SAtellite-based Signalling and Automation SysTems
on Railways along with Formal Method and Moving Block validation

D2.2 - Moving Block signalling system Hazard Analysis

Deliverable ID	**D2.2**
Deliverable Title	**Moving Block signalling system Hazard Analysis**
Work Package	**WP2**
Dissemination Level	**PUBLIC**
Version	**2.0**
Date	**2019-01-28**
Status	**Released**
Lead Editor	**ARD**
Main Contributors	**SIRTI, CNR**

Published by the ASTRAIL Consortium

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 777561
Call identifier: H2020-S2RJU-2017 | Topic: S2R-OC-IP2-01-2017 – Operational conditions of the signalling and automation systems; signalling system hazard analysis and GNSS SIS characterization along with Formal Method application in railway field

Document History

Version	Date	Author(s)	Description
0.1	2018-01-03	ARD	First Draft with TOC
0.2	2018-01-23	SIRTI, CNR	Revision of ToC and Chapters 1, 2, 3.
0.3	2018-01-25	ARD	Development of the Chapters 1, 2, 3. Corrections of the commentaries.
0.4	2018-02-13	CNR	Chapter 5 Application of formal methods to formalise safety requirements
0.5	2018-02-27	ISMB	Overall revision and commentaries
1.0	2018-02-28	ARD	Finalization and release of the deliverable
1.1	2018-06-01	ISMB	Added legal notice
1.2	2019-01-16	ARD, SIRTI	Correction of reviewer commentaries.
2.0	2019-01-28	ARD	Version release

Legal Notice

The information in this document is subject to change without notice.
The Members of the ASTRail Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the ASTRail Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.
The Shift2Rail JU cannot be held liable for any damage caused by the Members of the ASTRail Consortium or to third parties as a consequence of implementing this Grant Agreement No 777561, including for gross negligence.
The Shift2Rail JU cannot be held liable for any damage caused by any of the beneficiaries or third parties involved in this action, as a consequence of implementing this Grant Agreement No 777561.
The information included in this report reflects only the authors' view and the Shift2Rail JU is not responsible for any use that may be made of such information.

Table of Contents

1 Introduction

1.1 Background

The present document constituted the second deliverable (D2.2) of the WP2 "Safety analysis of Moving block signalling system" – in the framework of the project ASTRail, which is a Shift2Rail project complementary to X2Rail-1 and X2Rail-2.
ASTRail focuses on the following four workstreams:
1) Transfer the knowledge of aeronautical standard and existing integrity monitoring solutions to the application of fail-safe moving block location by performing an assessment of local error modelling, hazard analysis and verification activities before proposing minimum performance standards for such equipment for use in the rail domain;
2) Perform Hazard Analysis of the railway system examining safety level of Moving Block Signalling System operating without trackside detection, from technical and operational point of view, along with the hazard identification in the most significant operative conditions defined by the use cases;
3) Identify the most suitable technologies to be implemented in the railway field for performing automated driving;
4) Based on the state of the art, on the past experiences of the partners and on ad-hoc experiments, it will identify the most promising formal and semi-formal methods for the different development phases of railway equipment, and, particularly, for the signalling solutions targeted by ASTRail.

The WP2 and the D2.2 correspond to the second work-stream focuses safety and security analysis of the Moving Block system in view of complete removal of trackside detection. This work stream contributes to the X2Rail-1 WP5 "Moving Block" that aims to define a high capacity, low cost, high reliability signalling system, based on Moving Block principles, which is applicable across all railway market segments. High Capacity is based on the use of Moving Block principles, which permits decoupling of the infrastructure from train performance parameters. Low Cost is achieved by the reduction in the use of trackside train detection and line-side signals. High Reliability is achieved as a consequence of the reduction in trackside equipment associated with trackside train detection and line-side signals.

The D2.2 is an output of the Tasks 2.3 "Hazard identification and risk analysis and evaluation" and the Task 2.4 "Safety Related Application Conditions for operational procedures".
The results of the previous work done during the implementation of the Task 2.1 "Modelling of the moving block signalling system" and the Task 2.2 "Definition of the system use cases" that are documented in the D2.1 will serve as a base for the Moving Block signalling system safety analysis.

Also, the inputs from ASTRail WP1 "Introducing GNSS technology in the railway sector" and WP3 "Automatic driving technologies for railways" will be considered during the preparation of the deliverable.

1.2 Purpose and Scope

The present deliverable responds to the following objectives:

1) To identify hazards derived from possible system errors and faulty states in main operative conditions.
2) To assess the resulting risk level derived from identified hazards (risk qualifying);
3) To evaluate resulting safety level of a Moving Block signalling system operating without trackside train detection;
4) To define Safety Related Application Conditions (operational procedures to be applied in normal or degraded conditions, according to GoAx, operational maintenance activities).

The safety assessment of a Moving Block signalling system will consist in identification of hazards assigned to each safety function of the system, derived from GNSS relative errors (the input from the Task 1.3 will be considered), communication failure in main system interfaces and random and systematic failure of principal components of the system. The identified hazard will then be analysed, and so the risks associated with these hazards will be evaluated.

The inductive method (e.g. What If method) will be principally used for Hazard identification. The probability of occurrence and severity of the consequence as well as the final risk evaluation will be qualified according to

EN 50126 guidance ([1], [2]). These activities will allow to conclude about overall Safety level of the Moving Block signalling system in view of complete removal of trackside detection.

The analysis of the hazards and resulting risk will include the definition of the operational procedures and rules to apply in different use cases with the aim to avoid hazards or, at least, reduce the risk (T2.4).
The determination of the operational rules and procedures will be based on analysing the existing operational rules regarding ERTMS system and its fall-back modes, and regarding GoA of the system. The applicability of the existing operational rules for ERTMS level 3 signalling system without trackside detection will be examined, in these terms the gaps in operational procedures will be detected.
Being the degraded and emergency situations the critical point for moving block signalling system application, the special attention will be paid to the allocation of the responsibility to the driver.
The particular aspects of management of ordinary and extraordinary maintenance activities for ERTMS L3 conditions will be analysed. The procedures necessary to assure that the maintenance activities are carried out without endangering safety will be defined.

Moreover, the identified during Hazard analysis safety requirements will be mapped to formal properties to be used in the WP4 for moving block model validation.

The validation process for the Hazard Analysis results includes participation of external to project experts that form part of ASTRail Advisory Board. The feedback received from then after the deliverables revision and during Advisory Board meeting will be collected and included in the deliverable revision at M19 (March 2019).

1.3 Related documents

ID	Title	Reference	Version	Date
[RD.1]	D2.1 Modelling of the moving block signalling system	D2.1 ASTRAIL_MBSS Modelling _v1.0	1.0	2018-11-29
[RD.2]	Reserved			
[RD.3]	Reserved			

2 Hazard- analysis methodology

2.1 Moving block signalling system

Moving block system high level architecture and principal components are depicted in the following scheme:

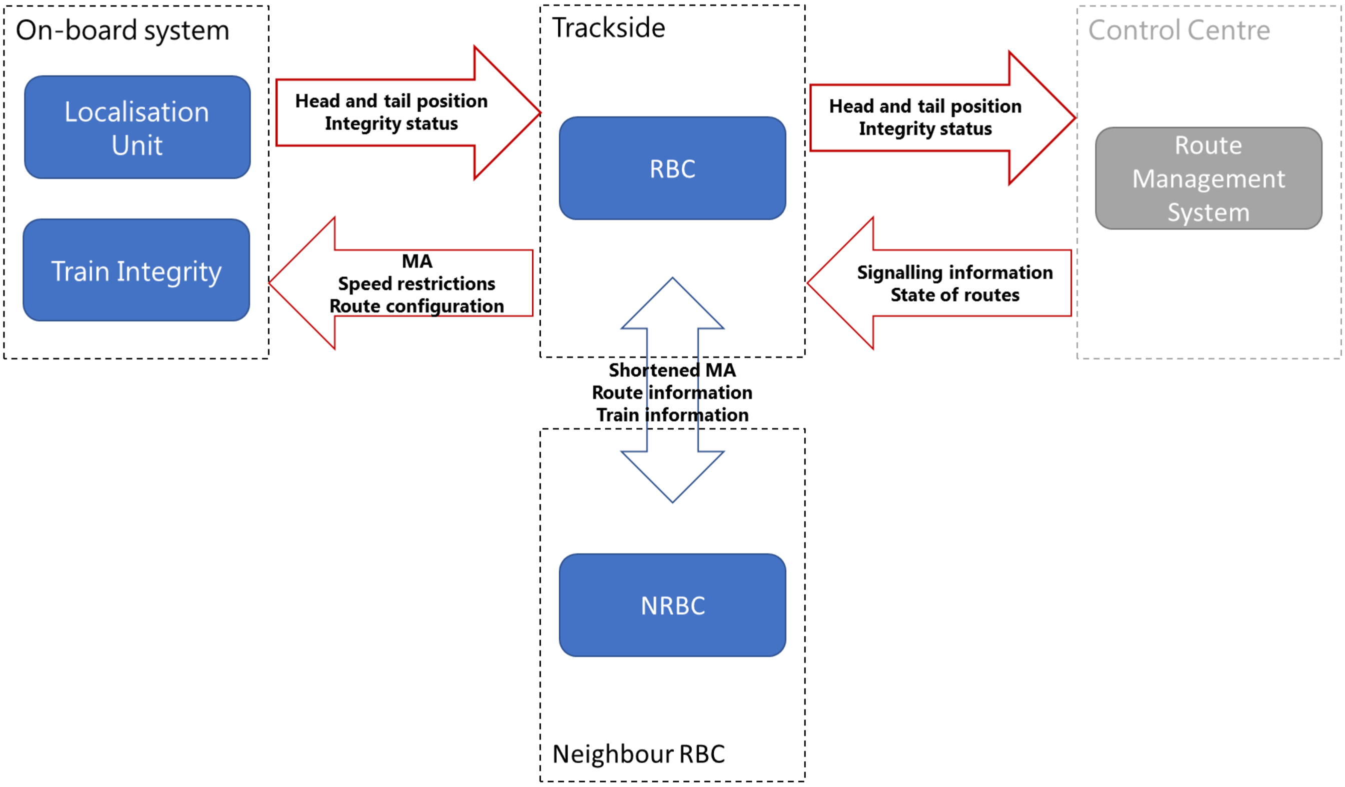

Figure 1. Moving block diagram

Moving Block signalling system without trackside detection, object of this deliverable, consists in the following main components:

- Radio Block Centre (RBC);
- On-board equipment:
  - Location Unit (GNSS based positioning system based on Virtual Balise principle);
  - Train Integrity;
- Radio communications Train – Trackside;
- Route Management System (e.g. Interlocking).

