D3.1: Hazard identification and risk assessment

Project acronym:	Maglev-Derived Systems for Rail
Starting date:	01-07-2023
Duration (in months):	12
Call (part) identifier:	HORIZON-ER-JU-2022-02
Grant agreement no:	101121851
Due date of deliverable:	Month 11
Actual submission date:	31-05-2024
Responsible/Author:	Marco Antognoli (DITS)
Dissemination level:	PU
Status:	Issued

Reviewed: no

This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No. 101121851.

Document history		
Revision	*Date*	*Description*
0.1	12-02-2024	First draft
0.2	10-05-2024	Second draft
1	31-05-2024	First Issue

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Simon Collart-Dutilleul	Uni Eiffel	Coordination, contribution in hazard identification, contribution in risk assessment and review of the deliverable
Marco Antognoli	DITS	Coordination in deliverable preparation, contribution in hazard identification, coordination and contribution in risk assessment
Gerardo Fasano	GESTE	Contribution to methodology, hazard identification, risk assessment and preparation of deliverable
Paweł Radziszewski	Nevomo	Contribution in hazard identification, risk assessment and in deliverable preparation
Jesus Felez Gregorio Romero Jose A. Lozano	UPM	Contribution in hazard identification, risk assessment
Vincenzo Leoncavallo	Italferr	Contribution to methodology and review of deliverable
Giuseppe Carcasi Angela Nocita Giovanni De Blasio Camilo Patino Puerta	RFI	Review of the deliverable
Francesca C. Antonacci	FSI	Review of the deliverable

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

The content of this report does not reflect the official opinion of the Europe's Rail Joint Undertaking (EU-Rail JU). Responsibility for the information and views expressed in the Deliverable lies entirely with the author(s).

Table of Contents

List of Figures

List of Tables

1 Executive Summary

Deliverable D3.1 illustrates the risk analysis conducted on the hybrid Maglev Derived Systems (MDS) within the scope of the MaDe4Rail project.

According to deliverable D2.1 of the MaDe4Rail project (Ref. [7]), three categories of MDS have been identified: Pure maglev systems, Hybrid MDS (defined as MDS deployed on existing railway infrastructure with full interoperability and integration) and Hyperloop systems. Among them, the risk analysis focuses on hybrid MDS based on air levitation, hybrid MDS based on magnetic levitation and conventional railway systems upgraded with MDS technologies, as these are the three configurations defined within the project as the most promising for integration with existing railway systems.

The methodological approach adopted is the one envisaged by the CSM, since it is the approach adopted by the railway sector to address problems related to operational safety, considering that the systems subject to the risk analysis will have to be integrated into traditional railway systems.

The definition of the systems is based on description of the solution, defined in the deliverables D2.1 (Ref. [7]) and D4.1 (Ref. [9]), which gives an overview of a possible configurations of MDS and the interaction/interfaces with the existing infrastructure. Each type of MDS configuration can be implemented with different technologies. Consistent with the level of detail of the information available, the system definition is limited to a short description of the system architecture, that will be used as basis for the hazard identification.

The hazards relating to three Hybrid MSD have been identified, considering those inherent to the technological innovations introduced or those which, despite being present in traditional railways, change significantly due to the use of new technologies.

Subsequently, the hazard log was built with the selected hazards, the preliminary risk assessment was performed, then the risk control measures were identified and, finally, the final risk assessment was performed.

The risk analysis conducted constitutes a first step towards the evaluation of the safety of the systems examined, susceptible to subsequent in-depth analysis in future research projects.

2 Abbreviations and acronyms

ATC	Automatic Train Controller
ATP	Automatic Train Protection
CoP	Code of Practice
CSM RA	Common Safety Method Risk Assessment
EDW	Electro Dynamic Wheels
EN	European Normative
HF	Human Factor
LM	Linear Motor
MDS	MagLev Derived System
RCM	Risk Control Measure
SIL	Safety Integrity Level
WP	Work Package

3 Background

The present document constitutes the Deliverable D3.1 *Hazard Identification and Risk Assessment* in the framework of the Flagship Project HORIZON-ER-JU-2022-FA7-02 – Maglev-Derived Systems for Rail (MaDe4Rail) as described in the EU-RAIL MAWP.

4 Objective/Aim

The main objective of transportation systems is to ensure a quality of service to the passengers both in term of safety and availability of the service. The safety of transportation systems plays a key role in the worldwide railway culture. EU has defined a set of laws and regulations to be applied to the railway sector (Ref. [1]) to ensure that the different actors (infrastructure managers, operators, manufacturers) integrate in their activity the process to ensure the safety of the railway transportation.

One of the key aspects in the achievement of the safety target, is the execution of a risk analysis aiming to identify the potential risks occurring on systems and defining the risk control measures for the control of such risks.

The identification and control of the risk is one of the main items contributing to ensure the safety of a transportation system. Additional aspects to be considered are organisation, role, and competence, which need to be fulfilled to complement the risk analysis.

Risk analysis play a crucial role in the design and development of new systems, such as the MDS under evaluation within the MaDe4Rail project. The potential risks introduced by a new system due to internal failures, external influences, human errors, and other causes, needs to be broadly investigated to ensure that the system can be operate ensuring the safety of the passengers.

The objective of this document is to document the risk analysis for the MDS defined in the MaDe4Rail project (Ref. [7]) (Ref. [8]).

According to the deliverable D2.1 (Ref. [7]), three categories of MDS have been identified:

1. Maglev systems / Full MDS
2. Hybrid MDS
    - Hybrid MDS based on air levitation
    - Hybrid MDS based on magnetic levitation
    - Conventional system upgraded with MDS technologies
3. Hyperloop systems

The common element of the three categories of MDS is the linear motor, as the technology used for the propulsion of the vehicles. Considering that the objective of the MaDe4Rail project is the identification and study of MDS systems compatible with existing railway infrastructure, the risk analysis will be performed to identify the main risk for hybrid MDS.

A short summary of the Hybrid MDS configurations is reported in the chapter 5. The objective of the description is to provide a system definition of the MDS to allow hazard identification. More detailed information can be found in the deliverables D2.1 (Ref. [7]) and D4.1 (Ref. [8]).

The risk analysis in the railway sector is performed according to the following standards:

- CMS-RA (Ref. [2], [3])
- EN 50126 (Ref. [4], [5])

The methodology defined in the existing standards will be applied to new systems introduced in the existing railway infrastructure. A description of the methodology for the risk analysis is reported in the chapter 6.

5 System definition

This chapters present the description for the three MDS configurations defined within the MaDe4Rail project as the most promising for integration with existing railway infrastructure.

5.1 Hybrid MDS based on air levitation

A hybrid MDS system based on air levitation refers to a transportation system able to operate on existing railway infrastructure that relies both on wheel-based suspension and air levitation suspension in combination propelled by a linear motor or Electro Dynamic Wheels (EDW). It can enable the integration of different rail systems such as high-speed rail, conventional rail, light rail, heavy rail, within the same network.

An example of such hybrid transport system combining technologies like air levitation and propulsion by Electro Dynamic Wheels (EDW) is depicted in figure1.

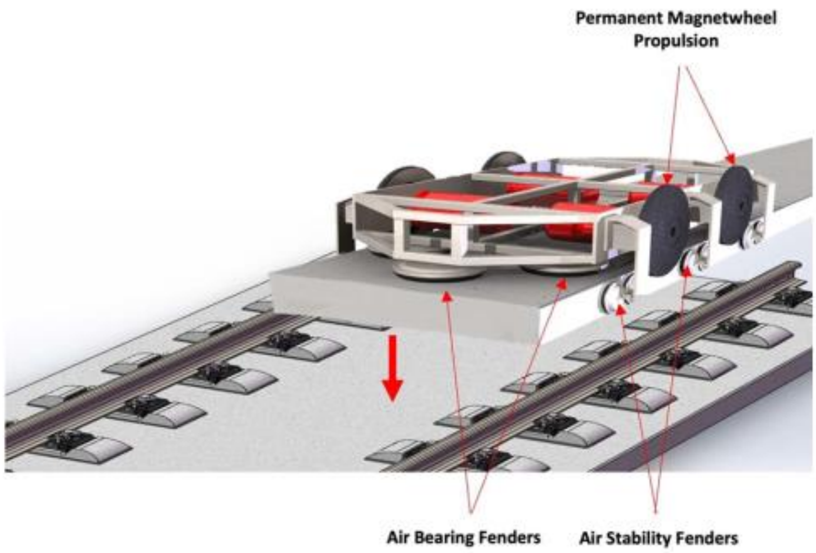

Figure 1 Example of an air levitation hybrid MDS bogie

Such a system facilitates the effortless movement of passengers and bulk goods in any direction by gliding on an ultra-thin layer of air. By channelling air into the specialized Air Bearing Fenders, which move along a flat surface such as a track, road, or floor, an upward force is created. This ultra-thin layer of air significantly reduces friction, allowing for smooth and virtually frictionless travel. This technology delivers a great value over traditional transport (wheels) by two facts:

1. The rolling resistance and wear is harshly minimized,
2. The mass of the vehicle is distributed evenly over a large contact area, compared to the view square centimetres in conventional railway systems, allowing for a much lighter infrastructure.

