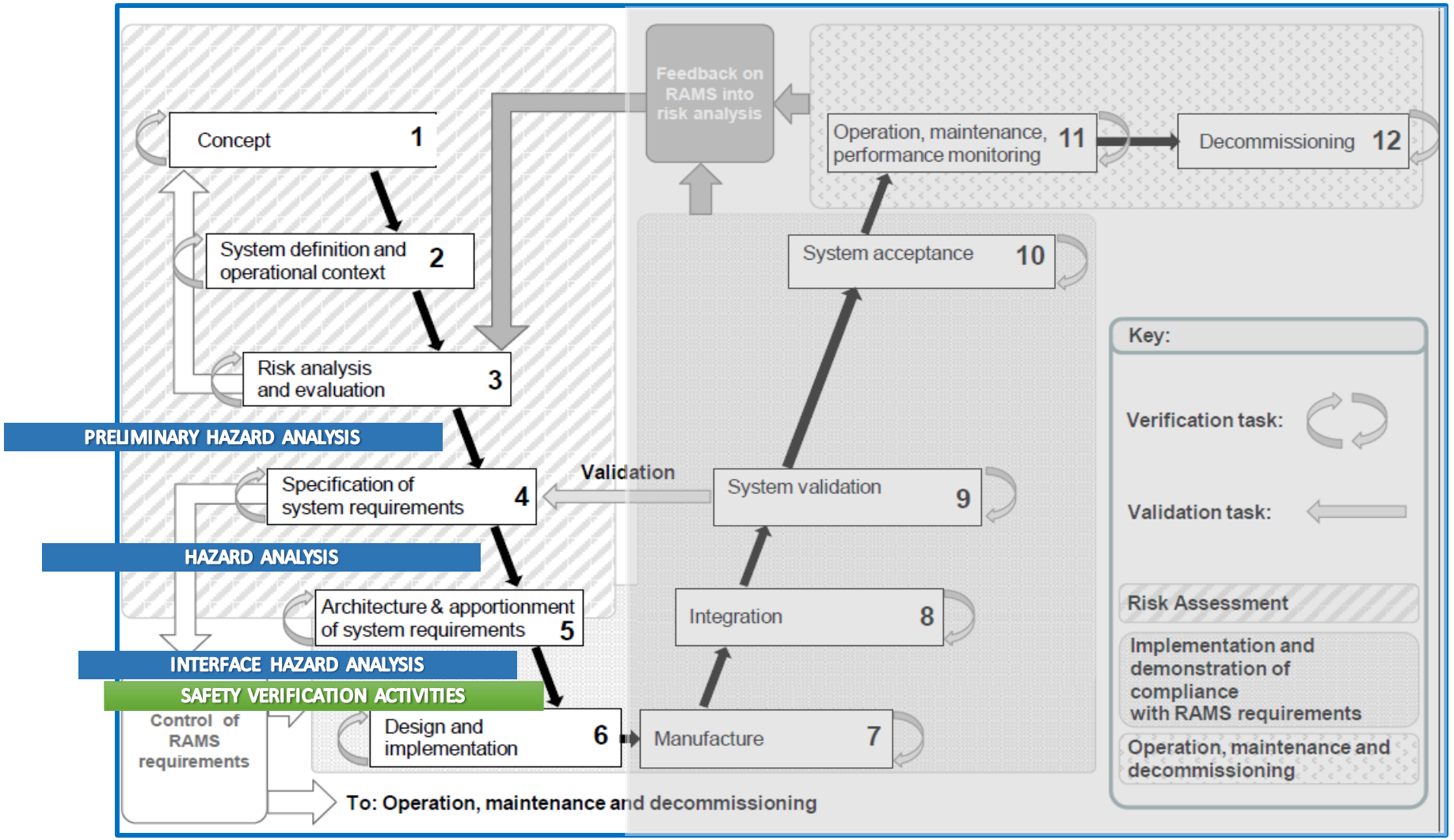
Brake panels of the leading Traction unit, including the existing panel operating on BP and the new DPS panel, monitoring the pressure in BP and the status of the safety loop and communicating with the guided Traction Units

Brake panels of the guided Traction unit including the new DPS panel operating on BP, communicating with the leading TU and monitoring the Brake pipe pressure

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SYSTEM LIFECYCLE AND SAFETY ACTIVITIES



PRELIMINARY HAZARD ANALYSIS (PHA)

Object:

Integrated railway system

Objectives:

- to identify the hazardous conditions related to the operation of DPS trains
- to identify the elements/factors of the system that could lead to the occurrence of hazardous conditions, because of one or more specific characteristics of long freight trains
- to specify mitigations to be implemented by DPS train and in the setting of the operational context.