The MBS system is based on continuous communication of variable data between RBC and the trains via radio communications system.

The RBC supports simultaneous open channel communication to all the trains within its controlled area, being vital safety SIL4 equipment. The RBC receive from on-board system the data regarding train position and train integrity status, including the alarms. The on-board system obtains these data from Location Unit and Train Integrity device through the internal interfaces.

The route related information (RRI) is provided to RBC by Route Management System (RMS), this information includes, but not limited to the position of switches and route status. This information is made available for trains via RBC – on-board interface.

The RBC communicates to any adjacent RBC and manage RBC/RBC handover, ref. [8].

The main interfaces of the MBS system are:

- RMS <-> RBC,
- On-board <-> RBC, ref. [10]
- RBC <-> NRBC, ref. [9]
- Localisation Unit <-> GNSS/GPS satellites

The RMS and the- interface between RMS and RBC are out of the scope of this analysis, only the RBC safety functions derived from the interchange of the data will be considered.
The interface between Localisation Unit and satellites (SIS), as well as the safety issues derived it, are covered in ASTRail WP1 (particularly, hazard analysis is provided in the Deliverable 1.3).

2.2 Safety functions identification (Top- down analysis)

To provide a base for the complete Hazard analysis of the system, it is necessary to identify system Safety functions, since the analysis will define the hazards that prevent from complying these safety functions.

The process of the definition of main safety function follows the scheme presented in the Figure 2, according to it, it is necessary to forecast the hazardous scenarios that could lead to the railway accidents and then derive from these scenarios the conditions in which they could happen and the functions that allows to avoid these events.

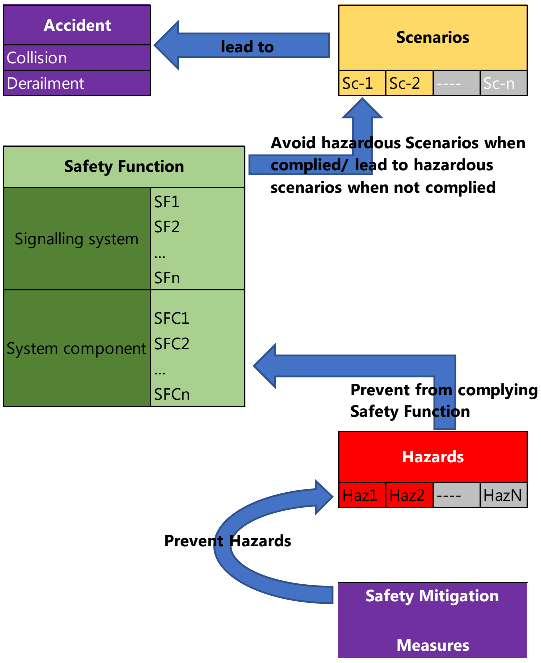

Figure 2. Method for MBS Safety function identification

2.3 Preliminary Hazard Analysis

The Preliminary Hazard analysis (PHA) is a technique that is adequate in the earlier stages of the project and it is based on the system specifications.

The methodology that is used to perform PHA can be:

- Inductive: Reasoning that consists in inserting failures in a system and analysing its consequences.
- Deductive: Reasoning that consists in analysing an accident to define its possible causes and by this way identify the protections that can be applied to avoid the occurrence of those causes.

For the MBS system analysis the combination of both methodologies is applied, a deductive methodology is used for the definition of the main system safety functions (Section 3), and the inductive analysis will be used to identify the hazards that could prevent system from complying its functions, as shown in the following figure:

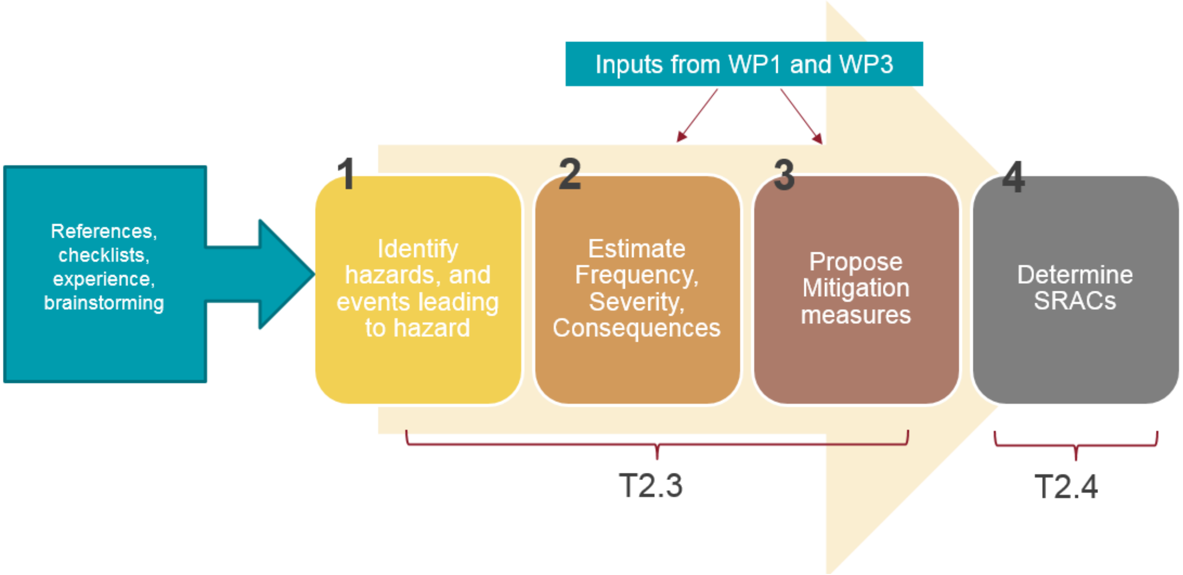
Inputs from WP1 and WP3
References, checklists, experience, brainstorming
1
Identify hazards, and events leading to hazard
2
Estimate Frequency, Severity, Consequences
3
Propose Mitigation measures
4
Determine SRACs
T2.3
T2.4

Figure 3. Hazard Analysis process

The hazards identified during PHA and the associated protections shall be collected to prepare a first version of the Hazard Log.

2.3.1 Risk evaluation

2.3.1.1 Qualitative Risk Assessment

Qualitative risk assessment involves a formal judgement on the consequence and probability using:

Risk = Severity x Likelihood

In the case it is likely that detected functional failure can have catastrophic consequences, the associated risk should not be reduced further if the rate of occurrence of such failure is equal to or less than 10^{-9} per operating hour (ref. [11]).

2.3.1.2 Risk classification

The concept of “risk” is the combination of the following 2 parameters:

- The probability of occurrence of an event or combination of events leading to a hazard, or the frequency of such occurrences;
- The severity of the consequence of a hazard, taking into account its effects on human beings, materials and environment.

The probability of occurrence of a hazardous event can be divided in 6 categories according to EN50126 (4.6.2):

Id	Category	Frequency (per hour/train)	Description
A	Frequent	$>10^{-3}$	Likely to occur frequently. The hazard will be continually experienced.
B	Probable	$<10^{-3}-10^{-5}$	Will occur several times. The hazard can be expected to occur often.
C	Occasional	$<10^{-5}-10^{-7}$	Likely to occur several times. The hazard can be expected to occur several times.
D	Remote	$<10^{-7}-10^{-9}$	Likely to occur sometime in the system life cycle. The hazard can reasonably expect to occur.
E	Improbable	$<10^{-9}-10^{-10}$	Unlikely to occur but possible. It can be assumed that the hazard may exceptionally occur.
F	Incredible	$<10^{-10}$	Extremely unlikely to occur. It can be assumed that the hazard may not occur.

Table 1. Categories of probability of a hazardous event

The severity level of a hazard can be classified as follows according to EN50126 (4.6.2):

Id	Severity Level	Consequence to Person or Environment	Consequence to Service
1	Catastrophic	Fatalities and/or multiple severe injuries and/or major damage to the environment.	Not applicable
2	Critical	Single fatality and/or severe injury and/or significant damage to the environment	Loss of a major system
3	Marginal	Minor injury and/or significant threat to the environment	Severe system(s) damage
4	Insignificant	Possible minor injury	Minor system damage

Table 2. Hazardous event severity levels

2.3.1.3 Risk evaluation and control

The risk evaluation is performed by combining the frequency of occurrence of a hazardous event with the severity of its consequence, as shown in the following matrix (EN50126):

Frequency	***RISK LEVELS***			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable

Remote	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Tolerable
Incredible	Negligible	Negligible	Negligible	Negligible
	Insignificant	**Marginal**	**Critical**	**Catastrophic**
	Severity Level			

Table 3. Risk evaluation

The management of the risks according to the corresponding evaluation will be performed as follows (EN50126):

Risk Levels	Abbreviation	Definition
Intolerable	IT	Shall be eliminated
Undesirable	UD	Shall only be accepted when risk reduction is impracticable and with the agreement of the Railway Authority
Tolerable	TO	Acceptable with adequate control and the agreement of the Railway Authority
Negligible	NE	Acceptable without any agreement

Table 4. Risk management

2.3.2 Interface hazard analysis

The Interface hazard analysis (IHA) aims to identify hazards derived from the interaction between subsystems of the MBS system through their interfaces.

In this case, the interface hazard can be defined as a hazard in which one subsystem affects negatively another subsystem by transferring a failure or partial performance over a defined interface or including through another subsystem.

This dependency can result in a failure in one subsystem causing a critical fault in another. Nevertheless, the types of failures which can be transferred are limited by the interfaces between systems.

The interfaces defined for MBS system consists in communications system between the following components:

- RMS <-> RBC,
- OBU <-> RBC,
- RBC <-> NRBC.

The interaction between these components is depicted thorough the Message Sequence Charts (MSC) in the Annex 1 of the D2.1 Modelling of the moving block signalling system.