5.2 Hybrid MDS based on magnetic levitation

A hybrid MDS system utilizing magnetic levitation typically describes a transportation system that combines both wheel-based and magnetic levitation suspensions, depending on the operational conditions, and allows for the operation of both traditional trains and MDS vehicles. For instance, the vehicle may use wheels during switch crossings or when approaching platforms, and switch to magnetic levitation in designated maglev corridors. Propulsion is typically wheel-based during wheeled operation, but may involve different technologies when operating on magnetic levitation. Selecting the appropriate propulsion technology requires a thorough compatibility study and economic evaluation. The design of the vehicle must ensure it is compatible with both existing and potentially upgraded railway infrastructure, as well as interoperable with the broader transportation system.

In figure 2, two variants of possible Hybrid MDS configurations based on maglev are displayed:

- A hybrid system, where wheel-based systems and levitation systems act on the same traditional guideways (series hybrid case);
- A parallel hybrid, where wheel-based systems and levitation systems act on additional parallel separate guideways (parallel hybrid case).

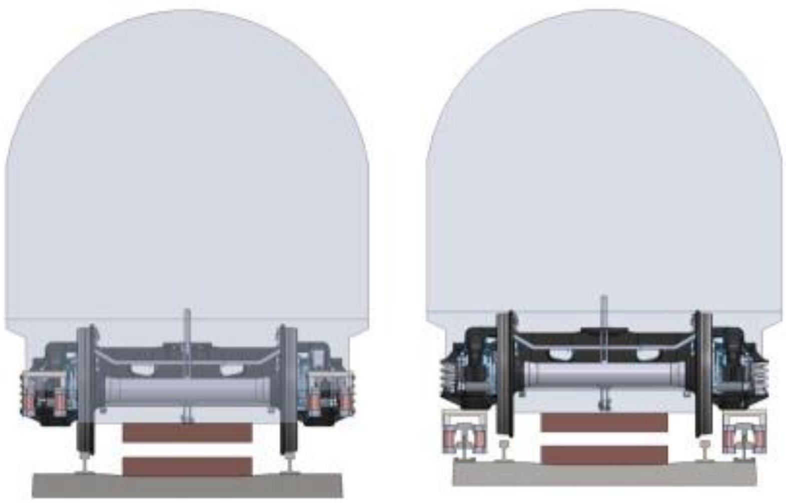

Figure 2 Example of Hybrid MDS based on magnetic levitation: left to right A) vehicle operating on wheels B) Ironlev system engaged on Ironlev guideways, on dedicated maglev corridors (source: Ironbox)

An MDS system can be integrated with conventional wheeled systems to create a hybrid architecture, utilizing traditional wheels for low-speed movements and track switches, and dedicated magnetic suspensions for high-speed, efficient travel. This design aims to enhance system efficiency by reducing contact friction.

On the infrastructure side, the hybrid setup involves augmenting existing railway tracks with auxiliary guideways that work with the MDS suspension subsystem. These could include conductive rails or coils for electromagnetic systems, iron rails for ferromagnetic levitation, or specialized tracks for air levitation. For iron rails, the MDS suspension can be applied directly to traditional guideways without the need for additional rails.

When the system operates on wheels, the guidance is provided by vertical wheels like traditional trains, instead when the system operates on MDS suspension, lateral guidance is required according to the suspension system itself. Generally, guidance subsystem is based on the same technology of the suspension system and integrated in the MDS suspension subsystem (e.g., EDS, EMS or air levitation), so it requires auxiliary guideways for lateral guidance that are generally integrated in the same auxiliary rail used for the suspension. The propulsion and braking can be implemented using different technologies of linear motors or electrodynamic wheels.

5.3 Conventional system upgraded with MDS technologies

A conventional system upgraded with MDS technologies refers to a transportation system that relies on traditional railway architecture, introducing MDS technologies to enhance its performance. Maglev technology has emerged as a breakaway from the conventional wheel-based technology for achieving higher speeds with better performance. On-wheel rail systems use adhesion between wheels and rails to move forward, while maglev systems use propulsion force generated by a linear electro-mechanical system, to move forward.

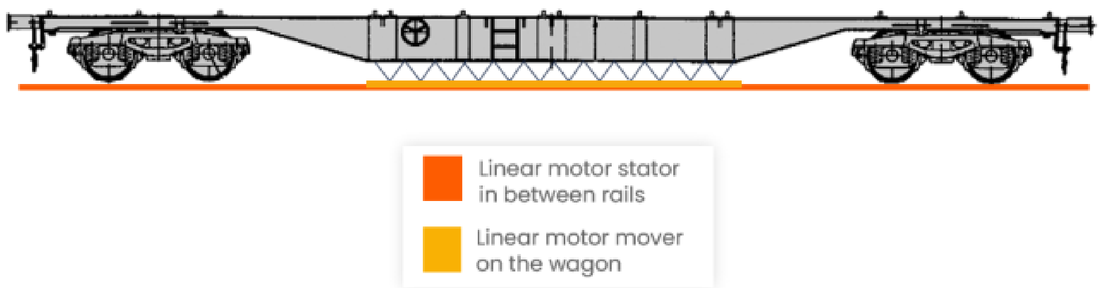

Figure 3 Linear motor-powered retrofitted freight platform

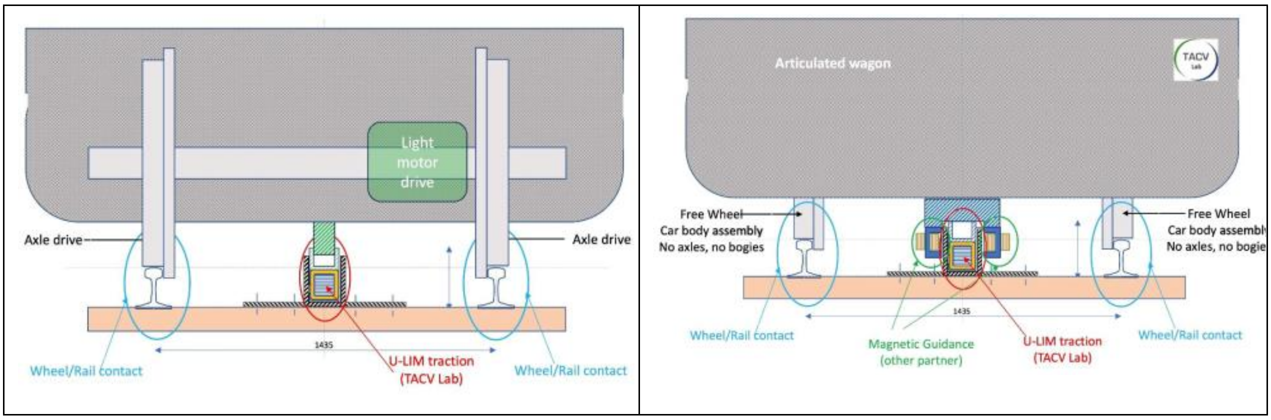

Figure 4 Example of LIM propulsion for MDS system

Alternatively, such a system can be equipped with Linear Induction motor (figure 4) with active part on the vehicle and passive infrastructure.

6 Risk Analysis Methodology

The objective of the risk analysis is to identify and evaluate the possible risks related to the safety of the people (passenger or third-party having interface with the line) that can occur during the operation phase of a system.

The risk analysis in railway sector is performed according to the following standards:

- CMS-RA (Ref. [2], [3])
- EN 50126 (Ref. [4], [5])

The methodology defined in the existing standards is considered to be applicable to new systems introduced in the existing railway infrastructure, such as MDS.

The process defined in the existing standards for the execution of a risk analysis is based on three main tasks:

1) System definition: the objective of the system definition is to define the perimeter of the system under analysis, including its functions and boundaries.
2) Hazard identification: aims to identify in a systematic way the risk to the people that can occur to the system during the operation due to malfunction, external influences, human error, etc.
3) Risk evaluation: aims to quantify the risk and assess if it's acceptable according to the risk acceptance criteria.

These three steps are shown in Figure 5. A more detailed description of the activity and objectives of these steps are described in the following paragraphs.

In addition, to the risk analysis process shown in Figure 5 foresees:

1) Hazard management process: this process requires to record the results of the risk analysis (hazards, risk control measure and risk evaluation) from their identification to the operation. The hazard records shall be updated during the design and implementation phase of the system to ensure that the risk control measures identified are implemented and the risk is controlled according to the applicable risk acceptance criteria. Once the system has been accepted and is in operation, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge of the operation of the system under assessment as an integrated part of its safety management system.
2) Independent assessment: The risk analysis process is subjected to inspection of an 'assessment body' (AsBo) as an independent and competent entity which undertakes investigation to provide a judgement, based on evidence, of the suitability of a system to fulfil its safety requirements.

For the scope of the present document, the results of the risk analysis will be recorded in a hazard log. However, the implementation of the risk control measures, and independent assessment evaluation are out of the scope of the present activity.