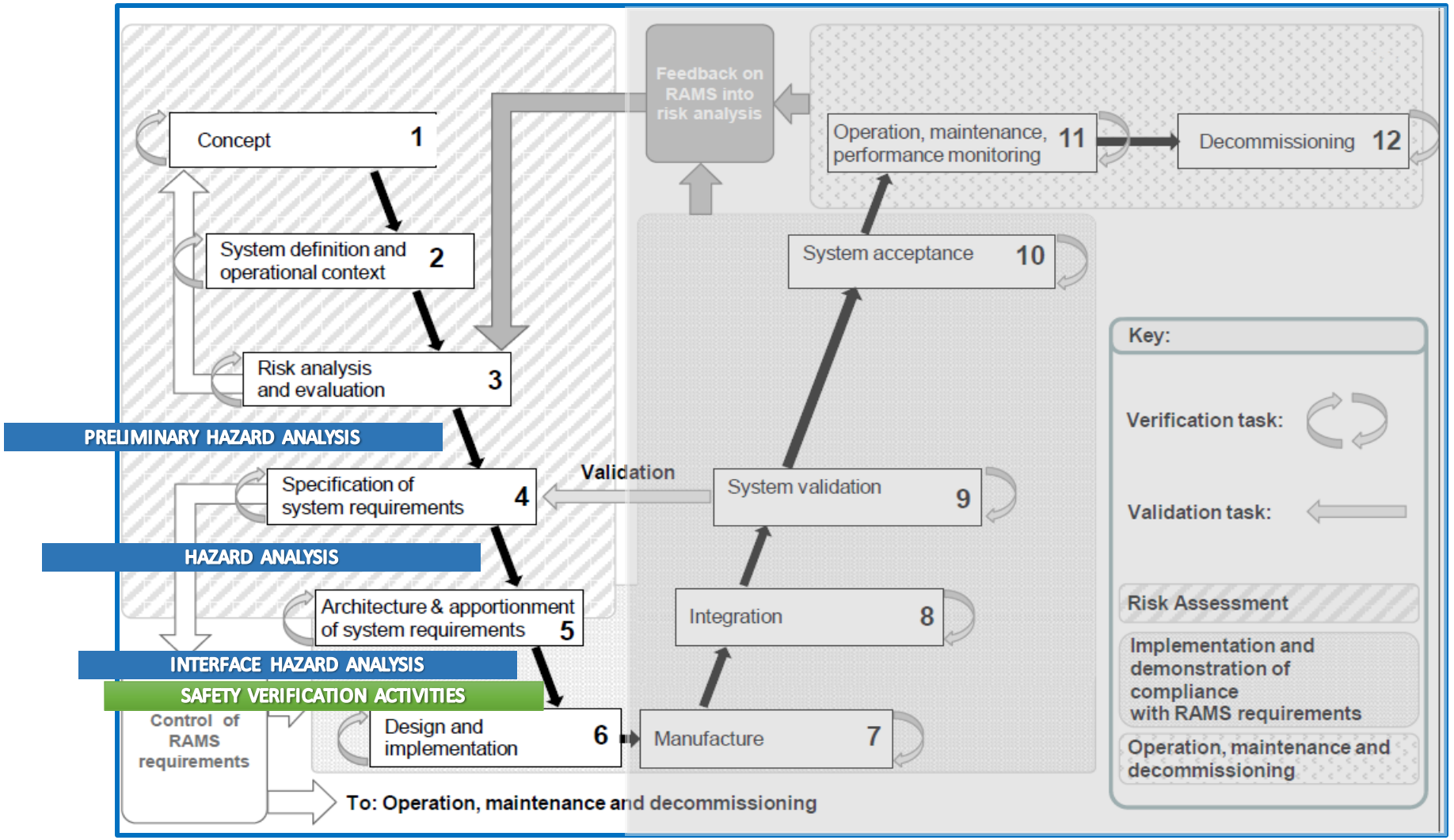
marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

SYSTEM LIFECYCLE AND SAFETY ACTIVITIES



HAZARD ANALYSIS (HA)

Object:

DPS train (function)

Objectives:

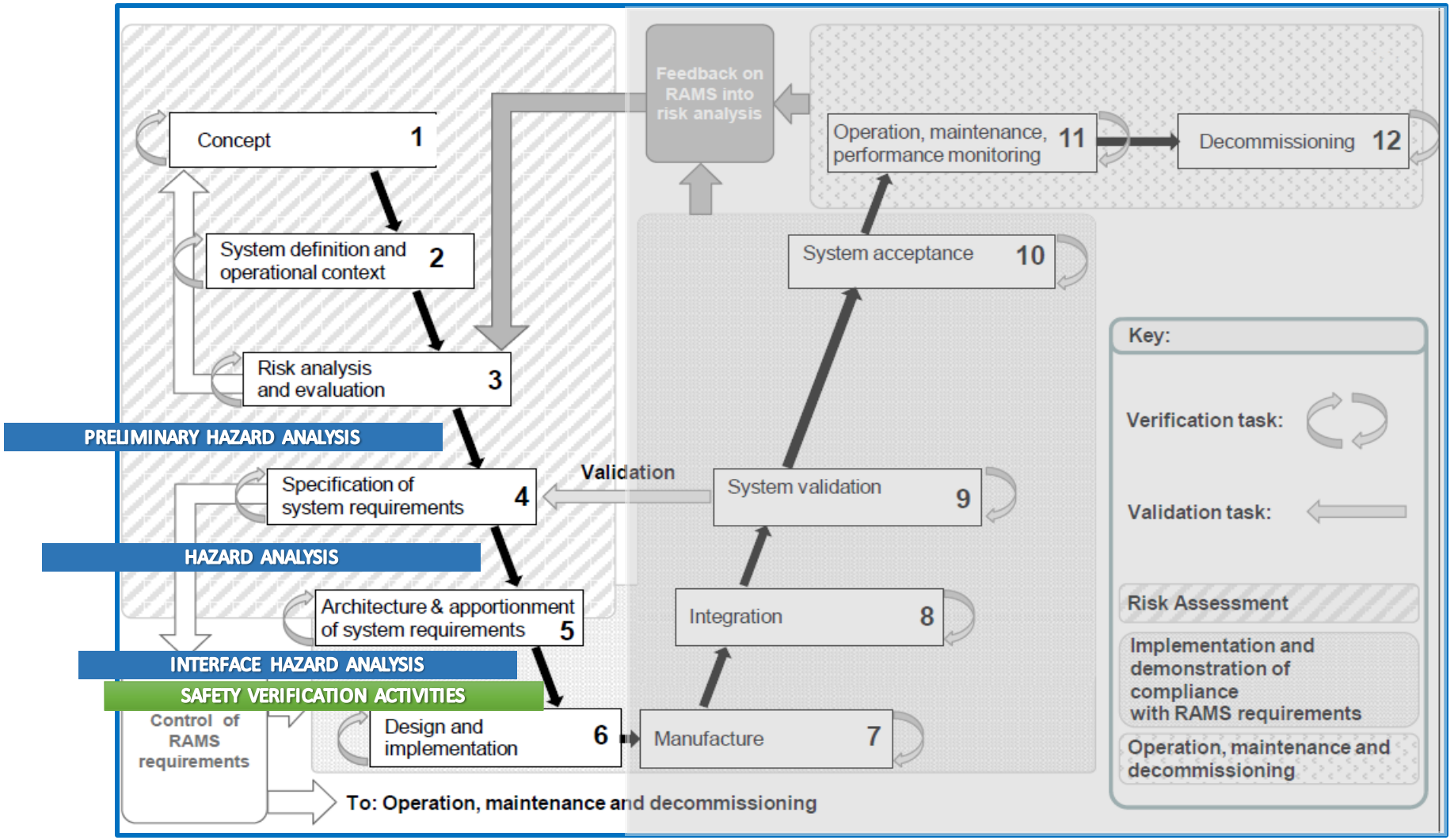
- to identify further hazards
- to specify further mitigations

through the <u>analysis of the potential deviations from the expected behaviour</u> in the execution of the “specific” functions