2.3.3 Identification of hazards related to transmission system

The effects of message errors on the functions where GNSS is involved can be analysed with regards to the error in:

- a single message,
- the communication stream between two functions,
- all communication in a system

In the safety analysis errors of location function (wrong reference location in position reports and MAs) and errors of odometry (measurement of space and speed) are considered separately.
Note that GNSS can be a cause of both (e.g reading of a wrong reference location, real accuracy greater than the estimated one, etc.)

CENELEC EN50159 [7] identifies the following basic message errors as threats to the transmission system.

Corruption: it means that the information received (and accepted by the receiving functions after checks made by communication protocols) is not the correct one. This error can be generated by errors of “sensors”, failures in evaluation function, communication errors.

Delay: it means that the information is received later than planned. This can be due to delayed information from sensors, delays in processing or delay in communication channel. Using GNSS to detect reference location and without linking information, delay should also cover the case of a location detected “after the correct position”.

Deletion: it means that information is not received. This can be due to missing input from sensors, failures in processing or interruption of the communication channel.

Resequencing: it means that a message arrives before or after another one, according to the planned sequence of transmission.

Repetition: it means that the same information is received more than one. The dangerous situation can occur if data no longer valid is received and accepted. This is the same case as for delay; for this reason it is not necessary to investigate separately the case of repetition.

Insertion: it means a piece of information not intended for the receiver, because of unintentional failures. This includes the GNSS error causing the reading of a location in a wrong place, i.e. the equivalent of cross talk between Eurobalises (insertion of a not planned message in the stream of information). Cross talk can be either “transversal” (GNSS locates the train on a adjacent track) or “longitudinal” (a location is detected before of after the correct position).

Masquerade: it means a piece of information not intended for the receiver, because of intentional attacks. This includes the same s for insertion, but because of intentional attacks.

These threats to the transmission system can be caused by the hazardous events that EN50159 lists in table A.1, hereafter reported in Table 5.

Hazardous events	Threats						
	Repetition	Deletion	Insertion	Re-sequencing	Corruption	Delay	Masquerade
HW systematic failure	X	X	X	X	X	X	
SW systematic failure	X	X	X	X	X	X	
Cross-talk		X	X		X		
Wires breaking		X			X	X	

Hazardous events	Threats						
	Repetition	Deletion	Insertion	Re-sequencing	Corruption	Delay	Masquerade
Antenna misalignment		X			X		
Cabling errors		X	X		X	X	
HW random failures	X	X	X	X	X	X	
HW ageing	X	X	X	X	X	X	
Use of uncalibrated instruments	X	X	X	X	X	X	
Use of unsuitable instruments	X	X	X	X	X	X	
Incorrect HW replacement	X	X	X	X	X	X	
Fading effects		X		X	X	X	
EMI		X			X		
Human mistakes	X	X	X	X	X	X	
Thermal noise		X			X		
Magnetic storm		X			X	X	
Fire		X			X	X	
Earthquake		X			X	X	
Lightning		X			X	X	
Overloading of TX system		X				X	
Wire tapping	X	X	X	X	X	X	
HW damage or breaking		X		X	X	X	
Unauthorised SW modifications	X	X	X	X	X	X	X(a)
Transmission of unauthorised messages	X		X				X(a)
Monitoring of channels (b)							

(a) In this case the message is fraudulent from the beginning; a strong defence is needed, for example the use of a key.

(b) Unauthorised monitoring of SR messages is not considered to be a directly hazardous event; the hazard to system safety arises from "transmission of unauthorised messages" resulting from unauthorised monitoring. Confidentiality of application data is a separate system requirement outside the scope of this standard.

Table 5. Relationship between hazardous events and threats (Table A.1 EN 50159:2010)

According to EN50159 we have to consider the threats related to the hazardous events – not protected by other means – that can occur for the system.

The threats can be analysed, taking into account the following items related to safety:

- existing mitigations / barriers: they refer to circumstantial conditions, typical for the rail system and independent of the installation and functionality of a train protection system (conditions "before" installation of train protection);

- actions: they refer to functionality to be installed and related performance (like SIL of the train protection functions), checks to be performed by communication protocols, etc (this item contains the principle to specify safety functional requirements for the use of GNSS in moving block systems);
- probability and risk: they are estimated after the existing mitigations and before the installation of functions indicated in actions. It is intended that the implementation of actions should reduce the risk at acceptable level.

3 Safety functions

3.1 Top-down analysis

To deduce safety functions of the moving block signalling system is necessary to consider that the main function of any signalling system is to avoid the possible accidents.
The most common type of accidents that can occur in the railway operation, related to the circulations of trains, are:

Collisions

- Head-on collision
- Rear collision
- Side collision (gauge factor)
- Collisions with buffer stops
- Collisions with obstructions on track

Derailments

- Plain track
- Curves
- Junctions

It shall be noted that some collision may be accompanied with derailment also. To analyse the hazardous situation that could lead to this type of accidents, it is necessary to foresee the possible scenarios in which the specific conditions are met to cause the accident. These scenarios are related to the signalling system area of responsibility:

Scenarios leading to Collision:

1. Coincidence of two vehicles on the same route (head-on collision, rear collision).
2. Invasion of a secured route by another vehicle (head-on collision, rear collision, side collision).
3. Two different routes include the same track element (head-on collision, rear collision, side collision).
4. Collision with fix track elements (Collisions with buffer stops and decoupled wagons).

Scenarios leading to Derailment:

4. Collision with objects on track.
5. The train traveling at excessive speed.
6. Pass over track elements susceptible to alter the route (switches).

Note: the term “route” in this case is referred to a section of track which cover the distance between the initial train position (when it is granted with MA) and the EOA. This section could contain the following field elements: junctions, switches, level crossings, signals, etc. It is understood that the train receives MA, its route is considered being “set”. Currently, the system responsible for setting the route is the Interlocking system which shall provide the information of the route state to RBC.

Intentionally excluded scenarios: The scenarios that correspond to level crossing situation and the accidents related to collisions with pedestrians and other type of vehicles (car, trolleys, buses, etc.) are intentionally left out of this analysis, since the necessary protection shall be managed by level crossing protection systems. Collisions with unforeseen obstructions on track (e.g. rocks on the tunnel entrance) scenario has been excluded from the present analysis since it shall be managed by own protection system (obstacles detection).

3.2 Safety functions of the moving block signalling system

Once the scenarios that could lead to the accidents have been defined, signalling system Safety Functions can be derived:

Scenario	System Safety Function (SF)
1. Coincidence of two vehicles on the same route in the same direction (rear collision) and in the opposite direction (head-on collision).	SF1 Prevent establishing of the same route for different trains in opposite directions. SF2 Manage safely the presence of two trains on the same route.
2. Invasion of a secured route by another vehicle (rear collision, side collision).	SF3 Foresee a safe distance and time to Supervised locations.
3. Two different routes include the same track element (side collision).	SF4 Prevent the use of a single-track element by two different trains in the same space of time.
4. Collision with objects on track (Collisions with buffer stops and decoupled wagons).	SF5 Supervise the conditions under which a train must circulate when approaching a buffer stop. SF6 Supervise train integrity.
5. The train traveling at excessive speed (overpassing switches or zones with permanent / temporary speed restrictions).	SF7 Implement protection systems to ensure that temporary and permanent speed limitations are respected.
6. Pass over track elements susceptible to alter the route (switches).	SF8 Ensure the track element state is known before authorizing the circulation.

Table 6. System Safety functions

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
SF1 Prevent establishing of the same route for different trains in opposite directions	Signalling: Do not allow two trains movement in the same section in the same time in the opposite directions	SIL4	RBC	SFSC 06 Receive signalling-related information and state of the routes
				SFSC 12 Send to train the information about the state of the route
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports
			Train integrity	SFSC 01 Detect and send to OBU the train integrity status
SF2 Manage safely the presence of two trains on the same route	Signalling: To assure the safe distance between trains	SIL 4	RBC	SFSC 09 Receive train head and tail position
				SFSC 06 Receive signalling-related information and state of the routes
				SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train
				SFSC 11 Inform Control Centre of alarms received
				SFSC 13 Receive alarms when train integrity is not confirmed
				SFSC 18 Inform the trains of the alarms received
				SFSC 08 Maintain safe headway distance

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
				SFCS 14 Manage the train integrity data of entire network
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 04 Send an alarm to RBC if train integrity is not confirmed
				SFSC 10 Send to RBC position reports
			Train integrity	SFSC 01 Detect and send to OBU the train integrity status
SF3 Foresee a safe distance and time to Supervised positions	Signalling: to consider the status of the track elements when establishing LoA and EoA	SIL 4	RBC	SFSC 09 Receive train head and tail position
				SFSC 05 Send train head and tail position to RMS
				SFSC 06 Receive signalling-related information and state of the routes
				SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train
				SFCS 14 Manage the train integrity data of entire network
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
				SFCS 15 Manage circulation restrictions in SH mode
				SFCS 16 Manage circulation restrictions in OS mode
				SFCS 17 Manage circulation restrictions in SR mode
				SFCS 20 Supervise ceiling speed
SF4 Prevent the use of a single-track element by two different trains in the same space of time	Signalling: To check the state of a single-track apparatus before MA emission.	SIL 4	RBC	SFSC 06 Receive signalling-related information and state of the routes
				SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train
				SFSC 09 Receive train head and tail position
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports
			Train integrity	SFSC 01 Detect and send to OBU the train integrity status
SF5 Supervise the conditions under which a train must circulate when approaching a buffer stop.	Signalling: to allow approaching to a buffer stop in a shunting mode only	SIL4	RBC	SFSC 06 Receive signalling-related information and state of the routes
				SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
				SFSC 09 Receive train head and tail position
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports
				SFCS 15 Manage circulation restrictions in SH mode
SF6 Supervise train integrity.	Signalling: To supervise continuously the train integrity and to manage safely the situations when train integrity is not confirmed.	SIL4	RBC	SFSC 05 Send train head and tail position to RMS
				SFCS 18 Inform the trains of the alarms received
				SFSC 11 Inform Control Centre of alarms received
				SFSC 18 Inform the trains of the alarms received
				SFSC 13 Receive alarms when train integrity is not confirmed
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 04 Send an alarm to RBC if train integrity is not confirmed
			OBU	SFSC 10 Send to RBC position reports
			Train integrity	SFSC 01 Detect and send to OBU the train integrity status

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
SF7 Implement automatic protection systems to ensure that temporary and permanent speed limitations are respected.	Signalling: to manage the permanent speed restrictions and to prevent the entering of trains over not allowed tracks (due to temporary works or infrastructure problems).	SIL4	RBC	SFSC 04 Send an alarm to RBC if train integrity is not confirmed
				SFSC 19 Send the information about existing speed restrictions to the train
				SFSC 06 Receive signalling-related information and state of the routes
				SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train
				SFSC 09 Receive train head and tail position
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports
				SFCS 15 Manage circulation restrictions in SH mode
				SFCS 16 Manage circulation restrictions in OS mode
				SFCS 17 Manage circulation restrictions in SR mode
				SFCS 20 Supervise ceiling speed
SF8 Ensure the elements composing each route are		SIL4	RBC	SFSC 06 Receive signalling-related information and state of the routes

Safety function	Description	Safety Integrity Level	Component	Component Safety Function
locked in correct position before authorizing its circulation.	Signalling: to verify that the status of the trackside equipment is known before MA emission.			SFSC 07 Calculate the MA
				SFSC 02 Send the movement authority to the train
				SFSC 09 Receive train head and tail position
			Location unit	SFSC 03 Detect and send to OBU the train position
			OBU	SFSC 10 Send to RBC position reports

Table 7. Component Safety Functions

In the table below the resume of identified component functions is presented.