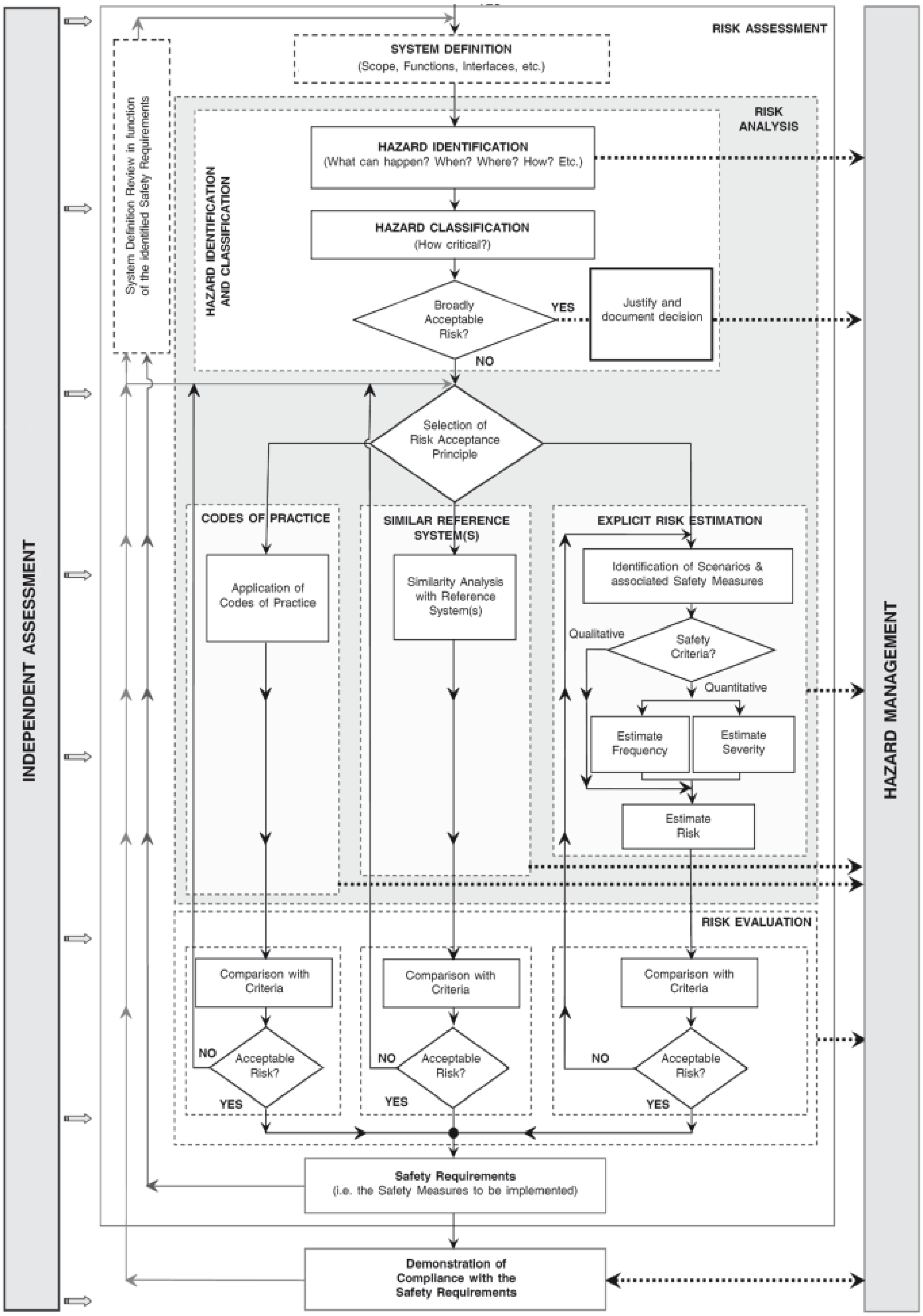

Figure 5 Process for risk analysis (Ref. [2])

6.1 System definition

The risk management process starts with the preparation of a system definition. This provides the key details about the system under analysis including its functions and boundaries.

According to the regulation (Ref. [2]), the system definition should address at least the following issues:

a) system objective, e.g. intended purpose;
b) system functions and elements, where relevant (including e.g. human, technical and operational elements);
c) system boundary including other interacting systems;
d) physical (i.e. interacting systems) and functional (i.e. functional input and output) interfaces;
e) system environment (e.g. energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);
f) existing safety measures and, after iterations, definition of the safety requirements identified by the risk assessment process;
g) assumptions which shall determine the limits for the risk assessment.

Considering the level of detail available of the hybrid MDS and the objective of the project, the system definition is limited to a short description of the system architecture, that will be used as basis for the hazard identification.

It must be noted that at this stage no focus is established on any specific solution. Each type of hybrid MDS can be implemented with different type of solutions and/or technologies. This detail of information is not defined and available at this stage.

The definition of the hybrid MDS is reported in the chapter 5 where for each configuration, the description of the solution is reported based on the information defined in the deliverables D2.1 (Ref. [7]) and D4.1 (Ref. [9]).

The description reported in chapter 5 gives an overview of a possible solution of hybrid MDS and the interaction/interfaces with the existing infrastructure.

6.2 Hazard identification

The hazard identification has as objective to identify any dangerous situation during the operation of the system that can lead to harm to passengers, workers or members of the public. The hazard identification shall be performed in a systematic way to identify any possible cases leading to dangerous situations, as system failures, external influences, human error, etc.

To ensure exhaustiveness of the analysis, the hazard identification is performed in different phases of the project applying different methods such as preliminary hazard analysis, subsystem hazard analysis, interface hazard analysis, etc. Description of the different techniques is reported in the MIL-STD-882E (Ref. [6]). The hazard identification is not limited to the design phases of a project, but it continues in an interactive way during the implementation and operation phase.

For the scope of this project and considering the level of detail available, the hazard identification has been performed for the Hybrid MDS defined in previews phases of the project (Ref. [7]).

The analysis has been focused on the novelty and innovation introduced by the MDS. Where the introduction of a MDS technology doesn't have any impact on the conventional railway architecture, the risk related to the traditional systems has not been investigated, because it has been assumed that they are already handled in the existing railway infrastructure.

The identification of the hazard for each MDS system included in the perimeter of the analysis has been performed by:

1) subsystem hazard identification;
2) hazard workshop integrating the hazards identified at the previous step.

The subsystem hazard identification aims to identify hazards associated with the design of subsystems; and, to recommend actions necessary to eliminate identified hazards or mitigate their associated risks. This approach has been integrated with hazard workshops involving different expertise aiming to review the hazards identified at the subsystem level and integrate them to identify other hazards.

The subsystem hazard analysis has been performed for each fundamental subsystem of MDS breakdown structure defined in the D2.1 (Ref. [7]): Vehicle, Infrastructure, Energy and Command and Control. (See Figure 6)

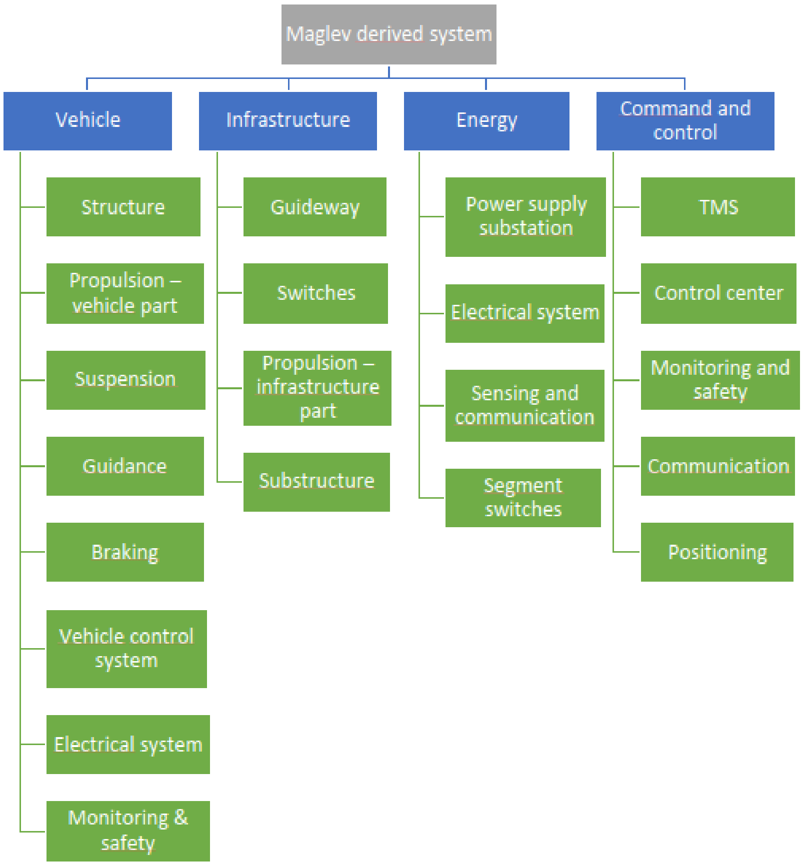

Figure 6 MDS Breakdown Structure

For each subsystem, the hazards have been identify considering the novelty and innovation introduced by the MDS solutions. The hazards have been identified considering causes raised by the subsystem malfunction and the interfaces with the other subsystems. The hazards will be then identified for each combination of Hybrid MDS and subsystem as shown in Table 1.

Table 1 Matrix of MDS / subsystem under analysis

	Vehicle	Infrastructure	Energy	Command and Control
Hybrid MDS based on air levitation	Hazards	Hazards	Hazards	Hazards
Hybrid MDS based on magnetic levitation	Hazards	Hazards	Hazards	Hazards
Conventional system upgraded with MDS technologies	Hazards	Hazards	Hazards	Hazards

For each hazard, the following information has been defined:

a) MDS category according to the perimeter defined in the Chapter 5;
b) Description of the hazard;
c) Description of the cause of the hazard (as malfunction, external influences, human error, etc);
d) Description of the consequences due to the hazard, as derailment, collision, fire, electrocution, etc.