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SYSTEM LIFECYCLE AND SAFETY ACTIVITIES



INTERFACE HAZARD ANALYSIS (HA)

Object:

DPS train (internal interfaces)

Objectives:

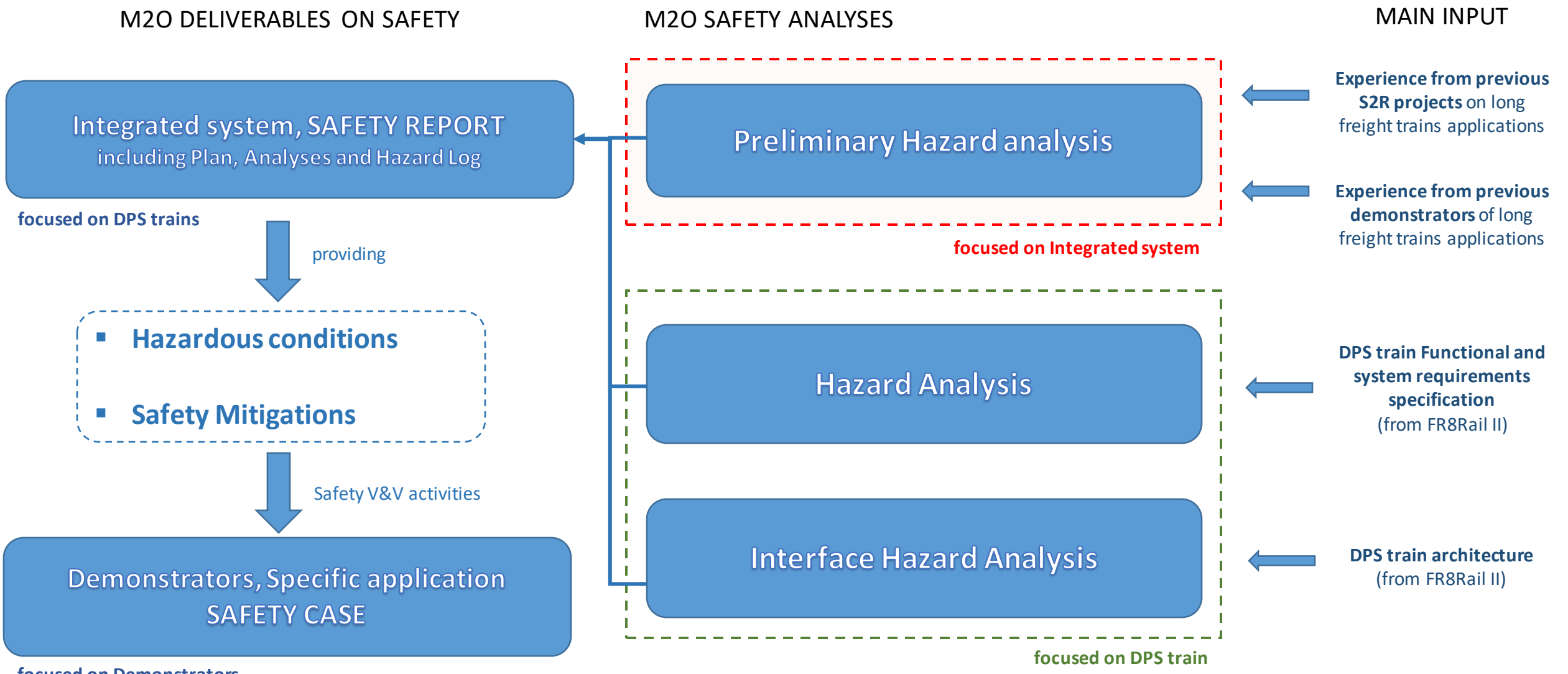
- to identify further hazards
- to specify further mitigations

through the analysis of the potential deviations in the data and signals exchanged between DPS train subsystems (i.e. thought its internal interfaces

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SYSTEM LIFECYCLE AND SAFETY ACTIVITIES



MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

HAZARDOUS CONDITIONS RELATED TO DPS TRAIN OPERATION

(Macro and Specific) Hazard	
H_1	**Impaired (or lost) train running stability**
H_1_1	Increase of vehicle axle load
H_1_2	Long bridges with excessive cross winds
H_1_3	Long bridges with hazardous dynamic behaviour (i.e. natural frequencies coupled with vibrations induced by trains)
H_1_4	Excessive overall mass of DPS train brake with respect to the infrastructure
H_1_5	Excessive longitudinal forces transmitted to the infrastructure due to the brake application by DPS train.
H_2	**Interference between train and loading gauge due to changes in train shape**
H_3	**Impaired (or lost) coupling between train units**
H_3_1	Loss of integrity of coupling between units (Traction units or wagons)
H_3_2	Excessive stretch length after stopping of the train due to distributed traction/braking
H_4	**Excessive longitudinal forces between train units**
H_4_1	Excessive in-train longitudinal forces due to the distributed traction and braking performance
H_4_2	Excessive in-train longitudinal forces due to specific track characteristics
H_4_3	Excessive in-train longitudinal forces due to specific maneuver
H_4_4	Excessive in-train longitudinal forces due to specific distribution of loads over wagons
H_5	**Excessive train braking distances or speed**
H_5_1	Excessive train braking distances or speed due to an impaired (or lost) braking capability
H_5_2	Excessive train braking distances or speed due to an excessive timing of reaction for braking application
H_5_3	Excessive train braking distances or speed due to distributed traction and braking performance
H_5_4	Excessive train speed due to an undue release of brakes
H_5_5	Temporary speed restriction not fulfilled with the whole length of the train
H_5_6	Missed / ineffective reduction of the train speed by the driver (acting on traction and brake).
H_6	**Undue train braking or train unduly immobilized**
H_7	**Undue train movement**
H_7_1	Undue train movement due to a failure / undue release of parking or holding brake
H_7_2	Undue train movement due to a shunting operation made by the driver
H_7_3	Undue train movement in an area where shunting is not allowed

They include:

- **specific hazards** (i.e. strictly related to the DPS trains characteristics)
- **"conventional" hazards** (i.e. generally applicable to freight trains) having a potential increase of risk because of one or more characteristics of DPS trains.