ID	Component	Safety Function
SFSC 01	Train Integrity	Detect and send to OBU the train integrity status
SFSC 02	RBC	Send the MA to the train
SFSC 03	Location Unit	Detect and send to OBU the train position
SFSC 04	OBU	Send an alarm to RBC if train integrity is not confirmed
SFSC 05	RBC	Send train head and tail position to RMS
SFSC 06	RBC	Receive signalling-related information and state of the routes
SFSC 07	RBC	Calculate the MA
SFSC 08	RBC	Maintain safe headway distance
SFSC 09	RBC	Receive train head and tail position
SFSC 10	OBU	Send to RBC position reports
SFSC 11	RBC	Inform Control Centre of alarms received
SFSC 12	RBC	Send to train the information about the state of the route
SFSC 13	RBC	Receive alarms when train integrity is not confirmed
SFSC 14	RBC	Manage the train integrity data of entire network
SFSC 15	OBU	Manage circulation restrictions in SH mode
SFSC 16	OBU	Manage circulation restrictions in OS mode
SFSC 17	OBU	Manage circulation restrictions in SR mode
SFSC 18	RBC	Inform the trains of the alarms received
SFSC 19	RBC	Send the information about existing speed restrictions to the train
SFSC 20	OBU	Supervise ceiling speed

Table 8. Component Safety functions

4 Inductive Hazard Analysis

4.1 Hazard Log

The Hazard Log is the evolving safety document that is modified and updated continuously to assure the traceability of the hazards, safety requirements and mitigation measures. Each time that a hazard is identified, it is registered in the Hazard Log. It contains all the subjects related to safety, having a structure as indicated in the following figure:

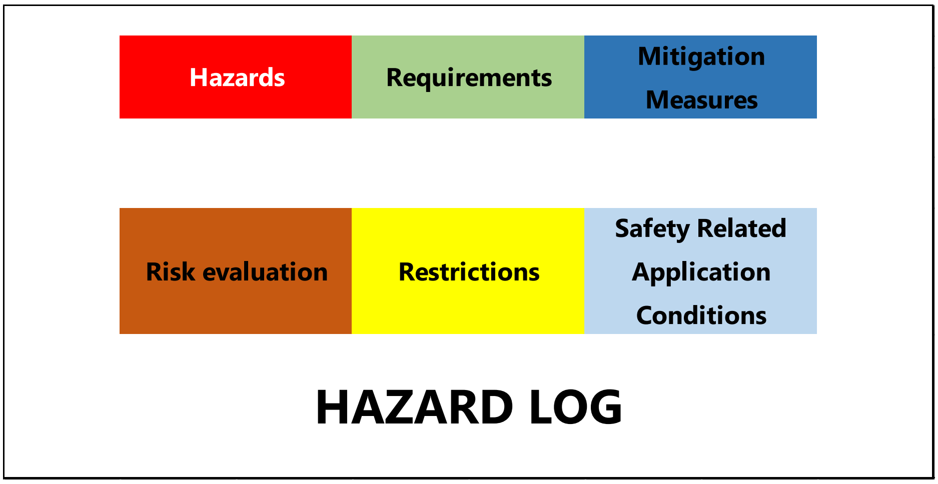

Figure 4. Hazard Log structure

The hazards identified during the PHA and so the risk deduced are registered and pondered in Hazard Log. The proposed mitigations measures, their justification, derived requirements, and SRACs are also recorded.

Hazard Log will be elaborated and presented in form of a table. The top of the table includes the following items:

- *ID*: Hazard Identification that allows the proper traceability of the detected hazards;
- *Hazard description*: describes the conditions and properties of detected hazards;
- *Safety Function*: Safety function of the system related to the identified hazard and/or mitigation measure and SRACs.
- *Consequences*: describes the consequences of the detected hazard occurrence;
- *Cause:* describes the causes of the detected hazard occurrence
- Requirement:
  - *ID*: Requirement Identification that allows the proper traceability;
  - *Description*: the required actions to mitigate the hazard.
- *Initial Risk:* Assessment of the risk level before application of the mitigation measures (see 2.3.1).
- *Mitigation measure:* The actions that have to be taken in order to implement the necessary mitigation measures where can be defined.
- *Formal Property:* a property of the model derived from the Requirement that could be verified applying formal methods (Chapter 0), where applicable.
- *Residual Risk:* Assessment of the risk level after the application of the mitigation measures.
- *Responsible for mitigation*
  - *Design*: the necessary mitigation activities has been implemented during the Design stage being the Design team the responsible for the implementation of the measures. When the Design are completed and verified the Hazard can be closed.
  - *Verification activities on field*: this type of activities shall be carried out during Works execution phase verifying that the measures forecasted in the Design phase are being

implementing properly being Verification team the responsible for the implementation of the measures. Hazard cannot be closed at the Design phase.

    - *Operation*: the mitigation measure shall be carried out by the Railway Operator during the operation phase.
    - *Maintenance*: requirement regarding Maintenance phase of the installation being Maintainer the responsible for the implementation of the measures.
- *Comments:* Additional information about pending actions, references and exported hazards.

The Hazard Log that has been opened and updated as the consequence of Preliminary Hazard Analysis, is included in the Annex A of the present deliverable.

5 Operation and maintenace procedures for Moving Block system

5.1 Maintenance procedures

Maintenance conditions contribute to define the ERTMS mission profile. The reference maintenance conditions have to be identified in order to allow operational and/or technical interoperability. For instance, CCS TSI indicates that to satisfy interoperability requirements an adequate availability of spare parts for ERTMS equipped foreign trains has to be ensured by each national maintenance system for ERTMS equipped lines.

We'd like also to point out that level 3 ERTMS equipped line transfers some maintenance activity from track infrastructure to trains: the absence of track circuit simplifies the maintenance for the track infrastructure, but on the other hand we have more equipment for the signalling on the train.

For this reason, the infrastructure manager and the managers of the railway undertakings have to consider the different impact on the maintenance procedures of the transformation to the level 3 of an existing ERTMS equipped line.

The maintenance procedures for a track with ERTMS lev.3 have to take into account the absence, along the line, of train detection devices and other related equipment to be maintained.

The introduction on the trains of the new equipment dedicated to GNSS imply the revision of maintenance files, in order to verify the maintenance requirements. The maintenance procedures for the trains, that are equipped with a GNSS receiver, have to consider the more complex equipment on board, that could introduce, at first glance, extra down time in case of failures.

The ERTMS level 3 doesn't allows generally the presence on the track of vehicles that are not equipped with ERTMS level 3. This fact has important consequences when a main failure makes the train a "ghost" for the center or the train is no longer able to evaluate its position. In these cases, suitable procedures have to be defined for vehicle recovery and restart of operation.

An important aspect of the level 3 ERTMS are the maintenance procedures that the manager of the infrastructure has to follow, for instance to access to the track for maintenance reason during railway traffic, considering the high frequency of the trains.

Due to the frequency of the traffic in the line equipped with level 3 ERTMS, we can exclude ordinary maintenance of the track infrastructure during normal operation of the trains.

Anyway, further analysis is necessary about track maintenance with train traffic interruption during night operation. In this case, vehicles that are not equipped with ERTMS level 3 equipment could be present on the track and accurate procedures have to be followed for traffic reactivation.

For exceptional maintenance we could access the track during operation of the trains: in this case the procedures can only consider the use of maintenance or recovery vehicles that are equipped with level 3 ERTMS, and therefore also GNSS receivers.

5.2 Operation procedures

The hazards associated to specific operational procedures derived from four Use Cases defined in the deliverable D2.1 is analysed in the present section.

This analysis is separated from the Preliminary Hazard Analysis since the mitigation measures applicable are out of scope of ERTMS/ETCS system (technical mitigation is not possible).

Specific attention is paid to Driver/ATO functions. If the functions required from ATO system are safety -related the applicable SIL level is estimated, based on the formula:

$$SIL = \frac{S}{E \times A \times C}$$

Where:

S- severity of consequences:
Catastrophic THR = 10^{-9}/h
Critical THR = 10^{-8}/h
Marginal THR = 10^{-7}/h
Insignificant THR = 10^{-6}/h

E- Exposure of members:
Frequent E = 1
Rare E = 0.1
Very rare E = 0.01

A- Accident probability reduction:
No barrier A = 1
One barrier A = 0.1
Two barriers A=0.01

C- Consequence reduction:
No barrier C = 1
One barrier C = 0.1
Two barriers C = 0.01

S- Safety Integrity Level:
THR = 10^{-9}/h - 10^{-8}/h → SIL 4
THR = 10^{-8}/h - 10^{-7}/h → SIL 3
THR = 10^{-7}/h - 10^{-6}/h → SIL 2
THR = 10^{-6}/h - 10^{-5}/h→ SIL 1

It should be highlighted that ATO safety-related functions are applicable only when there is no trackside detection available.

5.2.1 Use Case 1 Start of Mission when the train position is valid

The Use Case 1 Start of Mission corresponds to following conditions:

- The position is acquired correctly from location unit (optionally, it corresponds to the stored data);
- Train integrity is confirmed;
- Communication session with RBC is correctly set;
- Train information is correct.