This information has been recorded in the hazard log table as described in the paragraph 6.4. The results of the hazard identification are shown in Annex A, Annex B and Annex C.

6.3 Risk evaluation

Once the hazards have been identified, they shall be evaluated in term of risk and risk control measures (safety requirements) defined to make the risk acceptable according to the risk acceptance criteria.

The evaluation of the risk is performed in two stages:

1) Evaluation of the initial risk without risk control measures.
2) Evaluation of the residual risk considering risk control measures to mitigate the initial risk if it has been assessed as not acceptable according to the risk acceptable criteria.

The evaluation of the risk before the definition of the risk control measures aims to define if the initial risk of the hazards is broadly acceptable. As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional measure, for example when no injury to humans would be derived from the hazard. In this case the hazard must be recorded in the hazard log as long as the justification of broadly acceptable risk is provided.

Where the risk cannot be classified as broadly acceptable, risk control measures must be identified by applying the following risk acceptable principles:

- Code of practice
- Reference system
- Explicit risk estimation

The risk acceptance principles define the rules used in order to arrive at the conclusion whether or not the risk related to one or more specific hazards is acceptable.

The risk assessment process shall bring to the identification of different possible safety measures that might be put in place either to eliminate the risk(s) or to control the risk(s) to an acceptable level (i.e. decrease the frequency of its occurrence or mitigate the consequences of the hazard). These risk control measures could be technical, operational or organizational. The efficiency of the safety measures could be assessed quantitatively, where relevant, semi-quantitatively or qualitatively (e.g. use of trained drivers for controlling human factor errors).

The criteria for the application of the risk acceptance principle and the identification of the risk control measures are defined in the following paragraphs.

6.3.1 Code of practice

Codes of Practice (CoP), when correctly applied, may be used to control one or more specific hazards. Application of Codes of Practice may be used as a risk acceptance principle. Each Code of Practice should meet the following requirements:

- be a set of rules widely recognized in the transportation system domain. If this is not the case, the CoP shall be justified;
- be relevant for the control of the hazard in the system under consideration.

If one or more hazards are controlled by codes of practice fulfilling the requirements above, then the risks associated with these hazards shall be considered acceptable. This means that these risks don't need to be further analysed. The use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.

6.3.2 Reference system

The system under consideration may be compared with a reference system for risk assessment. The application of a reference system may be used as a risk acceptance principle. The similar reference system shall satisfy the following requirements:

- it has already been proven in-use to have an acceptable safety level and would therefore still qualify for approval;
- it has similar functions and interfaces as the system under consideration;
- it is used under similar operational conditions as the system under consideration for a sufficient period of time and has given confidence with the range of observed hazards and accidents;
- it is used under similar environmental conditions as the system under consideration.

This approach implies that the information was recorded for the project that introduced the reference system and that the information has been retained.

If a reference system fulfils the requirements listed above, then for the system under consideration:

- the risks associated with the hazards covered by the reference system shall be considered as acceptable;

- the safety requirements for the hazards covered by the reference system shall be derived from the safety analyses or from an evaluation of safety records of the reference system;
- these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.

If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system, applying another reference system or one of the two other risk acceptance principles. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.

6.3.3Explicit risk estimation

If the previous risk acceptance principles are not applicable, then the evaluation of the risk can be performed applying explicit risk estimation. The explicit risk estimation aims to evaluate the risk of each hazard by combining the consequence and frequency of the hazard.

The estimation may be done quantitatively and/or qualitatively:

- Quantitative explicit risk estimation is performed by estimating the frequency of occurrence and the severity of an accident scenario. This shall be done for the consequences of all identified hazardous scenarios, using data and I or expert judgment;
- Qualitative explicit risk estimation shall be performed by use of expert judgement (e.g. using a logical argument based on system definition).

The consequences classes defined to evaluate a risk are presented in Table 2:

Table 2 Consequence classes from EN 50126 (Ref. [4])

Class	Description	Definition
S1	Insignificant	At least single minor injury
S2	Marginal	At least single major injury or multiple minor injuries
S3	Critical	Single fatality or multiple major injuries
S4	Catastrophic	Multiple fatalities > 10

The frequency classes used to determinate the rate of occurrence of each hazard are presented in Table 3:

Table 3 Frequency classes from EN 50126 (Ref. [4])

Class	Frequency range	Description
F1	Frequent $F > 10^{-3}$	More than once within a period of approximately times 6 weeks
F2	Probable $10^{-3} \leq F < 10^{-4}$	Approximately once per weeks to once per year
F3	Occasional $10^{-3} \leq F < 10^{-5}$	Approximately once per 1 year to once per 10 years
F4	Rare $10^{-5} \leq F < 10^{-7}$	Approximately once per 1 0 years to once per perhaps once at most 1 000 years
F5	Improbable $10^{-7} \leq F < 10^{-9}$	Approximately once per not expected to happen 1 000 years to once per within the lifetime 100 000 years
F6	Highly improbable $F \leq 10^{-9}$	Once in a period of extremely unlikely to approximately 100 000 happen within the lifetime years or more

To apply explicit risk estimation the definition of a risk acceptance criteria is needed. They are defined by following risk matrix combining consequences and frequency classes (Table 4 and

Table 5).

Table 4 Risk matrix from EN 50126 (Ref. [4])

			Severity Classes			
			S1	S2	S3	S4
			Insignificant Minor injury	Marginal Major injury	Critical Single fatality	Catastrophic Multiple fatalities
Frequency Classes	F1	Frequent $F > 10^{-3}$	Undesirable	Intolerable	Intolerable	Intolerable
	F2	Probable $10^{-3} \leq F < 10^{-4}$	Tolerable	Undesirable	Intolerable	Intolerable
	F3	Occasional $10^{-4} \leq F < 10^{-5}$	Tolerable	Undesirable	Undesirable	Intolerable
	F4	Rare $10^{-5} \leq F < 10^{-7}$	Acceptable	Tolerable	Undesirable	Intolerable
	F5	Improbable $10^{-7} \leq F < 10^{-9}$	Acceptable	Acceptable	Tolerable	Intolerable
	F6	Highly improbable	Acceptable	Acceptable	Acceptable	Tolerable

		$F \le 10^{-9}$				

Table 5 Risk classification from EN 50126 (Ref. [4])

Intolerable	The risk shall be eliminated
Undesirable	The risk shall only be accepted if its reduction is impracticable and with the agreement of the railway duty holders or the responsible Safety Regulatory Authority.
Tolerable	The risk can be tolerated and accepted with adequate control (e.g. maintenance procedures or rules) and with the agreement of the responsible railway duty holders.
Acceptable	The risk is acceptable without the agreement of the railway duty holders.

6.4 Hazard log format

The hazard log is the tool identified by the railway safety standard (Ref. [4]) to track the hazards and their closure. The hazard log is updated throughout the life cycle whenever a change to identified hazards occurs or a new hazard is identified. The hazard log includes among others:

a) description of the hazard, including causes and consequences;
b) the evaluation of the hazard in term of severity and frequency;
c) the measure taken to reduce risks to a tolerable level or to remove the risks;
d) the responsible party to ensure the and the implementation of the risk control measures;
e) the evidence showing the implementation of the risk control measures.

A hazard log has been established to record the hazard identified for the hybrid MDS as well as the risk evaluation and risk control measures identified to mitigate each risk.

The hazard log is composed by the fields reported in Table 6:

Table 6 Fields of the hazard log

Field	Description
Hazard ID	It defines the unique identifier of the hazard (H01, H02, etc)
Subsystem	It defines to which subsystem of the MDS system the hazard is applicable: • Infrastructure • Vehicle • Energy • Command and Control
Hazard Description	Text describing the hazardous scenario
Hazard Cause	Text describing the cause leading to the hazardous scenarios
Accident/Danger	It describes the consequence when the hazardous scenarios occur
Initial Severity	Initial severity of the hazard defined according to the severity classes of table 2
Initial Frequency	Initial severity of the hazard defined according to the frequency classes of table 3. This field may by empty if the risk evaluation is qualitative
Initial Risk	Initial risk of the hazard defined according to the risk classes of the risk matrix (Ref. table 4 and table 5)
Type of Hybrid MDS	It defines for which Hybrid MDS system the hazard is applicable: • Hybrid MDS based on air levitation • Hybrid MDS based on magnetic levitation • Conventional system upgraded with MDS technologies
Risk Acceptance Principle	It defines the risk acceptance principle used to evaluate mitigate and evaluate the residual risk
RCM ID	ID of the risk control measures used to mitigate the hazard: • RCM_HyAirLev_xx: RCM related to Hybrid MDS based on air levitation • RCM_HyMagLev_xx: RCM related to Hybrid MDS based on magnetic levitation • RCM_CS-wMDS_xx: RCM related to conventional system upgraded with MDS technologies
RCM Description	Text describing the RCM used to mitigate the hazard
RCM owner	Subsystem responsible to implement the risk control measure to mitigate the hazard
Residual Severity	Residual severity of the hazard defined according to the severity classes of table 2 taking into consideration the risk control measures
Residual Frequency	Residual frequency of the hazard defined according to the frequency classes of table 3 considering the risk control measures. This field may by empty if the risk evaluation is qualitative

Field	Description
Residual Risk	Residual risk of the hazard defined according to the risk classes of the risk matrix (Ref. table 4, table 5) taking into consideration the risk control measures
Remarks	Additional notes related to the hazard (hypotheses, assumptions, etc.)