The remaining conventional hazards are assumed to be properly mitigated by the existing technological and procedural provisions.

Marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

HAZARDOUS CONDITIONS RELATED TO DPS TRAIN OPERATION

(Macro and Specific) Hazard	
H_8	**Damage to 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)
H_8_2	Damage to overhead contact line (catenary) and/or trainborne power supply equipment due to an incorrect management of power supply equipment (i.e. opening and closing of the main circuit breakers and/or lowering and arising of pantograph(s))
H_9	**Incorrect detection of track occupancy/clearance**
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
H_9_2	Incorrect detection of track occupancy/clearance due to a too high number of axles of a single train to be counted (by axle-counter, if applicable)
H_10	**Hazardous operation of train/maintenance staff**
H_10_1	Incorrect (unsafe) train composition or configuration due to staff error
H_10_2	Intendent change of train configuration data by staff during operation
H_10_3	Unsafe maneuver of the train, due to a wrong orientation
H_10_4	Unsafe maneuver of the driver, which does not remember the received prescriptions after a long train stop or after driver change
H_10_5	Unsafe management of train equipment in the crossing of neutral section due to staff error
H_10_6	Improper use of compressor to restore the minimum pressure in the main air reservoir
H_10_7	Unsafe condition of the train after end-of mission due to staff error
H_11	**Interference with track-side equipment**
H_11_1	The distance between a main signal and a critical points (e.g. switch point, level crossing, hotbox-detector, balises providing protective messages is too short to host the train.
H_11_2	A main signal stop the train with the pantograph of the guided Traction units under a neutral section of the catenary (preventing contribution to traction)
H_11_3	The braking distance is too long to stop the train at the first main signal after a Hotbox-detector.
H_11_4	New switch points (e.g. introduced to allow shunting movement and stop of DPS train) are not taken into account by the interlocking central logic
H_11_5	Level crossing unduly switched on before the full passage of the end of the train
H_11_6	Switch point unduly maneuvered or released or before the full passage of the end of the train.
H_12	**Train misrouted on a wrong (non-adequate) line**
H_13	**Ineffective DPS train initial tests**
H_13_1	Missed or incomplete execution of DPS train initial tests
H_13_2	Incorrect execution of DPS train initial tests
H_14	**Other hazardous conditions on train**
H_14_1	Fire on-board during train run
H_14_2	Operational relevant failures and disturbances during train run

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

HAZARDOUS CONDITIONS RELATED TO DPS TRAIN OPERATION

HAZARDOUS CONDITION	
…	… … … …

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

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)

The hazardous conditions identified during the safety analyses have the **potential to produce fatalities and/or multiple severe injuries and/or major damage to the environment and/or major damages to main systems** (i.e. catastrophic consequences according to EN 50126)

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SAFETY INTEGRITY LEVELS ALLOCATION

Two Safety Integrity levels are adopted:

EN 50129	Safety Integrity Levels
Basic integrity	Basic integrity
SIL1	Low Safety Integrity
SIL2	
SIL3	High Safety Integrity
SIL4	

Two mitigation strategies are adopted to achieve an acceptable a risk levels:

- ❑ **"high safety integrity"**

is required to the functions that could lead to hazardous conditions, guarantying a frequency of occurrence of hazardous failures less than 10^{-8} event/h (limit stated for SIL4 function by the EN 50129)

- ❑ **"low safety integrity"**

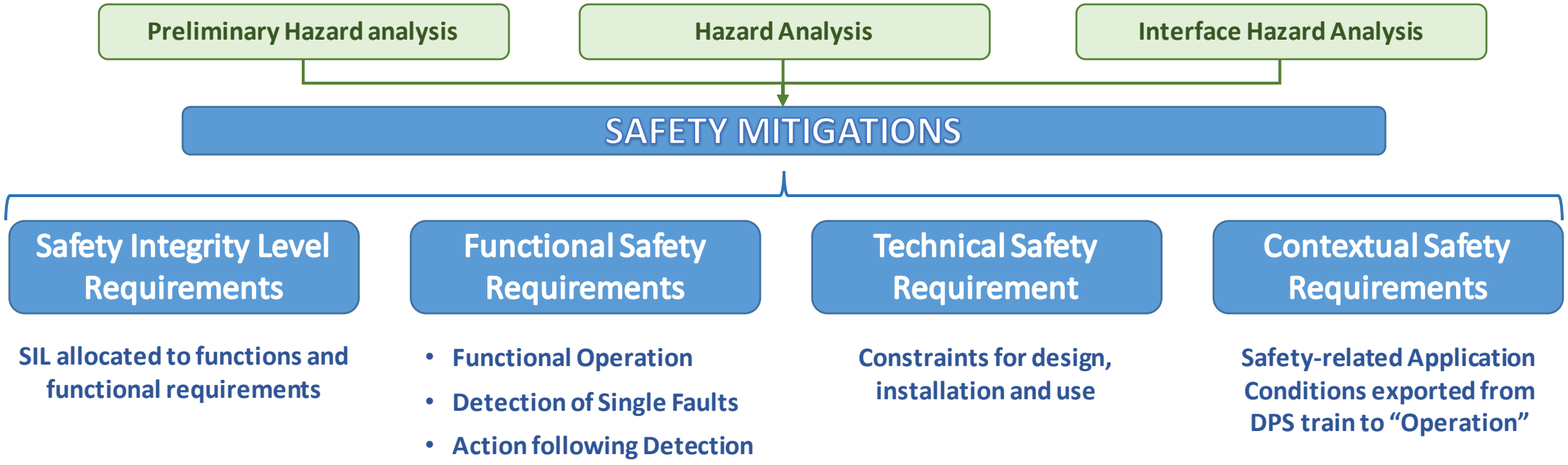
is required to the functions that could lead to hazardous conditions, guarantying a frequency of occurrence of hazardous failures less than 10^{-6} event/h (limit stated for SIL2 function by the EN 50129), with additional operational mitigations that should be