Traffic type and density	System states		Grade of Automation	Environmental conditions
Railway profile	**Mode of operation**	**Operational conditions**		
High density lines High speed lines Medium density lines Low density lines Regional lines	Normal operation	The train knows its location and is able to report. .	GoA1 GoA2 GoA3 GoA4	Open Sky Environment

Table 9 - External conditions considered in the Use Case 1

The Use Case 1 is suitable for each railway profile and corresponds to the normal operation where train position is valid and GNSS has required availability (LoS).

Driver/ATO functions, external to ERTMS/ETCS:

- The driver/ATO switches on the ERTMS equipment and shall check the clearance in front of the train before, since there can potentially be another standstill train in SB mode that has not yet started the mission and for this reason “invisible” for RBC (in absence of trackside detection).
- In GoA 3 and 4 level, obstacle detection function is required, and it is safety related, nevertheless the required level of performance is low (distance of hundreds of meters at standstill).

Hazards introduced by trackside detection removal:

1. Coincidence of two trains in the same route in SB mode waiting for SoM and MA from RBC.
2. Wrong detection of train direction.

Operational Hazard	Consequence	Probability	Safety barrier/ Probability reduction	Required SIL
OPH-1: Coincidence of two trains in the same route in SB mode waiting for MA from RBC	Collision	Probable in high – density lines Occasional in medium density lines Remote in low density lines	No barrier is assumed	ATO (GoA3 and 4) shall check track clearance ahead during the SoM procedure **High and Medium density SIL3** **Low density SIL2**

	Severity= Critical
	THR = 10^{-8}/h
		High and Medium density E=1
		Low density E=0.1
			A=1	

OPH-2 Wrong detection of train direction Covered in PHA (OBU-LU-7)	-	-	-	-

Table 10- Use Case 1 Operational Hazards

5.2.2 Use Case 2 Start of Mission when the train position is invalid/ unknown

The Use Case 2 Start of Mission corresponds to the case when the system is not performing correctly with the following conditions:

- The position cannot be acquired from location unit (erroneous or unavailable position) or/and cold movement detection has not occurred;
- Train integrity is confirmed;
- Communication session with RBC is correctly set;
- Train information is correct.

Traffic type and density	System states		Grade of Automation	Environmental conditions
Railway profile	**Mode of operation**	**Operational conditions**		
High density lines High speed lines Medium density lines Low density lines Regional lines	Degraded operation	The train doesn't know its location and is able to report.	GoA1 GoA2 GoA3 GoA4	Restricted environment Urban environment

Table 11 - External conditions considered in the Use Case 2

The Use Case 2 is suitable for each railway profile and corresponds to the degraded operation where train position is invalid (the system version number X of a received virtual balise telegram is greater/smaller than the highest/smallest version number X supported by the on-board equipment or positioning function is unavailable) or unknown (cold movement detection has not occurred).

In this case train shall be moved until the position can be acquired. The maximum allowed time of driving without supervision shall be set depending on the line speed and density.

Driver/ATO functions, external to ERTMS/ETCS:

- The driver/ATO shall be able to enter/re-enter train data, select ERTMS level, as well as select/acknowledge the mode of operation (e.g. SH, OS).
- In case the SoM positioning report from OBU to RBC informs that the position of train is invalid/unknown, RBC will either reject or accept the train, in any case Full supervision will not be available. Driver/ATO will need to unblock the situation selecting either SH mode or re-enter train information and then select OS mode (in level 3, LS and SR modes will not be available without trackside detection).
- GoA3 and 4 will require ability of system to drive in OS mode. Route programming, obstacles detection, as well as virtual signals state detection, EoA stop markers detection and evaluation functions are required and are safety related.

Hazards introduced by trackside detection removal:

1. No flank protection in OS mode.
2. Neither RBC none IXL will know where the train is while it is moving on-sight.
3. As no route can be set for a train without its position, the right position of switches cannot be assured. Also, there is hazard that a switch can be moved while train is overpassing it.

The specific operational procedures shall be established to protect the area with time/distance restrictions for on-sight driving.

Operational Hazard	Consequence	Probability	Safety barrier/ Probability reduction	Required SIL
OPH-3 No flank protection in OS mode	**Collision**	Probable **in high – density lines** **Occasional** in medium density lines **Remote** in low density lines	**No barrier is assumed**	ATO (GoA3 and 4) shall check parallel track clearance during the SoM procedure **High and Medium density SIL4** **Low density SIL3**
	Severity= Catastrophic THR = 10^{-9}/h	**High and Medium density** E=1 **Low density** E=0.1	A=1	
OPH-4: Neither RBC none IXL will know where the train is while it is moving on-sight	**Collision**	Frequent **in high – density lines** **Probable** in medium density lines **Occasional** in low density lines	**No barrier is assumed**	ATO (GoA3 and 4) shall check track clearance during the SoM procedure **SIL4**
	Severity= Catastrophic THR = 10^{-9}/h	**High and Medium density** E=1 **Low density** E=1	A=1	Time/distance restrictions for on-sight movements must be foreseen (national values)

Operational Hazard	Consequence	Probability	Safety barrier/ Probability reduction	Required SIL
				Operational personnel at station/ marshalling yards may be involved.
OPH-5: Correct block of switches cannot be assured	**Derailment**	Occasional	**EoA marking before switches**	ATO (GoA3 and 4) shall be able to drive in OS, SR and SH with EoA marking detection. **SIL3**
	Severity= Critical **THR = 10^{-8}/h**	E=1	C=0.1	

Table 12- Use Case 2 Operational Hazards

5.2.3 Use Case 3 Start of Mission when the train integrity is not confirmed

The Use Case 3 corresponds to the case when the system is not performing correctly with the following conditions:

- The position can be correctly acquired from location unit;
- Train integrity is not confirmed;
- Communication session with RBC is correctly set;
- Train information is correct.

Traffic type and density	System states		Grade of Automation	Environmental conditions
Railway profile	**Mode of operation**	**Operational conditions**		
High density lines High speed lines Medium density lines Low density lines Regional lines	Degraded operation	The train knows its location and is able to report.	GoA1 GoA2 GoA3 GoA4	Open Sky Urban environment

Table 13 - External conditions considered in the Use Case 3

The Use Case 3 is suitable for each railway profile and corresponds to the degraded operation where train integrity is not confirmed during the Start of the Mission procedure, nevertheless the position of train can be acquired.

In this case, the shunting movements shall be performed to solve the uncoupling (assuming that the train integrity is not confirmed due to real uncoupling of the wagons, otherwise train integrity device shall be checked).

Driver/ATO functions, external to ERTMS/ETCS:

- The driver/ATO shall be able to select/acknowledge the mode of operation (SH).
- In case the SoM positioning report from OBU to RBC informs that the train integrity is not confirmed, RBC will accept the train, but FS will not be available. Driver/ATO will need to unblock the situation selecting SH mode.
- GoA3 and 4 will require ability of system to drive in SH mode. Route programming, obstacles detection, as well as virtual signals state detection and evaluation functions are required and are safety related.

Hazards introduced by trackside detection removal:

1. Wrong detection of train direction.
2. In SH mode the communication link with RBC is not active, so IXL will not know the train position. Unexpected virtual balises overpassing can be supervised on-board (in case trackside has provided a list of virtual balises or the list is stored on-board).

When the list of reference virtual balises is not available, the operational procedures similar to on-sight driving case shall be considered.

Operational Hazard	Consequence	Probability	Safety barrier/ Probability reduction	Required SIL
OPH-6: In SH mode the communication link with RBC is not active, so IXL will not know the train position	Collision	Probable in high – density lines Occasional in medium density lines Remote in low density lines	Unexpected virtual balises overpassing can be supervised on-board	ATO (GoA3 and 4) shall be able to perform Shunting movement **High and Medium density SIL3** **Low density SIL2**

	Severity= Catastrophic
	THR = 10-9/h
		High and Medium density **E=1**
		Low density **E=0.1**
			A=0.1	

OPH-2: Wrong detection of train direction **Covered in PHA (OBU-LU-7)**	-	-	-	-

Table 14- Use Case 3 Operational Hazards

Note: While in shunting close to stations, siding or yards, the permission to move may be managed by operational staff, when all necessary precautions are in place (like setting stop locations to prevent other trains to enter the area where the train will be permitted to move without MA under operational control).
Information that can be sent from the train to RBC depends on the specific use of this mode and on external conditions:

- movement of a train in case of trackside failures, other than GNSS failures. If a train cannot receive a MA because, for example the Evaluation of MA functions failed, the train can however send complete information to train detection functions and support normal Route Management System operations;
- Rescue of a failed train: Train length information can be entered in on-board equipment, but train integrity confirmation may be unavailable;
- Failure of on-board location functions: the concerned train is not able to send any information.
- General failure of GNSS: no train can send location information.

5.2.4 Use Case 4 Transition from Full Supervision to TRIP if train position is invalid/unknown

The Use Case 4 corresponds to the case when the system is not performing correctly with the following conditions:

- The position cannot be acquired from location unit;
- Train integrity is confirmed;
- Communication session with RBC is correctly set;
- Train information is correct.

Traffic type and density	System states		Grade of Automation	Environmental conditions
Railway profile	**Mode of operation**	**Operational conditions**		
High density lines High speed lines Medium density lines Low density lines Regional lines	Degraded operation	The train doesn't know its location and is able to report.	GoA1 GoA2 GoA3 GoA4	Restricted environment Urban environment

Table 15 - External conditions considered in the Use Case 4

The Use Case 4 is valid for each railway profile and corresponds to the degraded operation where during the mission (train circulating in FS) either train integrity is not confirmed, or train position becomes invalid/unknown. The diagram covers the case in which train position is invalid/unknown (the system version number X of a received virtual balise telegram is greater than the highest version number X supported by the on-board equipment or positioning function is unavailable).

In this case, the TRIP mode is triggered on-board and emergency brakes are activated, TR reports will be sent to RBC and it will delete current MA. OBU will ask driver/ATO to acknowledge TR and once ACK is given, the OBU will transit to PT mode and stop commanding emergency brakes. In PT mode, the backwords movements are only allowed to a given distance (national value). Backward movement can be undertaken in the case that received virtual balise telegram is greater than the highest version number X supported by the on-board equipment, in this case if after performing the movement the valid position is valid, driver/ATO can select Start to trigger MA request to RBC (Use case 5.2.1).