The hazard logs containing the results of the hazard identification and risk evaluation for the different hybrid MDS are shown in the appendices of this document.

7 Risk analysis results

This chapter aims to present the results of the task 3.1 (hazard identification) and 3.2 (risk evaluation) from WP3 of the MaDe4Rail project.

7.1 Hazard identification results

The hazard lists were prepared performing, with contribution of the different participants of WP3, a hazard analysis for each subsystem (infrastructure, vehicle, energy and CCS). Afterwards, hazard workshops were performed to review and discuss the list of identified hazards (e.g. eliminating the risks not linked to operational safety and which did not meet the criteria illustrated by the methodology (Ref. 6.2)) and integrated additional hazardous scenarios derived by the discussion.

The hazards related to the human factors and external factors have been considered as possible causes for the different subsystems and included within them.

Finally, the different hazards were referred to the subsystems considered:

- Vehicle;
- Infrastructure;
- Energy;
- Command and Control;

And to the three different MDS configurations examined:

- Hybrid MDS based on air levitation;
- Hybrid MDS based on magnetic levitation;
- Conventional system upgraded with MDS technologies.

8 The hazard identified are collected in the Appendices

*Annex A*Annex A, Annex B and Annex C respectively for each type of hybrid MDS.

Considering that the hazard identification has been focused on the novelty and innovation introduced by the hybrid MDS, the hazards identified are mainly related to:

- Malfunction of levitation and guidance of new system
- Malfunction of propulsion and braking system realised with a linear motor
- Malfunction of new generation of switches allowing to integrate linear motor and levitation.

Table 7 shows the matrix that associates the hazards relating to the subsystems considered to each MDS. It should be noted that for systems based on air levitation there are no risks for the energy subsystem, as it has been assumed that for these systems there are no active components on the route different to the catenary.

Table 7 Matrix of MDS / subsystem hazards

	Vehicle	Infrastructure	Energy	Command and Control
Hybrid MDS based on air levitation.	H01, H03, H06, H08, H10, H14, H16, H23	H01, H04, H09, H16, H17, H20, H21,	–	H01, H02, H04, H8, H15
Hybrid MDS based on magnetic levitation.	H01, H03, H05, H06, H7, H08, H10, H14, H16, H23	H01, H02, H03, H04, H05, H06, H08, H09, H10 H11, H12, H13, H14, H16, H17, H18, H19, H20, H21, H22, H23	H03, H08	H01, H02, H04, H08, H15.

	Vehicle	Infrastructure	Energy	Command and Control
Conventional system upgraded with MDS technologies.	H01, H03, H05, H07, H08, H14, H16, H23.	H01, H03, H04, H05, H06, H08, H09, H11, H12, H13, H14, H16, H17, H18, h19, H20, H23.	H03, H08	H01, H02, H04, H08, H15.

8.1 Risk evaluation

Once the hazards had been defined, their causes had been determined and the accident scenario that may arise had been identified, the hazard log was completed with the risk evaluation.

The objectives of the risk evaluation are:

- Evaluate if the risk associated to each hazard is broadly acceptable;
- Define the risk acceptance principle for the identification of the risk control measure and justification of the residual risk;
- Define the risk control measures in accordance with the risk acceptance principle;
- Evaluate the effectiveness of the measures to make the residual risk acceptable according to the risk acceptance criteria.

Safety review workshops have been organised with the experts from the partners of Task 3.2 to review and integrate the results of the subsystem hazard identification.

The initial risk assessment in the absence of any risk control measures have been evaluated to define if the initial risk of each hazard was broadly acceptable. As shown in the Annex A, annex B and Annex C, the severity associated to all hazards without any risk control measures has been defined as S5 – Catastrophic (multiple fatalities). As described in the previous paragraph, the introduction of MDS impacts on guidance, propulsion and braking of the vehicle. Therefore, the malfunction of the systems implementing these functions may have catastrophic consequence as derailment or collision leading to multiple fatalities.

Therefore, the initial risk of the hazards has been assumed “Intolerable” (Ref. table 4). It means that more than one event every 100’000 years is expected without any risk control measure (initial frequency > 10^{-9} event per hour).

Subsequently, the mitigation risk control measures were identified, and a new risk assessment was carried out based on the selected risk acceptance principle. The risk estimation has been performed for most of the hazards applying the explicit risk estimation. Considering that the hazards identified are related to novelty and innovation introduced by MDS system, the application of code of practice, reference system has resulted difficult in several cases due to missing existing standards or reference systems on which to base the risk estimation and derive existing safety requirements. In addition, considering that the definition of the system is not fully defined, only a qualitative risk estimation has been applied in several cases.

The risk control measures have been identified with the support of the experts participating in the workshops. The risk control measures are mainly related to the implementation of technical solutions in the design of the system (i.e. safety functions). To make catastrophic hazards acceptable according to the risk acceptance criteria defined by the risk matrix (ref. Table 4) the risk control measures shall present a high level of safety integrity to reduce the risk to a tolerable level.

Considering that the hazard identification and risk assessment have been performed on generic solution of MDS systems, without considering specific technologies, the feasibility of the risk control measures must be further studied in the next phases, considering also alternative solutions not identified at this stage and the cost for the implementation of the different measures.

Annex A, Annex B and Annex C show the tables with the completed hazard log, respectively, for the hybrid MDS based on air levitation, for the hybrid MDS based on maglev and for conventional railway system upgraded with MDS technologies.

9 Conclusion

The hazard analysis conducted is based on three generic MDS system configurations, without specification to the underlying technologies that will ultimately be applied. This approach necessitates a thorough review and detailing of the analysis for each system in more specific analysis, taking into account the possible technological solutions. The current analysis is, therefore, a preliminary step that can be expanded upon in future research projects. These projects should aim to provide a more detailed definition of the technical-functional characteristics of the different systems.

Given that the technology in question is new and lacks existing codes of practice, regulations, standards and reference systems, most of the hazards have been evaluated based on explicit risk estimations. This introduces a level of uncertainty and necessitates caution in interpreting the results.

Within the limitations described, particularly due to the state of definition of the MDS configurations analysed within the MaDe4Rail project, the identified mitigation measures should be viewed as a series of requirements that these systems must meet rather than concrete security measures. These requirements serve as a guideline for ensuring the safety and reliability of the systems. Such requirements will be considered in further tasks and deliverables of the project, such as the technical feasibility analysis and the design concept of a prototype for a MDS vehicle.

In further research and development activities, t is essential that the identified measures be discussed with the system designers. This discussion should explore possible alternatives and compare the measures against the As Low As Reasonably Practicable (ALARP) criteria. Such collaboration will help in refining the measures and ensuring they are practical and effective.

Despite the limitations mentioned, the performed risk analysis does not reveal any insurmountable critical issues for the future application of the systems examined. This preliminary analysis provides a foundation upon which more detailed and specific risk assessments can be built as the technical solutions become clearer.

10 References

[1] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety

[2] Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009

[3] Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment

[4] EN 50126-1 (2017) Railway applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process

[5] EN 50126-2 (2017) Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[6] MIL-STD-882E Department of Defense - Standard Practice – System Safety