- effective (able to avoid the event and to put and maintain the system into a safe state)
- and reliable (probability of failure/error < 10^{-2}, to achieve acceptable frequency of occurrence for catastrophic consequences)

SAFETY REQUIREMENTS SPECIFICATION

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION



The mitigations specified during safety analyses are classified through different categories, as defined in EN 50126 (Part2)

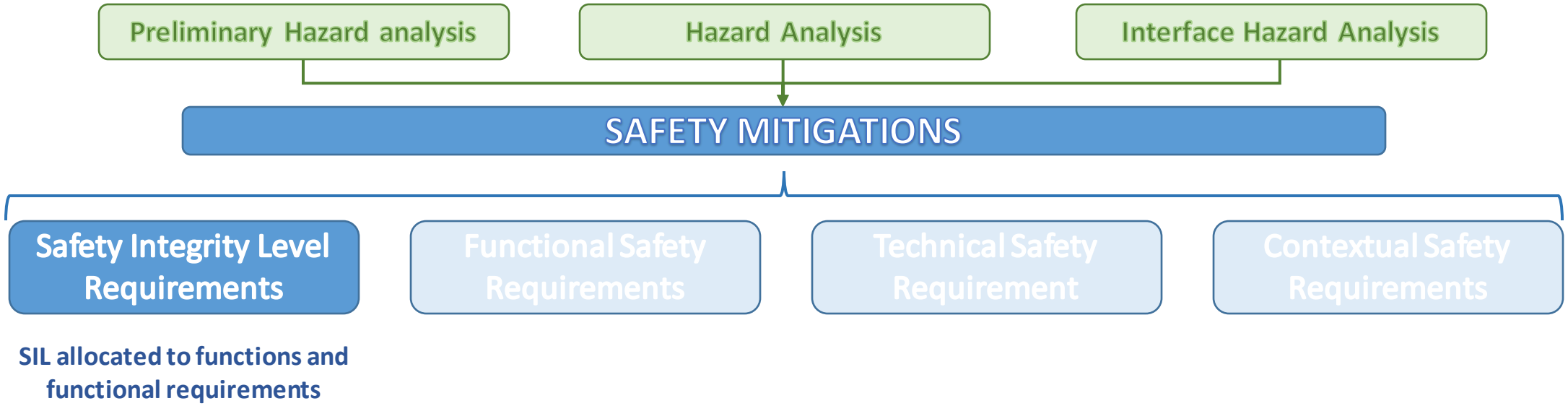
MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SAFETY REQUIREMENTS SPECIFICATION

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION



SIL allocated to functions and functional requirements

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

SAFETY REQUIREMENTS SPECIFICATION, SIL REQUIREMENTS

Main function	(Worst) Hazardous scenario	SIL	Further mitigations
Train composition	Inconsistency between the train physical composition and configuration data, leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**No safety instrumented function**	PHA_MIT_22 HA_MIT_03
Communication set-up	Incomplete exchange of data between DPS train locomotives and use of potential unsafe configuration data, leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Basic integrity level**	HA_MIT_03 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**	PHA_MIT_25 HA_MIT_03 HA_MIT_08
Train operational status management	Missed or undue remote controls from the leading locomotive to the guided one(s), leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety integrity level**	PHA_MIT_25 HA_MIT_08
Train initial test	Latent failure and/or incorrect configuration data remain non detected, leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety integrity level**	PHA_MIT_23 PHA_MIT_32 HA_MIT_42
Communication between Traction units	Missed or incorrect exchange of remote controls between the DPS train locomotives ,leading to an hazardous management of distributed traction and brake with missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety integrity level**	HA_MIT_30 HA_MIT_31 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 dynamic brake and/or excessive in -train longitudinal forces (and potential DPS train separation and/or derailment).	**Low Safety integrity level**	PHA_MIT_28 PHA_MIT_29 HA_MIT_08 HA_MIT_19
Service brake management	Ineffective pneumatic brake with potential exceeding of space and/or speed limits (and potential collision of DPS train with other trains, infrastructure or obstacle and/or derailment) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety integrity level**	HA_MIT_27
Emergency brake management	Missed stop of DPS train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**High Safety Integrity level**	PHA_MIT_30
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**	PHA_MIT_32
Energy management	Potential damage to the infrastructure (catenary overhead) and/or to the DPS train (on-board power supply system).	**Low Safety integrity level**	PHA_MIT_31
Air management	Ineffective pneumatic brake and missed stop of DPS train within the maximum allowable braking distance (and potential collision with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety integrity level**	PHA_MIT_30 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**	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**	PHA_MIT_33 HA_MIT_06 HA_MIT_08
System de-activation	Undue deactivation of DPS equipment, leading to an hazardous management of distributed traction and brake with missed stop of the train within the maximum allowable braking distance (and potential collision of DPS train with other trains, infrastructure or obstacle) and/or excessive in-train longitudinal forces (and potential train separation and/or derailment).	**Low Safety Integrity level**	HA_MIT_45