In case the positioning function is not available, driver/ATO also can select Start to trigger MA request to RBC (Use case 5.2.2). In this case it is the RBC responsibility to give an SR authorisation, or an On Sight/Shunting MA to an ERTMS/ETCS equipment that is in Post Trip mode. In each of these modes the train can be driven to the next safe location (station, siding, etc.) relying on a backup positioning system (e.g. odometry system), with limited speed and increased safe distance with the preceding and following trains. In case that after performing the backward movement that train integrity is not confirmed, the last detected maximum rear end position shall be established as an EoA for the following train.

Driver/ATO functions, external to ERTMS/ETCS:

- The driver/ATO shall be able to acknowledge TR mode and perform backwards movements to a given distance in PT mode.

- Once position is found or maximum distance in PT is reached, driver/ATO shall be able to select Start.
- In case the positioning function is not available (FS MA unavailable). Driver/ATO will need to unblock the situation selecting either SH, OS or SR mode.
- GoA3 and 4 will require ability of system to drive in SH, OS or SR mode. Route programming, obstacles detection, as well as virtual signals state detection and evaluation functions are required and are safety related.

Hazards introduced by trackside detection removal:

1. In case positioning function is not available it will be not possible to provide a list of reference virtual balises. In this case some of the trackside supervision function in SR mode will not be available.
2. As no route can be set for a train without its position, the right position of switches cannot be assured. Also, there is hazard that a switch can be moved while train is overpassing it.

The ceiling speed and maximum distances shall be established for restricted modes of operation (SH, SR, OS).

It needs to be highlighted that train integrity device must be highly reliable since its faults will impact the line availability, especially critically for high density and high-speed lines (false negative alarms of the device), since without trackside detection there will be no possibility to check the information provided by train integrity function.

Operational Hazard	Consequence	Probability	Safety barrier/ Probability reduction	Required SIL
OPH-7: In case positioning function is not available it will be not possible to provide a list of reference virtual balises	Collision	Probable in high – density lines Occasional in medium density lines Remote in low density lines	End of authority marking	ATO (GoA3 and 4) shall be able to drive in OS, SR and SH with EoA marking detection. **High and Medium density SIL4** **Low density SIL3**
	Severity= Catastrophic THR = 10^{-9}/h	High and Medium density **E=1** Low density **E=0.1**	**C=0.1**	
OPH-5 Correct block of switches cannot be assured	Derailment	Occasional	EoA marking before switches	ATO (GoA3 and 4) shall be able to drive in OS, SR and SH with EoA marking detection. **SIL3**
	Severity= Critical THR = 10^{-8}/h	**E=1**	**C=0.1**	

Table 16- Use Case 4 Operational Hazards

6 Application of formal methods to formalise safety requirements

6.1 Introduction and motivation

This section aims at giving an overview of the foreseen process for formal validation of the moving block model, provided in [RD.1], based on the safety requirements identified in the current deliverable [RD.1]. The approach increases the confidence on the correctness of the designed model with respect to its expected safety-critical behaviour, and possibly triggers changes to the design of the system, in case discrepancies between expected and observed behaviour are identified.

The approach will be applied within WP4, and, specifically, in the **Task T4.3**. However, it is useful to provide its preliminary definition, and showcase its application as a proof of concept, given its tight connection with the current deliverable.

The foreseen approach consists of the following steps:

1. Identification of safety requirements that have an impact on the modelled portions of the moving block system. The safety requirements to be considered are reported in the column "Requirement" of the document **Annex A Hazard Log**.
2. Formalization of the RT-UML model of the Moving Block from the document [RD.1] into a suitable formalism.
3. Formalization of each requirement into a verifiable formal property, e.g., a temporal logic formula, to be verified on the above formal model. In particular, only formulae capturing aspects that are modelled can be verified.
4. Verification of each property on the model of the moving block, based on the capabilities of the tool used for modelling and verifying the system.
5. Update/refinement of the model, in case the property is not satisfied, or the model does not account for the specific aspects the requirement should be verified upon.

In the following, we list an exemplary case of a formal representation of property, derived from the safety requirements, and how this property is verified on the formal model. The technique used for the verification phase will be *model checking*.

6.2 Background

In this section, fundamental notions of model checking are introduced, and are then specified for a particular framework: timed automata, metric interval temporal logic and the Uppaal tool [29].

6.2.1 Model Checking

Recent developments in probabilistic analysis using formal methods have improved the accuracy and reliability of dependability analysis, which was traditionally performed through not fully automated proof methods and computer simulations. In the literature, several approaches for the verification and validation of stochastic models have been proposed, as for example testing, theorem proving, model checking. In particular, model checking is a widely-used and powerful approach for the verification of finite state systems.

Model checking [30] is a technique for automatically verifying correctness properties, which is exhaustive for finite-state systems. It consists in proving that a model M, i.e. a suitable abstraction of the system under analysis, satisfies a particular property φ, written $M \models \varphi$. An example of a property φ could be the absence of deadlock states, i.e. the system never gets stuck. The model is generally described by some form of finite-state transition system, such as a Kripke structure [31] and the property of interest φ by a modal temporal logic. In this logic each formula has a truth value in each possible state of the system. States are temporally ordered: if a state q^0 is reachable from a state q then q temporally precedes q^0. Modal operators allow to express properties that must hold in every possible future state or in one future state. Since the system is finite-state, the procedure is decidable: an exhaustive search on the states space suffices to find states that eventually violate the property φ, if any.

Properties under which a model is verified are traditionally:

- *invariant properties*: this type of properties are memory-less, it suffices to check if the property holds in each state separately;

- *safety properties*: these properties are history-dependent; in order to check if a state q satisfies a safety property φ all the states that are traversed for reaching q are needed (i.e. the prefix). In particular, φ is characterized by its set of *bad prefixes*, that are all those finite traces that lead to a violation of the property: if the initial state satisfies φ, then the set of bad prefixes in empty.
- *liveness properties*: these properties cannot be violated by any finite prefix of an execution. An example of liveness properties are fairness properties, that are used for ensuring that if a state q is visited infinitely often, then all possible transitions from q must be traversed.

In our case, in order to take into account probabilities and time as expressed in the RT_UML model of D2.1, models will be specified in the stochastic extension of *Timed Automata* formalism [32] while formulae will be specified using the *Metric Interval Temporal Logic* (MITL) [33].

6.2.2 Timed Automata, Uppaal and Metric Interval Temporal Logic

Timed automata combine discrete systems with real-valued variables that evolve during the time a system spends in a state. These variables, called *clocks*, evolve uniformly and they can be used for guarding transitions and states invariants. Reachability and other key problems are decidable for timed automata.

Stochastic Timed Automata include also probabilistic transitions, with algorithms supporting them implemented in tools such as Uppaal [29].

We start by introducing some useful notation. In a timed automaton the system can evolve according to continuous clocks (i.e. time elapses within a particular state) or *jumps*, that are transitions between different states.

Let X be a set of clocks, and let v : $X \rightarrow$ R be a valuation of the variables in X, $\pi \in$ pred(X) be a predicate over X and $[[\pi]] \in R^{|X|}$ be the set of valuations of X that satisfies the predicate π. Predicates are used to (*i*) guard transitions, (*ii*) specify the jumps of a system (i.e. how variables evolve in a discrete step) and (*iii*) define the invariants for each state of the automaton.

A timed automaton A is defined as a tuple A = $<Q, Q_0, \Sigma, X, T, I, V_0>$ where:

- Q is a finite set of *states* including a distinguished initial singleton set $Q_0 \subseteq Q$,
- Σ is a finite set of *actions*,
- X is a finite set of real-valued *variables*, called *clocks*,
- pred(X) is a set of predicates over X
- T $\subseteq Q\times$pred$(X)\times\Sigma\times$pred$(X \cup X^0)\times Q$ is the *transition relation*,
- $I : Q \rightarrow$ pred(X) that assigns an invariant function to each state,
- $V_0 \in$ pred(X) is the set of initial valuations.

We now briefly describe the semantics of timed automata. A configuration of a timed automaton is a tuple (q,v) where $q \in Q$ is a state and v $\in R^{|X|}$ is a variable valuation.

The initial configuration of a timed automaton is (q_0,v$_0$), where $q_0 \in Q_0$, $v_0 = [[\pi]]$ such that $\pi \in V_0$ and $v_0 \in [[I(q_0)]]$ (the invariant constraints are satisfied). During the time t a system spends in a state q, the clocks in X are updated uniformly, and at each step the new valuation must respect the invariant constraints in q. A transition $\delta = (q,g,a,j,q_1)$ is enabled after time t when the guard $g \in$ pred(X) is satisfied. When δ is executed, the automaton jumps to a new configuration (q_1,v$_1$) such that q_1 is the target state of δ, v_1 is the valuation of the jump constraints $j \in$ pred($X \cup X^0$), and $v_1 \in [[I(q_1)]]$.

Composing Timed Automata For modelling complex systems it is convenient to adopt a modular approach where systems are described by interacting entities. This allows to separately verify different smaller components more efficiently than verifying a bigger monolithic model. Timed automata can be composed through a synchronous product operator, and they interact through actions and shared variables. Let $I = \{1,...,n\}$ be a set of indexes, the product of timed automata is denoted as $\otimes_{Hi\in C} H_i$, where $C = \{H_i \mid i \in I\}$. The states of the cartesian product are composed by the product of the states of its components. Similarly, the alphabet and the variables are the union of those of its components. The invariants and initial valuations are defined homomorphically on their elements. Finally, the transitions are synchronous, i.e. all the components (satisfying the constraints on the corresponding transition) synchronise when performing the same action a $\in \Sigma$, while the others stay idle (in the following we will also distinguish between input and output actions through broadcast channels).

Uppaal Uppaal is a toolbox that has been adopted for verifying real-time systems, represented by (extended) timed automata, that interact through broadcast channels and shared variables. Uppaal SMC is an extension of Uppaal that allows to express both stochastic and non-linear dynamic features, by adopting a stochastic and hybrid extension of timed automata. The stochastic interpretation replaces the non-deterministic choices for multiple enabled transitions and time delays with, respectively, probabilistic choices and probability distributions (uniform for bounded time and exponential for unbounded time). By composing different automata through the product operator, arbitrary complex behaviours can be obtained, where it is possible to statically or dynamically generate new instances of automata, that are uniquely identified.