[7] 2023-10-31_MaDe4Rail_D2.1_Nevomo_V1.0

[8] 2023-12-20_MaDe4Rail_D2.2_DITS_V2.0

[9] 2023-12-05_MaDe4Rail_D4.1_ITF_V1.0

11 Appendices

Annex A – Hazard Log – MDS based on air levitation

Hazard Identification							Risk Assessment									
Hazard ID	Component name	Hazard Description	Hazard causes	Accident/Danger	Type of Hybrid MDS	Initial Severity	Initial Frequency	Initial Risk	Risk Acceptance Principle	RCM ID	RCM Description	RCM Owner	Residual Severity	Residual Frequency	Residual Risk	Remarks
H01	Infrastructure	Passing point at danger	Failure of LM (insufficient brake)	Collision with the infrastructure or other vehicle; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_23	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Vehicle	Passing point at danger	Insufficient brake	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_23	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Command and control	Passing point at danger	Failure in command and control system	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_19	The command and control system shall have safety integral level 4.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	HF	Passing point at danger	Driver doesn't stop the train	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_01	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the operation with drivers
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization to MDS driverless vehicle or	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_11	Maintenance vehicle shall be contoller by Automatic Train Protection (ATP) to allow safe operation with driverless passegner vehicles	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario with driverless operation
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization to MDS driverless vehicle or	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_12	Operation procedure shall be implemented by operator to avoid that maintenance vehicle without APT enters in the track during the passengers sevice	Operator/maintainer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H03	Vehicle	Too high acceleration	Failure of wrong command of the onboard propulsion control system	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_22	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is onboard of the vehicle
H04	Infrastructure / Switches	Switch in the wrong position	Mechanical MDS turnout failure	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_05	Interlocking system shall monitor the position of the switches. The passage of the train shall be allowed only if the switches is detected on the right position.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	1. MDS system may requires now type of switches which integrate the linear motor. The linear motor can move together with the switch. 2. Physical turnout malfunction may be caused by objects blocking the points, pointing to machince defect
H04	Infrastructure / Switches	Switch in the wrong position	Movement of of the swich during the train runnig on it	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_18	Switches shall be equipped with pointlocking system to avoid mouvement during the passage of the train.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	MDS system may requires new type of switches which integrate the linear motor. The linear motor can move together with the switch.
H04	Command and control	Switch not aligned to the position required to follow the route of the vehicle	Command failure	Derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_06	Interlocking system shall monitor the position of the switches. The passage of the vehicle shall be allowed only if the switches is detected on the right position of the vehicle route.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H06	Vehicle/electrical system	Insufficient active levitation force.	On board energy supply failure	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_27	Vehicle shall be equipped with a levitation monitoring system. Vehicle shall be put in safe state if levitation is under the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system onboard
H06	Vehicle/electrical system	Insufficient active levitation force.	On board energy supply failure	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_21	The vehicle shall be equipped with emergency power supply sufficient to allow the stop of the the vehicle in case of loss of normal power to the active levitation system	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system onboard
H06	Vehicle	Insufficient active levitation force.	Failure of air levitation devices on board	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_31	Vehicle levitation system shall be designer considering safety factor	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H08	Vehicle	Too high deceleration	vehicle control	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_22	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H08	HF	Too high deceleration	Driver's error	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_01	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers
H09	Infrastructure	Infrastructure component in the gabarit	Lack of maintenance	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_14	Period inspection and maintenance of the infrastructure installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H10	Exeternal	Lack of guidance	Winding	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_31	Weather station shall be foreseen to detect the presence of adverse weater conditions. An alarm shall be raised when the acceptable thresholds are exceeded and the service shall be stopped	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Hazard Identification								Risk Assessment										
Hazard ID	**Component name**	**Hazard Description**	**Hazard causes**	**Accident/Danger**	**Type of Hybrid MDS**	**Initial Severity**	**Initial Frequency**	**Initial Risk**	**Risk Acceptance Principle**	**RCM ID**	**RCM Description**	**RCM Owner**	**Residual Severity**	**Residual Frequency**	**Residual Risk**	**Remarks**		
H10	Exeternal	Lack of guidance	Winding	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_13	Operator shall monitor weather condition with forecast and stop the service if the adverse weater conditions are foreseen.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H10	Vehicle	Lack of guidance	Failure of guidance devices on board	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_25	Vehicle guidance system shall be designer considering safety factor	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H10	Vehicle	Lack of guidance	Failure of guidance devices on board	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_17	Periodic inspection and maintenace of guidance system to prevent for possible failure	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H14	Vehicle	Vibration	Incorrect functioning of on-board levitation/guidance equipment	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_20	The vehicle shall be equipped with a vibration control system. It commands the emergency stop of the vehicle if the vibrations exceed the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H15	command and control	Too high speed in curve	Incorrect functioning of on-board control	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_01	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H15	command and control	Too high speed in curve	Incorrect functioning of central control	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_01	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H15	HF	Too high speed in curve	Driver's errror	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_01	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers		
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_02	Design and construction of the vehicle shall ensure that the components are well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_15	Period inspection and maintenance of the vehicle components shall be performed to ensure that they are well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_03	Design and construction of the vehicle shall ensure that the infrastructure installation are outside the vehicle gauge and well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_14	Period inspection and maintenance of the infrastructure installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_28	Vehicle shall be equipped with object detection system. The system commands the stop of the vehicle in case of object detection. Note: this solution is not applied to high speed system.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_24	Track shall be protected with fence to avoid intrusion or introduction (voluntary and non) of objects on the track.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_16	Period inspection of the track shall be performed to dected and remove external objects	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H20	Infrastructure	Contact of people with powered equipment on the track	Exceptional presence of people on track	Electrocution	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_08	Linear motor on the track shall be protected by non conductive protection to avoid contact with live parts	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H21	Infrastructure	Loss of guidance	presence of ice/snow	Collision with infrastructure and deraillment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_04	Guidance system shall be equipped with a system that avoid the formation of ice/snow	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H21	Infrastructure	Loss of guidance	presence of ice/snow	Collision with infrastructure and deraillment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_10	Maintainer shall clean the track to remove the ice and snow before the start of the operation and if needed during the operation	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_30	On board linear motor shall be equipped with cooling system to maintenance the temperature of the magnent in the acceptable range	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Hybrid MDS air lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyAirLev_29	On board linear motor (stator) shall be equipped with monitoring temperature system. If the temperature exceeds the limits, an alarm shall be sent to the vehicle to stop	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable			

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Annex B – Hazard Log – MDS based on magnetic levitation