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

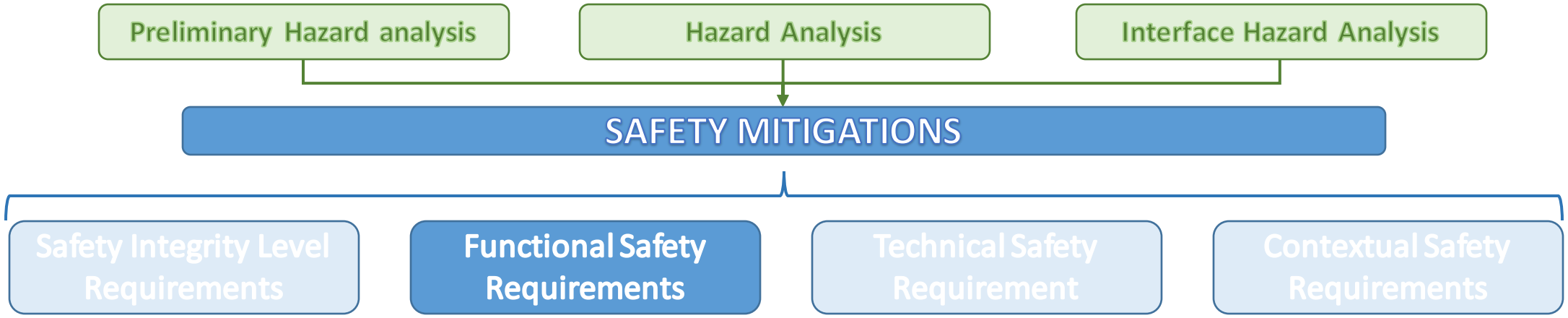
Grant Agreement Number **826087**

Shift2Rail

SAFETY REQUIREMENTS SPECIFICATION, FUNCTIONAL SAFETY REQUIREMENTS

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION



- Functional operation
- Detection of single faults
- Action following detection

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

E.g. EMERGENCY BRAKING

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

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

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

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

E.g. DETECTION OF RADIO COMMUNICATION LOSS

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

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

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

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

SAFETY REQUIREMENTS SPECIFICATION, FUNCTIONAL SAFETY REQUIREMENTS

E.g. REACTIONS TO LOSS OF RADIO COMMUNICATION AND BRAKE PIPE PRESSURE DECREASE

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

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

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

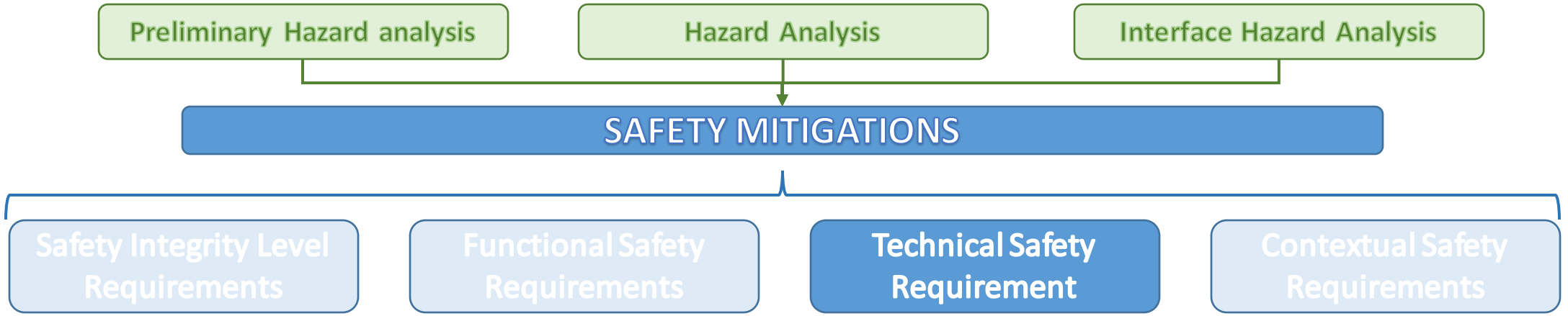
Each Traction unit of DPS Train shall cut off the traction if the brake pipe pressure is below a defined limit*, independently from the status of the radio connection and received information, with a defined ramp down. (HA_MIT_19)*

The (leading and guided) Traction units of DPS train, in case of reduction of the brake pipe pressure, shall cut off the traction with a defined ramp down and vent or assist the venting of the brake pipe *(by a defined mechanisms), independently from the radio communication status, guarantying the brake automaticity extended on the whole length of DPS train. The pressure decrease triggering the reaction and the type of reaction shall be defined guarantying the fulfilment of the limits stated for in-train longitudinal forces and braking distance. Residual risk concerns the collision of the two separated train parts in case of train separation (as for conventional train. (HA_MIT_30 and HA_MIT_31 , High SIL)*

SAFETY REQUIREMENTS SPECIFICATION, TECHNICAL SAFETY REQUIREMENT

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION



Compatibility between DPS train with track

- train length, mass, axle load, number of axles
- possibility to misrouting
- position of signals, swicth points
- area for shunting movement,
- area for coupling/decoupling of vehicles
- trackside logic (switch point, level crossing operation)
- neutral section

Safety-related Application Conditions exported to DPS train

- by Signaling systems (IXL, ATP)
- by Train detection system

LTD studies (LCF, LTF, braking distance)

- train consists configuration
- train maneuvers
- degraded operational modes

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Mitigations concerning longitudinal train dynamic