Uppaal Verification Uppaal allows to verify, among the others, safety properties and reachability properties. In particular, a safety property is typically expressed by the formula $A\Box\phi$, whilst a reachability property is expressed by the formula $E\Diamond\phi$.
The operators A and E are *branching* operators: A checks whether the subsequent formula holds in all possible future executions of the system, whilst E checks if the subsequent formula holds in at least one future execution. The temporal operator $\Diamond$ (existential quantifier) checks whether there exists in the current run a future state in where ϕ holds, while the forall operator $\Box$ checks whether ϕ holds in all future states of the current run. A special property can be verified in Uppaal: $A\Box$ *not deadlock*, which checks the absence of deadlocks in the modelled system.
In addition to standard model checking techniques of properties as reachability and deadlock-freedom, in Uppaal it is possible to evaluate the probability that a random run of a network *M* satisfies a property ϕ in a given amount of time *t*.
Properties are defined using (an extension) of the Metric Interval Temporal Logic (MITL) [33]. A MITL formula ϕ is built by:

- atomic predicates over states of an automaton,
- standard logical operator,
- the next operator $\circ\phi$ that checks whether the formula ϕ holds in the next state,
- the operator $\phi_1 \, U_{x\le t} \, \phi_2$ that checks whether a formula ϕ_1 is satisfied in a run *until* a formula ϕ_2 is satisfied, and this must happen before the clock *x* exceeds the value *t*.

As usual, it is possible to derive the operators *exists* and *forall* as $\Diamond_{x\le t}\phi$ = true $U_{x\le t}\,\phi$ and $\Box_{x\le t}\phi = \neg\Diamond_{x\le t}\neg\phi$, where both quantifiers are bounded by the time *t* for the clock *x*.

Generally, checking if a model *M* satisfies a probabilistic property of type $P_M(\Diamond_{x\le t}\phi) \ge p$, $p \in [0,1]$, that is checking if the probability that the corresponding formula holds is greater than p, is undecidable [34]. Uppaal uses Statistical Model Checking to evaluate probabilistic properties of interest. Statistical Model Checking uses results from statistic area to decide, based on a given number of monitored simulations, whether the system under analysis satisfies the property of interest within a given degree of confidence. An advantage of Statistical Model Checking is that it avoids the exploration of the whole state-space of a model, which is a main drawback of standard model checking techniques.

Statistical algorithms are developed in Uppaal for estimating the probability of cost-bounded reachability problems in a given interval of confidence. There are three types of queries: $P_M(\Diamond_{x\le t} ap)$ (probability estimation), $P_M(\Diamond_{x\le t} ap) \ge p, p\in[0,1]$ (hypothesis testing), $P_M(\Diamond_{x_1\le t_1} ap_1) \ge P_M(\Diamond_{x_2\le t_2} ap_2)$ (probability comparison).

6.3 Preliminary formalization and verification of the Moving Block

In Figure 1 the preliminary formalization of the RT-UML model of the Moving Block from the document [RD.1] is provided, using the Stochastic timed automata formalism introduced above. Details about the semi-formal specification can be found in the document [RD.1].

6.3.1 Mapping RT-UML model into Stochastic Timed Automata

We now briefly comment on the mapping from the RT-UML model to the Timed Automata model. This step is crucial for providing an *executable* specification, amenable to formal verification. Since both RT-UML and Timed Automata are based on notions of states and transitions, and probabilistic and temporal aspects are primitively supported by both of them; the mapping is almost straightforward.
However, slight changes have been performed on the Timed Automata model, in order to reflect the intuition behind the semi-formal models. These intuitions have been provided during the various meetings with the ASTRail partners. Note that this is only a preliminary model, that will be refined in future phases of the ASTRail project, according to further refinements in the former RT-UML model.

The mapping is now informally discussed:

- The parallel regions of the RT-UML are mapped as separate automatons, that are then composed together through the product operator described in the previous section.
- States and transitions are in one-to-one correspondence, plus additional so-called urgent states in Timed Automata. These are states where basically the system spends a zero amount of time and are simply used for splitting the communication actions from the probabilistic choices.
- Guards and Triggers in RT-UML have been modelled as, respectively, input and output broadcast channels. Hence, it is assumed that communications between different entities (i.e. On-board Unit, Location Unit and Radio Block Center) are synchronous, where messages are discarded in case the receivers are not ready to receive them. The main intuition behind this choice is that, for example, a fresh Movement Authority sent by the Radio Block Center to the Onboard Unit supersedes previous Movement Authorities, in case those have not been received yet.
- Probabilistic transitions are in one-to-one correspondence. The probability of each transition will be an output from WP1 of ASTRail, and the actual weights in Figure 1 are place-holders.
- Timed aspects are rendered as follows. Each automaton has a clock, that is used for counting time. Delays of type *Rtat* are modelled as invariant conditions and clock guards, which force transitions to be executed when the exact amount of time has been reached. Probabilistic delays (*Rtdelay*) have been modelled probabilistic delays: when a transition is enabled, the time in which the transition will be fired is probabilistically distributed. As for probabilistic transitions, these delays will be an input from WP1 of ASTRail. We assume that no time divergence is present in our model. Accordingly, each state has an invariant constraining the clock to not exceed a given upperbound.

6.3.2 From Hazard Log to Verifiable Properties

We have discussed the formalization of the Moving Block model. This enables the formal verification of properties on such model. These *properties* will be extracted from informal requirements provided in the document **Annex A Hazard Log.** In order for such requirements to be verifiable, the same aspects captured by them must also be present in the corresponding formal model subject of the analysis. Indeed, the formal model must satisfy the requirements.

In the current version of the moving block model, communications and delays aspects are modelled. Moreover, a safety mechanism is also modelled, which *stops* a train in case it has not received a Movement Authority in a given amount of time (see state Stop in Figure 5).

We now turn our attention to current version of the document **Annex A Hazard Log**. In particular, the hazard OBU-TI-2 reports as cause a failure in the communications. Moreover, it requires to enter a safe state in case of such failure. Since both aspects (communications and safe state) have been modelled, we are ready to specify such informal requirement into the verifiable temporal logic property:

$$A\Diamond\ (\text{Controlling.Stop}\ \|\ \text{ReplyMA.ReplyRequest})$$

Intuitively, this property checks whether it is always true that either (operator ||) a Movement Authority is received, that is, state *ReplyRequest* is reached (see Figure 5) or the train enters a safe state (i.e. state *Stop* in Figure 1). The property is satisfied if one of these two events happen at some point in the execution. However, the property does not express whether this happens *infinitely often*. Indeed, in Uppaal it is not possible to express nested operators. Nevertheless, given that the model in Figure 1 is *cyclic* (i.e. it always returns to its initial state), in this particular case if the property holds than it will holds infinitely often.

Note that, the only reason why a movement authority cannot be received is because of repeated failures in communications, as reported in the OBU-TI-2 hazard.

This property has been verified on the model in Figure 5 through the Uppaal tool, which reports its satisfaction.

Note that the property does not express the amount of time in which the Movement Authority must be received, or the probability of entering a safe state. Indeed, these aspects are currently not considered, hence they have been neglected by the formal analysis, but they could be seamlessly integrated in the future.

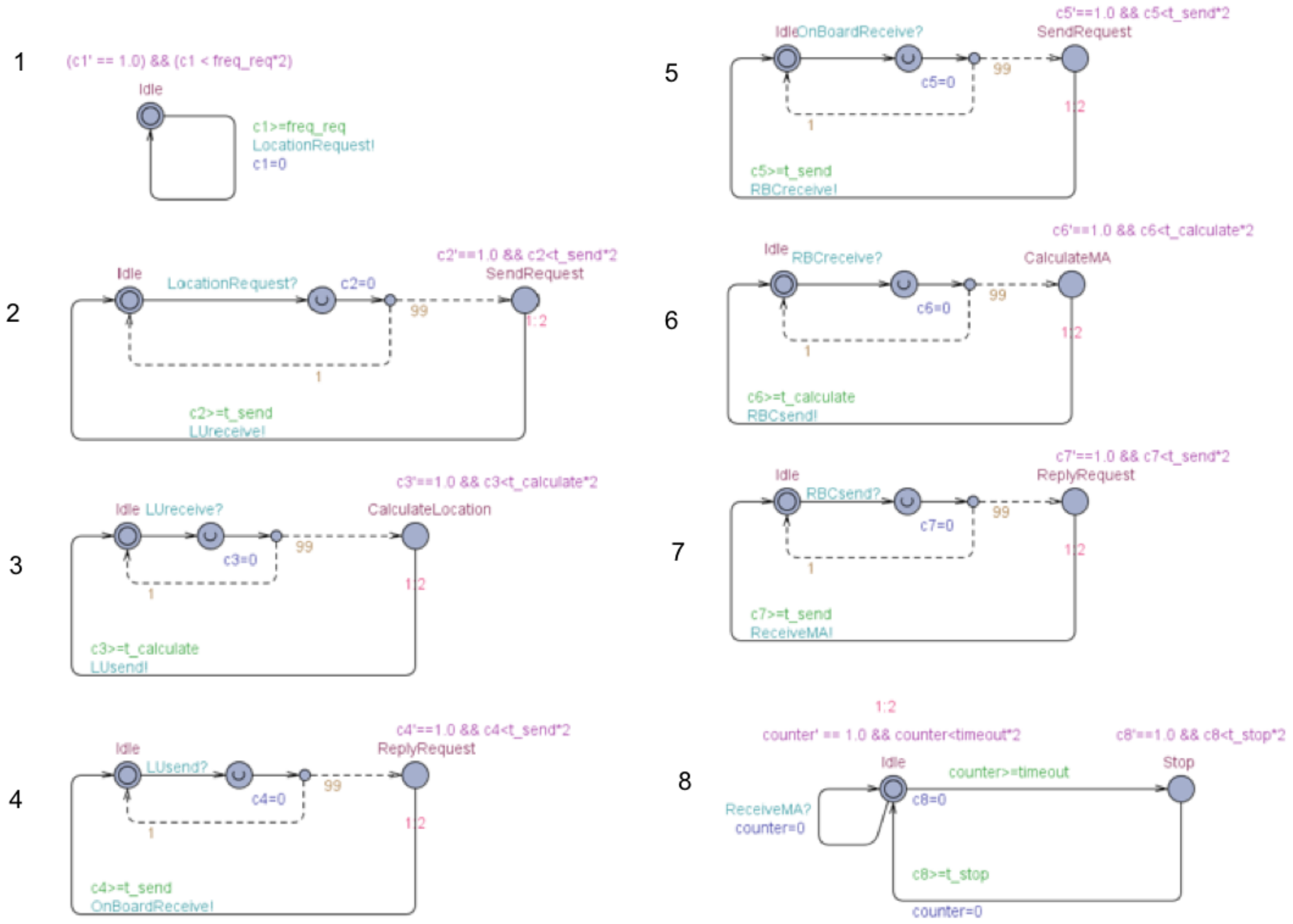

Figure 5. Moving block formalised with Stochastic Timed Automata modelled in Uppaal

7 Achievable Safety level for Moving Block without trackside detection

In the present chapter the results of the Hazard analysis of the moving block system without trackside detection are presented along with the conclusion on how the desired safety level may be earned by the system.