Hazard Identification							Risk Assessment									
Hazard ID	**Component name**	**Hazard Description**	**Hazard causes**	**Accident/Danger**	**Type of Hybrid MDS**	**Initial Severity**	**Initial Frequency**	**Initial Risk**	**Risk Acceptance Principle**	**RCM ID**	**RCM Description**	**RCM Owner**	**Residual Severity**	**Residual Frequency**	**Residual Risk**	**Remarks**
H01	Infrastructure	Passing point at danger	Failure of LM (insufficient brake)	Collision with the infrastructure or other vehicle; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_32	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train (e.g. two linear motors)	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Vehicle	Passing point at danger	Failure of LM (insufficient brake)	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_32	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train (e.g. two linear motors)	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Command and control	Passing point at danger	Failure in command and control system	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_26	The command and control system shall have safety integral level 4.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	HF	Passing point at danger	Driver doesn't stop the train	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the operation with drivers
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_16	Maintenance vehicle shall be contoller by Automatic Train Protection (ATP) to allow safe operation with driverless passegner vehicles	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario with driverless operation
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_17	Operation procedure shall be implemented by operator to avoid that maintenance vehicle without APT enters in the track during the passengers sevice	Operator/maintainer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H03	Infrastructure	Too high acceleration	Failure of wrong command of the wayside propulsion control system	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_31	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is on the wayside
H03	Vehicle	Too high acceleration	Failure of wrong command of the onboard propulsion control system	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_31	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is onboard of the vehicle
H03	Energy	Too high acceleration	Overvoltage in the linear motor	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_13	Linear motor shall be equipped with over voltage protection	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is onboard of the vehicle
H04	Infrastructure / Switches	Switch in the wrong position	Mechanical MDS turnout failure	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_07	Interlocking system shall monitor the position of the switches. The passage of the train shall be allowed only if the switches is detected on the right position.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	1. MDS system may requires now type of switches which integrate the linear motor. The linear motor can move together with the switch. 2. Physical turnout malfunction may be caused by objects blocking the points, pointing to machince defect
H04	Infrastructure / Switches	Switch in the wrong position	Movement of of the swich during the train runnig on it	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_25	Switches shall be equipped with pointlocking system to avoid mouvement during the passage of the train.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	MDS system may requires new type of switches which integrate the linear motor. The linear motor can move together with the switch.
H04	Infrastructure/Propulsion Energy/Segment	High deceleration of the vehicle due to linear motor unpowered	Power supply provided to the wrong LIM segment of the switch	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_09	Interloking system shall monitor the corrct segment supply in order to supply those in the direction of the vehicle	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Hazard can occur when in presence of a swich, the power supply is not provided to the correct segment in the direction of the vehicle.
H04	Command and control	Switch not aligned to the position required to follow the route of the vehicle	Command failure	Derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_08	Interlocking system shall monitor the position of the switches. The passage of the vehicle shall be allowed only if the switches is detected on the right position of the vehicle route.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H05	Infrastructure/levitation	Insufficient passive levitation force.	Wayside levitation device failure/ magnet wear	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_30	The vehicle shall be equipped with monitoring system of the magnetic field generated by the passive levitation system. Vehicle shall be put in safe state if the magnetic field exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard covers the case of passive levitation system on the track
H05	Vehicle/guidance	Insufficient passive levitation force.	On board levitation device failure/ magnet wear	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_36	Vehicle shall be equipped with a levitation monitoring system. Vehicle shall be put in safe state if levitation exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard covers the case of vehicle equipped with passive levitation system
H06	Infrastructure/levitation	Insufficient active levitation force.	Not correct power supply in levitation magnet	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_39	Wayside active livitation system shall be power by emergency power supply to allow the safe stop of the train in case of loss of normal power.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system on the track
H06	Infrastructure/levitation	Insufficient active levitation force.	Not correct power supply in levitation magnet	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_40	Wayside active livitation system shall be power by redundant and independent power supply sources	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system on the track
H06	Vehicle/electrical system	Insufficient active levitation force.	On board energy supply failure	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_37	Vehicle shall be equipped with a levitation monitoring system. Vehicle shall be put in safe state if levitation is under the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system onboard
H06	Vehicle/electrical system	Insufficient active levitation force.	On board energy supply failure	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_29	The vehicle shall be equipped with emergency power supply sufficient to allow the stop of the the vehicle in case of loss of normal power to the active levitation system	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system onboard
H07	Vehicle	Insufficient levitation force	Vehicle too heavy	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_27	The vehicle shall be equipped with a load weighing systems. The traction of the vehicle shall be inhibited if the load threshold is exceeded	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Hazard Identification							Risk Assessment									
Hazard ID	**Component name**	**Hazard Description**	**Hazard causes**	**Accident/Danger**	**Type of Hybrid MDS**	**Initial Severity**	**Initial Frequency**	**Initial Risk**	**Risk Acceptance Principle**	**RCM ID**	**RCM Description**	**RCM Owner**	**Residual Severity**	**Residual Frequency**	**Residual Risk**	**Remarks**
H08	Infrastructure/Propulsion Energy/Segment	Too high deceleration	Segment defect	Infrastructure, vehicle, personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_11	Linear motor shall be designed to ensure a limitation of deceleration in case of segment failure	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Hazard can occur in systems with infrastructure-controlled propulsion. For linear syncronus motors
H08	Vehicle	Too high deceleration	vehicle control	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_31	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H08	HF	Too high deceleration	Driver's error	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers
H08	Energy/Power Supply Substation	Too high deceleration	LM power inverter failure	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_14	Linear motor shall be supplier by redundant and independennt inverters	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	While moving at high speed
H09	Infrastructure	Infrastructure component in the gabarit	Lack of maintenance	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_19	Period inspection and maintenance of the infrastructure installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H10	Exeternal	Lack of guidance	Winding	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_43	Weather station shall be foreseen to detect the presence of adverse weater conditions. An alarm shall be raised when the acceptable thresholds are exceeded and the service shall be stopped	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H10	Exeternal	Lack of guidance	Winding	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_18	Operator shall monitor weather condition with forecast and stop the service if the adverse weater conditions are foreseen.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H10	Vehicle	Lack of guidance	Failure of guidance devices on board	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_35	Vehicle guidance system shall be designer considering safety factor	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H10	Vehicle	Lack of guidance	Failure of guidance devices on board	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_22	Periodic inspection and maintenace of guidance system to prevent for possible failure	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H11	Infrastructure/Guidance	Delay in activation of the active lateral guide	Comunication failure	Collision with infrastructure	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Code of practice	RCM_HyMagLev_03	Communication system shall be design according to the applicable standard to ensure reliable and safe transmission of the data. Emergency braking of the vehicle shall be applied if the loss of communication exceed the fixed timout.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes
H12	Infrastructure/Guidance	Insufficent active guidance force	Power outage infrastructure (electro magnet)	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_40	Wayside active livitation system shall be power by redundant and independent power supply sources	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes due to failure of guidance active guidance system
H12	Infrastructure/Guidance	Insufficent active guidance force	Power outage infrastructure (electro magnet)	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_39	Wayside active livitation system shall be power by emergency power supply to allow the safe stop of the train in case of loss of normal power.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes due to failure of guidance active guidance system
H13	Infrastructure/Guidance	Insufficient passive guidance force	Magnets deterioration	Collision with infrastructure	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_30	The vehicle shall be equipped with monitoring system of the magnetic field generated by the passive levitation system. Vehicle shall be put in safe state if the magnetic field exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H14	Vehicle	Vibration	Incorrect functioning of on-board levitation/guidance equipment	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_28	The vehicle shall be equipped with a vibration control system. It commands the emergency stop of the vehicle if the vibrations exceed the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H14	Infrastructure	Vibration	Incorrect functioning of on-site levitation/guidance equipment	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_28	The vehicle shall be equipped with a vibration control system. It commands the emergency stop of the vehicle if the vibrations exceed the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H15	command and control	Too high speed in curve	Incorrect functioning of on-board control	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H15	command and control	Too high speed in curve	Incorrect functioning of central control	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H15	HF	Too high speed in curve	Driver's errror	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_04	Design and construction of the vehicle shall ensure that the components are well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_20	Period inspection and maintenance of the vehicle components shall be performed to ensure that they are well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Hazard Identification							Risk Assessment												
Hazard ID	**Component name**	**Hazard Description**	**Hazard causes**	**Accident/Danger**	**Type of Hybrid MDS**	**Initial Severity**	**Initial Frequency**	**Initial Risk**	**Risk Acceptance Principle**	**RCM ID**	**RCM Description**	**RCM Owner**	**Residual Severity**	**Residual Frequency**	**Residual Risk**	**Remarks**			
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_05	Design and construction of the vehicle shall ensure that the infrastructure installation are outside the vehicle gauge and well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_19	Period inspection and maintenance of the infrastructure installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_38	Vehicle shall be equipped with object detection system. The system commands the stop of the vehicle in case of object detection. Note: this solution is not applied to high speed system.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_34	Track shall be protected with fence to avoid intrusion or introduction (voluntary and non) of objects on the track.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_21	Period inspection of the track shall be performed to dected and remove external objects	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H18	Infrastructure/Propulsion Energy/Segment	Erroneous activation of the propulsion system	Failure of the control center operators; failure in command and control system; error of the driver in the vehicle, if any.	collision with other vehicle	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_01	Automatic Train Protection (ATP) and Automatic Train Controller (ATC) shall be foreseen to mitigate driver or operator error.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Ground controlled propulsion system			
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Derailment, collision with the infrastructure or other vehicle; vehicle damage; personnel and passengers may be harmed	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_12	Linear motor shall be equipped with monitoring system that detects failures of segment integrity. In case of detection, an alarm shall be raised to stop the vehicle before of the failed segment.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.			
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_12	Linear motor shall be equipped with monitoring system that detects failures of segment integrity. In case of detection, an alarm shall be raised to stop the vehicle before of the failed segment.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.			
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_24	Signalling system shall command the cut off of the power supply to the wayside linear motor to ensure a safe evacuation of the people.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.			
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_23	Procedure shall be implemented to ensure that power supply on wayside linear motor is removed in case of maintenance personnel on the track	Operator/maintainer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.			
H20	Infrastructure	Contact of people with powered equipment on the track	Exceptional presence of people on track	Electrocution	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_10	Linear motor on the track shall be protected by non conductive protection to avoid contact with live parts	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H21	Infrastructure	Loss of guidance	presence of ice/snow	Collision with infrastructure and deraillment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_06	Guidance system shall be equipped with a system that avoid the formation of ice/snow	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H21	Infrastructure	Loss of guidance	presence of ice/snow	Collision with infrastructure and deraillment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_15	Maintainer shall clean the track to remove the ice and snow before the start of the operation and if needed during the operation	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H22	Infrastructure	Loss of active levitation	Failure of wayside levitation system	Collision with infrastructure and deraillment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_03	The wayside active levitation system shall be equipped with emergency power supply sufficient to allow the stop of the the vehicle in case of loss of normal power. Vehicle shall be stopped in case of loss of normal power to the wayside active levitiation system.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H23	Infrastructure	Overheat of wayside magnets	Failure in winding	Fire and derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_42	Wayside linear motor shall be equipped with cooling system to maintenance the temperature of the magnent in the acceptable range	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H23	Infrastructure	Overheat of wayside magnets	Failure in winding	Fire and derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_41	Wayside linear motor (stator) shall be equipped with monitoring temperature system. If the temperature exceeds the limits, an alarm shall be sent to the vehicle to stop	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_42	On board linear motor shall be equipped with cooling system to maintenance the temperature of the magnent in the acceptable range	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Hybrid MDS mag lev.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_HyMagLev_41	On board linear motor (stator) shall be equipped with monitoring temperature system. If the temperature exceeds the limits, an alarm shall be sent to the vehicle to stop	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable				

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Annex C – Hazard Log – MDS based on Upgrade of conventional railway system