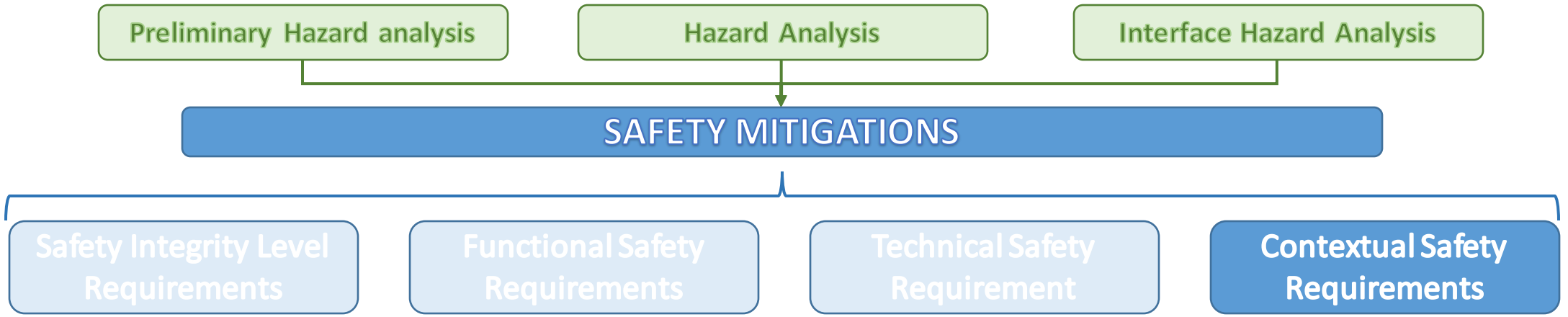
ID	Description	Validation
PHA_MIT_15	For each class of specific applications, it shall be verified that **the in-train longitudinal forces in DPS train are acceptable** (compared to absolute limits or to a reference train configuration already authorized for operation) **in all the conditions defined by the train configuration** (position of Traction units and loaded wagons), **credible degraded operating modes** (interruption of radio communication), **train manoeuvres** (traction, brake, particular operations), and **track characteristics** (e.g. maximum track gradient). Unsafe Train configurations (i.e. distribution of loaded wagons) shall be identified (if any) by simulations of in-train longitudinal forces and braking distance of DPS trains.	LTD simulations are performed on family of trains having length between 720 and 740 m (TU included) and hauled mass between 1800 and 1850 ton (generated according to UIC Leaflet 421) and on the specific configuration defined for Demonstrators. The relative approach envisaged by UIC Leaflet 421 is followed. Longitudinal Compressive Forces (LCF) and Longitudinal Tensile Forces (LTF) are evaluated under different train manoeuvres, at different track positions (including ones with the maximum gradient) for DPS and for Reference trains (families) and then compared. LTD simulations are mainly focused on in-train longitudinal forces. Additional studies have been performed, confirming that the stopping distance of DPS train at high speed is always less than for the Reference trains.
PHA_MIT_17	For each class of specific applications, the **time required for EB application** in DPS train, both triggered by radio communication and by the change of brake pipe pressure, accounting for nominal performance and uncertainty, shall be estimated for DPS train and compared with limits considered / coming from simulations of (in-train longitudinal forces and) braking distance of DPS trains.	A model of the processing and transmission of data on the traction vehicles and between cars has been developed for latency calculation. Time required for EB application (and thus brake distances) is no longer than ones of the Reference system (which operates on the test track fulfilling all brake distance requirements). LTD simulations are performed with consistent assumption on LTE latency time
PHA_MIT_18	For each class of specific applications, **if the effective brake (sum of dynamic and pneumatic braking contributions) could decrease** in case of loss of the radio communication between the Traction units of DPS train, simulations shall demonstrate that (because of potential train acceleration) braking distance degradation and in-train longitudinal forces are still acceptable. The contribution of dynamic brake shall not be considered for the fulfilment of braking distance (if/as applicable).	LTD simulations are performed considering ED removal when the train is in a slope section under degraded operation condition due to the loss of radio communication between TUs.
PHA_MIT_19	For each class of specific applications, the maximum traction effort and dynamic braking forces shall be specified for each Traction unit, for each DPS train configuration. The **acceptability of in-train longitudinal forces in case of different traction levels applied in different Traction units** shall be verified by simulations of in-train longitudinal forces and braking distance.	Longitudinal forces experienced by Demonstrators, with their limits of traction force, are assessed (and verified against the Reference system) by LTD simulations. LTD simulations are performed by applying the maximum braking force by all wagons and the maximum traction forces force is applied by all TUs. If the traction or braking forces are lower than their maximum values, the LTD is less enhanced. Specific study is performed for train-consist LWLWL, assuming different traction forces applied by TUs.

Evidences are on M2O deliverables on LTD (D2.1 and D3.1 on general DPS Train simulations, D3.3 on and D3.2 on DPS Train Demonstrators)

SAFETY REQUIREMENTS SPECIFICATION, CONTEXTUAL SAFETY REQUIREMENT

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION



Existing procedures on

- coupling and decoupling of vehicles
- departure of DPS train on slope
- loading gauge
- shunting movement
- air in the main reservoirs

Specific procedures on

- dangerous goods on board
- handling of the parking brake
- limits of traction and/or dynamic brake
- train inauguration and initial test
- train orientation
- reaction to alarms
- management of pantographs
- isolation of traction units in standstill
- train run without radio communication
- train run with DPS switch-off

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

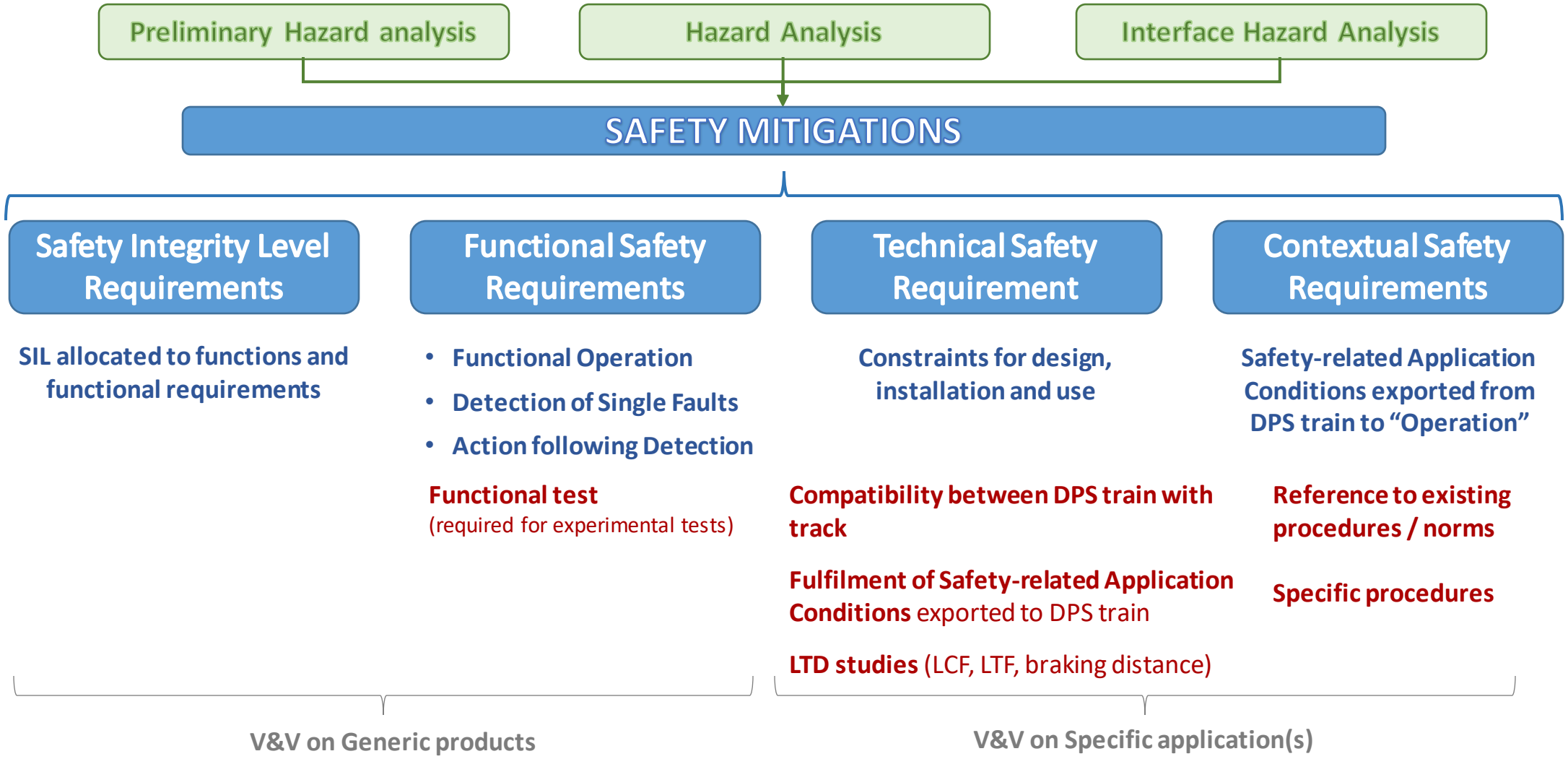
SAFETY REQUIREMENTS SPECIFICATION AND VERIFICATION

SAFETY ANALYSIS

REQUIREMENT SPECIFICATION

REQUIREMENT VERIFICATION FOR TESTS

ACTIVITIES FOR FUTURE CERTIFICATION



MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

EXPERIMENTAL TEST CAMPAIGN, MAIN CHARACTERISTICS RELEVANT WITH SAFETY

The test track has a **maximum slopes** of 27‰ (impacting on in-train longitudinal forces)

DPS Test train will include **Traction units approved** (BR 187) **or under approval** (BR 188) retrofitted with DPS and vehicles (Eanos 59, Res 677, Facns 124 and Facns 133 types) approved freight wagons

DPS Test train **length, mass, number of axles and axle load will not exceed the allowable limits** for the test track

DPS Test train experiences **longitudinal forces not higher than for Reference system** (i.e. trains already admitted to the traffic on the track selected for the tests (results from LTD simulations).

EXPERIMENTAL TEST CAMPAIGN, COMMUNICATION BETWEEN TRACTION UNITS

TECHNOLOGY-NEUTRAL TECHNICAL REQUIREMENTS

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

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

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

IMPLEMENTATION

The communication between TUs is based on the **Safe Data Transmission version 2 (SDTv2) safety layer**, supporting safety functions up to SIL2

The **security provisions** implemented for LTE radio communication used for test runs (limited in space and time) include

- the use of special credentials for each mobile to access the private APN
- the absence of direct communication between mobiles and with fixed entities (except the VPN tunnel with the Control Center)
- the monitoring of sessions and data traffic in the Control Center

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

EXPERIMENTAL TEST CAMPAIGN, SAFETY VERIFICATION AND VALIDATION ACTIVITIES

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

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

CONCLUSION, GENERAL

Safety analyses have been performed on DPS trains within an Integrated railway system, providing:

- a set of **hazardous conditions** related to the DPS trains operation
- a set of **functional safety requirements** to be implemented by DPS trains
- a set of **requirements for LTD simulations** development
- a set of **safety-related application conditions** exported to the remaining elements of the system

Results coming from the safety analyses developed during the M2O project is provided in a **SAFETY REPORT**, as **basis for the safety demonstration of "specific applications" DPS trains** (specific train/train family and tracks where the running authorization applies), including the next experimental test campaign (February 2021)

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

CONCLUSION, EXPERIMENTAL TEST CAMPAIGN

Verification and Validation activities have been defined to provide evidence of the implementation of each safety mitigation, including

- ❑ **LTD simulations performed under M2O project**, focusing on the DPS train Demonstrators, consistently with safety analysis
- ❑ **further evidences to be gathered by FR8RAIL II project**, concerning
  - Compatibility between DPS train with track
  - Instruction to staff / driver (covering SRAC exported to Operation)
  - Traceability between safety mitigations and functional requirements / tests
  - Report of functional tests
  - Report of LTE-Antennae interference

Safety relevant information produced and collected during the M2O project is provided by a structure of content compliant with a **SPECIFIC APPLICATION (SA) SAFETY CASE**, as defined by EN 50129

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

CONCLUSION, EXPERIMENTAL TEST CAMPAIGN

As intrinsic limitation:

- ❑ No formal Verification & Validation process has been performed (nor planned) for (DPS) developments and integration
- ❑ No reference to Generic Product Safety case for (DPS revamped) Traction unit and/or its systems is available

Additional Safety-related Application conditions are specified for the safe execution of the experimental tests campaign:

- ❑ Each guided Traction Unit (TU) shall be manned; the personnel attending the guided TU shall have an independent way of communication with the driver (at the leading TU)
- ❑ **If** responsibility on brake application is defined (currently under confirmation by LTD studies), the personnel shall be aware of the execution of tests (including planning, modality, expected behaviour), intervention criteria and required reactions

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail

Thanks for your attention!

NIER

Stefano La Rovere

www.nier.it

s.larovere@nier.it

marathon 2 operation

MAke RAil The HOpe for protecting Nature 2 future OPERATION

Grant Agreement Number **826087**

Shift2Rail