Hazard Identification							Risk Assessment									
Hazard ID	Component name	Hazard Description	Hazard causes	Accident/Danger	Type of Hybrid MDS	Initial Severity	Initial Frequency	Initial Risk	Risk Acceptance Principle	RCM ID	RCM Description	RCM Owner	Residual Severity	Residual Frequency	Residual Risk	Remarks
H01	Infrastructure	Passing point at danger	Failure of LM (insufficient brake)	Collision with the infrastructure or other vehicle; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_27	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train (e.g. two linear motor and classic train braking system)	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Vehicle	Passing point at danger	Failure of LM (insufficient brake)	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_27	The vehicle shall be quipped with two indipendent braking systems. Each of tem shall be able to stop the train (e.g. two linear motor and classic train braking system)	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	Command and control	Passing point at danger	Failure in command and control system	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_22	The command and control system shall have safety integral level 4.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H01	HF	Passing point at danger	Driver doesn't stop the train	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the operation with drivers
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_14	Maintenance vehicle shall be contoller by Automatic Train Protection (ATP) to allow safe operation with driverless passegner vehicles	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario with driverless operation
H02	command and control	Presence of maintenance vehicle not controlled by signalling system during operation with secured vehicles	Worng authorization	Collision of a technically secured maglev vehicle with non-technically secured vehicles	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_15	Operation procedure shall be implemented by operator to avoid that maintenance vehicle without APT enters in the track during the passengers sevice	Operator/maintainer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H03	Infrastructure	Too high acceleration	Failure of wrong command of the wayside propulsion control system	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_26	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is on the wayside
H03	Vehicle	Too high acceleration	Failure of wrong command of the onboard propulsion control system	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_26	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is onboard of the vehicle
H03	Energy	Too high acceleration	Overvoltage in the linear motor	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_12	Linear motor shall be equipped with over voltage protection	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard considers the scenario where the active part of the linear motor is onboard of the vehicle
H04	Infrastructure / Switches	Switch in the wrong position	Mechanical MDS turnout failure	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_06	Interlocking system shall monitor the position of the switches. The passage of the train shall be allowed only if the switches is detected on the right position.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	1. MDS system may requires new type of switches which integrate the linear motor. The linear motor can move together with the switch. 2. Physical turnout malfunction may be caused by objects blocking the points, pointing to machince defect
H04	Infrastructure / Switches	Switch in the wrong position	Movement of of the swich during the train runnig on it	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_21	Switches shall be equipped with pointlocking system to avoid mouvement during the passage of the train.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	MDS system may requires new type of switches which integrate the linear motor. The linear motor can move together with the switch.
H04	Infrastructure/Propulsion Energy/Segment	High deceleration of the vehicle due to linear motor unpowered	Power supply provided to the wrong LIM segment of the switch	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_08	Interloking system shall monitor the corrct segment supply in order to supply those in the direction of the vehicle	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Hazard can occur when in presence of a swich, the power supply is not provided to the correct segment in the direction of the vehicle.
H04	Command and control	Switch not aligned to the position required to follow the route of the vehicle	Command failure	Derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_07	Interlocking system shall monitor the position of the switches. The passage of the vehicle shall be allowed only if the switches is detected on the right position of the vehicle route.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H05	Infrastructure/levitation	Insufficient passive levitation force.	Wayside levitation device failure/ magnet wear	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_25	The vehicle shall be equipped with monitoring system of the magnetic field generated by the passive levitation system. Vehicle shall be put in safe state if the magnetic field exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard covers the case of passive levitation system on the track
H05	Vehicle/guidance	Insufficient passive levitation force.	On board levitation device failure/ magnet wear	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_29	Vehicle shall be equipped with a levitation monitoring system. Vehicle shall be put in safe state if levitation exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard covers the case of vehicle equipped with passive levitation system
H06	Infrastructure/levitation	Insufficient active levitation force.	Not correct power supply in levitation magnet	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_31	Wayside active livitation system shall be power by emergency power supply to allow the safe stop of the train in case of loss of normal power.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system on the track
H06	Infrastructure/levitation	Insufficient active levitation force.	Not correct power supply in levitation magnet	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_32	Wayside active livitation system shall be power by redundant and independent power supply sources	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	The hazard cover the case of active levitation achieved with system on the track
H07	Vehicle	Insufficient levitation force	Vehicle too heavy	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_23	The vehicle shall be equipped with a load weighing systems. The traction of the vehicle shall be inhibited if the load threshold is exceeded	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H08	Infrastructure/Propulsion Energy/Segment	Too high deceleration	Segment defect	Infrastructure, vehicle, personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_10	Linear motor shall be designed to ensure a limitation of deceleration in case of segment failure	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Hazard can occur in systems with infrastructure-controlled propulsion. For linear syncronus motors
H08	Vehicle	Too high deceleration	vehicle control	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_26	The vehicle shall be equipped with speed protection system able to prevent high acceleration and deceleration	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H08	HF	Too high deceleration	Driver's error	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers
H08	Energy/Power Supply Substation	Too high deceleration	LM power inverter failure	Collision with the infrastructure or other vehicle; derailment; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_13	Linear motor shall be supplier by redundant and independennt inverters	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	While moving at high speed
H09	Infrastructure	Infrastructure component in the gabarit	Lack of maintenance	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_16	Period inspection and maintenance of the infrastructure installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	
H11	Infrastructure/Guidance	Delay in activation of the active lateral guide	Comunication failure	Collision with infrastructure	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Code of practice	RCM_CS-wMDS_03	Communication system shall be design according to the applicable standard to ensure reliable and safe transmission of the data. Emergency braking of the vehicle shall be applied if the loss of communication exceed the fixed timout.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes
H12	Infrastructure/Guidance	Insufficent active guidance force	Power outage infrastructure (electro magnet)	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_32	Wayside active livitation system shall be power by redundant and independent power supply sources	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes due to failure of guidance active guidance system
H12	Infrastructure/Guidance	Insufficent active guidance force	Power outage infrastructure (electro magnet)	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_31	Wayside active livitation system shall be power by emergency power supply to allow the safe stop of the train in case of loss of normal power.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Systems with active guidance (electromagnets) activated when the vehicle passes due to failure of guidance active guidance system

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable

Hazard Identification							Risk Assessment										
Hazard ID	**Component name**	**Hazard Description**	**Hazard causes**	**Accident/Danger**	**Type of Hybrid MDS**	**Initial Severity**	**Initial Frequency**	**Initial Risk**	**Risk Acceptance Principle**	**RCM ID**	**RCM Description**	**RCM Owner**	**Residual Severity**	**Residual Frequency**	**Residual Risk**	**Remarks**	
H13	Infrastructure/Guidance	Insufficient passive guidance force	Magnets deterioration	Collision with infrastructure	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_25	The vehicle shall be equipped with monitoring system of the magnetic field generated by the passive levitation system. Vehicle shall be put in safe state if the magnetic field exceeds the acceptable limits	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H14	Vehicle	Vibration	Incorrect functioning of on-board levitation/guidance equipment	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_24	The vehicle shall be equipped with a vibration control system. It commands the emergency stop of the vehicle if the vibrations exceed the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H14	Infrastructure	Vibration	Incorrect functioning of on-site levitation/guidance equipment	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_24	The vehicle shall be equipped with a vibration control system. It commands the emergency stop of the vehicle if the vibrations exceed the acceptable threshold	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H15	command and control	Too high speed in curve	Incorrect functioning of on-board control	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H15	command and control	Too high speed in curve	Incorrect functioning of central control	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H15	HF	Too high speed in curve	Driver's errror	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_02	Automatic Train Protection (ATP) system shall be foreseen to react and put the system in safe state in case of driver's error	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	in case of operation with drivers	
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_04	Design and construction of the vehicle shall ensure that the components are well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H16	Vehicle	Wedging of vehicle with track/girde	Detached part from the vehicle	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_17	Period inspection and maintenance of the vehicle components shall be performed to ensure that they are well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_05	Design and construction of the vehicle shall ensure that the infrastructure installation are outside the vehicle gauge and well fixed in related to the loads and stress generated during the operation.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H16	Infrastructure	Wedging of vehicle with track/girde	Presence of detached part from infrastructure	Collision with infrastructure; derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_16	Period inspection and maintenance of the infrastracture installations shall be performed to ensure that they are outside the vehicle gauge and well fixed.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_30	Vehicle shall be equipped with object detection system. The system commands the stop of the vehicle in case of object detection. Note: this solution is not applied to high speed system.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_28	Track shall be protected with fence to avoid intrusion or introduction (voluntary and non) of objects on the track.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H17	Infrastructure	Presence of objects in clearance gauge	Lack of maintenance	Collision with system equipment in clearance gauge	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_18	Period inspection of the track shall be performed to dected and remove external objects	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H18	Infrastructure/Propulsion Energy/Segment	Erroneous activation of the propulsion system	Failure of the control center operators; failure in command and control system; error of the driver in the vehicle, if any.	collision with other vehicle	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_01	Automatic Train Protection (ATP) and Automatic Train Controller (ATC) shall be foreseen to mitigate driver or operator error.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Ground controlled propulsion system	
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Derailment, collision with the infrastructure or other vehicle; vehicle damage; personnel and passengers may be harmed	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_11	Linear motor shall be equipped with monitoring system that detects failures of segment integrity. In case of detection, an alarm shall be raised to stop the vehicle before of the failed segment.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.	
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_11	Linear motor shall be equipped with monitoring system that detects failures of segment integrity. In case of detection, an alarm shall be raised to stop the vehicle before of the failed segment.	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.	
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_20	Signalling system shall command the cut off of the power supply to the wayside linear motor to ensure a safe evacuation of the people	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.	
H19	Infrastructure/Propulsion Energy/Segment	The linear motor stator segment has broken winding	Failure of linear motor segment	Electrocution of the personnel, passengers	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_19	Procedure shall be implemented to ensure that power supply on wayside linear motor is removed in case of maintenance personnel on the track	Operator/maintainer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable	Broken winding can be caused by physical impact or electrical overvoltage. Regular means: at regular time intervals.	
H20	Infrastructure	Contact of people with powered equipment on the track	Exceptional presence of people on track	Electrocution	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_09	Linear motor on the track shall be protected by non conductive protection to avoid contact with live parts	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H23	Infrastructure	Overheat of wayside magnets	Failure in winding	Fire and derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_34	Wayside linear motor shall be equipped with cooling system to maintenance the temperature of the magnent in the acceptable range	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H23	Infrastructure	Overheat of wayside magnets	Failure in winding	Fire and derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_33	Wayside linear motor (stator) shall be equipped with monitoring temperature system. If the temperature exceeds the limits, an alarm shall be sent to the vehicle to stop	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_34	On board linear motor shall be equipped with cooling system to maintenance the temperature of the magnent in the acceptable range	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		
H23	vehicle	Overheat of onboard magnets/magnet wheels	Energization of magnet	Fire and derailment	Conventional system with MDS tec.	S5 - Catastrophic	See note (1) under the table	Intolerable	Explict Risk Estimation	RCM_CS-wMDS_33	On board linear motor (stator) shall be equipped with monitoring temperature system. If the temperature exceeds the limits, an alarm shall be sent to the vehicle to stop	System designer	S5 - Catastrophic	F7 - Higly Improbable	Tolerable		

(1) the frequencies of hazards, before the implementation any risk control measures, has considered greater than 10-9 and, consequently, make all the risks examined unacceptable