The chapter is organized in the way that in the first place, the Use Cases are discussed offering analysis of the hurdles encountered to assure SIL4 with the explanation of the related hazards. Then, the hazards with residual risk different from negligible are highlighted along with the discussion on the possibilities to reduce it to at least “tolerable” level. In the analyses it is assumed that only technical measures can assure risk reduction to “negligible” level, while operational measures will in the best case achieve “tolerable” level due to human factor presence.

1. Use Case 1 Start of Mission when train position is valid

The Start of Mission procedure can be performed safely for all railway profiles in case the positioning information is valid (cold movement detection has occurred), nevertheless two specific operational hazards shall be considered (Table 10) because of trackside detection absence.
The OPH-1 concerns the driver/ATO, as either driver or ATO shall be able to check the clearance before the train at standstill to assure there is no other train in SB waiting for awakening. The ATO function in this case is safety related.

In relation to OPH-2, there is a hazard of wrong detection of train direction at low speeds (OBU-LU-7), additional mitigation measures shall be provided (either technical or operational) to cope with it, since GNSS standalone is not able to assure SIL4 for this function. If appropriate SIL4 technical measures will be taken, the residual risk can be assumed to be “negligible”.

2. Use Case 2 Start of Mission when the train position is invalid/unknown

The SoM procedure performed in degraded mode of operation when the train position is invalid (cannot be acquired from LU) or unknown (cold movement detection has not occurred) can be managed safely of the hazards OPH-3, OPH-4 and OPH-5 (Table 12) are considered.
It was assumed than the adequate mode of operation for SoM in degraded conditions is OS, which means that either Driver or ATO shall be able to move the train on-sight without trackside detection support.
Moreover, no flank protection can be assured since the train position is not know to trackside, neither the safe operation of switches may be possible. If train shall overpass the switch, ATO/driver shall be able to detect switch position and check that no train is approaching to the same switch from parallel tracks. On the other side, ATO/driver shall react on stopping marker which shall be placed before switches.
For ATO system these functions are safety- related.
Railway operator shall define operational procedure for turnout management for OS SoM, if these measures will be established the Residual Risk for the hazards can be “tolerable”.

3. Use Case 3 Start of Mission when the train integrity is not confirmed

If during the Start of Mission procedure the train location is known but train integrity is not confirmed, the Full supervision mode may not be available, nevertheless shunting movements can be performed by driver/ATO to solve the uncoupling if possible, after the driver/personnel at station confirm the uncoupling.
SRS include the possibility for the driver to confirm the train integrity manually if everything is correct, thus allowing the FS mode, but it is not clear what shall be done if TI device is faulty and is not able to provide the TI status.
Emergency brake application (Train Trip) is not applicable for the situation of train integrity loss, so in case RBC receives the alarm from OBU or the communications with train has been lost, it shall revoke/shorten the MA for the following train establishing the last reported rear end minimum safe position as an EoA. The emergency management will be then under Railway Authority procedures.

In case train has switched to shunting mode, the OPH-6 and OPH-2 shall be considered (Table 14), in which case driver/ATO are required to be able to drive in SH (for ATO it is safety- related), nevertheless the unexpected virtual balises overpassing can be supervised on-board (a list of reference balises shall be provided by trackside whenever possible). The residual risk can be deemed “negligible” if shunting movement can be performed safely.
In relation to OPH-2, the same restrictions as in the Use Case 1 are applicable.

4. Use Case 4 Transition from Full Supervision to TRIP if train position is invalid/unknown

When the train is running in Full Supervision with a valid MA and the position becomes invalid (the system version number X of a received virtual balise telegram is greater than the highest version number X supported by the on-board equipment) or unknown (positioning function is unavailable), the TRIP mode will be triggered on-board with emergency brake application.

It shall be noted that “positioning function unavailable” is referred to the situation when no indication from location unit can be obtained, instead, if GNSS is out of service (non LoS), but a backup system (e.g. odometry) is providing correctly monitored positioning information (the safe front end can be computed and the backup system is SIL4), the train will not be tripped. The maximum distance allowed for a train moving with backup system only shall be defined.

Once the transition to TR is acknowledged by RBC and the driver/ATO, the driver/ATO will be offered to select SH, OS or SR mode.

When in SH, OS or SR, the OPH-7 and OPH-5 hazards (Table 16) must be considered.

If the train is being moved in one of chosen modes to next safe location (a station, siding, marshalling yard, etc.), the section where it is moving shall be assured from the trackside from the last reported minimum safe rear end position until the next safe location, the train will be driven at limited speed with OBU supervision. Nevertheless, the ATO/driver will be required to recognize the safe location, signals and markers and stop the train safely. The switches position shall be managed by operational procedures (e.g. from command posts). For ATO these functions are safety – related.

If these measures will be established the Residual Risk for the hazards can be “tolerable”.

5. Train is running in Full Supervision

Aside from above mentioned Use Cases, the case of train running in Full Supervision shall be considered, and the hazards associated to it are listed in the Table 17 and the Table 18.

The acceptable level of safety in this case can be achieved when the Hazards 7, 8, 9, and 10 are mitigated by technical measures, assuring that GNSS based positioning system is SIL4. These hazards will be further analysed within ASTRail WP1 to assess whether SIL4 can be potentially achieved.

On the other hand, the Hazards 13 and 14, related to train direction detection at low speed and to the track discrimination, shall be mitigated by additional to GNSS measures (either technical or operational), since it is unlikely that GNSS system standalone is able to provide the accuracy needed for track discrimination and it is prone to fail detecting slow frequency drift phenomenon at low speeds (this phenomenon and its potential impact on position integrity supervision will be further investigated in ASTRail WP1).

6. Timing challenges

While the operation with the Moving Block system without trackside detection, can be performed safely if the above-mentioned hazards are mitigated appropriately, the impact on the availability of the system shall be estimated.
Without trackside detection, it will not be possible to switch to ERTMS L0, 1 or 2 operation if train positioning system fails, which means that the speed of the trains operated in degraded modes will be significantly reduced (possibly to 25 – 30 kmph), and the distance between the failed train and the other trains will need to be increased until it can be driven to safe location (an entire section from the last reported minimum safe rear end of failed train to the next safe location will ned to be cleared, which can mean several kilometres). Also, the loss of communication with RBC will suppose the trains

operated in its area become “invisible” for trackside, and if transition to lower ERTMS level is not possible, the trains will be tripped.
These issues will obviously produce a high impact on high speed and high-density lines operation, even though the acceptable safety level could be assured.

These hurdles can be potentially solved with virtual coupling with high levels of reliability of train-to-train communications.

It needs to be highlighted that timing challenges discussion is not in the scope of this report, since basically impact the availability of the system, despite of this, the prolonged operation in degraded modes is undesirable since the “average” safety will be affected. To avoid it the highest levels of reliability must be achieved for all critical components (>99,9999%).

8 Conclusions

To perform the PHA, the MBS system safety functions have been defined implementing the top-down analysis which has been derived from the most common type of railway accidents and the scenarios which can lead to these accidents that involve signalling system. The analysis is based on MBS system model considering the interchange of the data between its main components.

After the determination of the MBS system safety functions, the hazards which can prevent system from performing its safety function have been defined, their plausible causes and consequences have been analysed.

The results of the analysis are recorded in the Hazard Log (Annex A) which contains the hazards identified during the PHA and the evaluated risk, proposed mitigations measures, derived requirements and SRACs.

The main inputs that has been used for the Hazard Analysis are:

- The MBS system definition and model from D2.1;
- The system Use cases modelled in UML Sequence charts for Interface Hazard Analysis and operational hazard analysis;
- The detailed analysis of the ERTMS hazards related to GNSS faults performed in the T1.5 (WP1);
- Results of the simulation of local effects performed in T1.3;

The outputs of the Hazard Analysis will be exploited in the T4.3 (WP4) during the for formal validation of the moving block model, provided in [RD.1]. This validation will be based on the safety requirements mapped to formal properties suitable for validation process by formal method/s chased within WP4.

The hazards identified during the PHA are related to the Moving Block system without trackside detection considering the ERTMS L3 application. The hazards which are common to ERTMS L2 and ERTMS L3 applications have not been considered in the present analysis since they are already covered in other reference sources (e.g. [12], [13]).

A specific hazard ID has been assigned, the ID contains the indication of components of the systems are involved and a number.

From each hazard a requirement has been defined, this requirement aims to reduce the initial risk to acceptable level where possible. Where appropriate a resulting mitigation measure and a formal property has been identified and recorded. The requirement ID contains the indication of the component /function of the system to which is applicable.

Some of the mitigation measure are not in the scope of ASTRail project (e.g. Train Integrity system), and those particularly related to GNSS system will be analysed in the Task 1.5 (e.g. RE-LU-1), since T2.3 and T1.5 hazard analyses are aligned.

Safety Related Application Conditions include the indication for the degraded mode operation considering the particular conditions of ERTMS L3, highest grades of automation and the conditions related to the specific applications.

The residual risk corresponds to the level of risk after the application of identified safety requirements/ mitigation measures; where the residual risk is different from “negligible”, further mitigation (technical and/or operation) is needed. Due to the presence of the hazard with residual risk “tolerable”, “undesirable” and even “intolerable”, the further analysis will be conducted in the WP1 with the aim to provide the definitive conclusion regarding MBS system without trackside detection likelihood to comply with required safety level.

The outcomes of the T2.3 will provide hints for the Task 1.8 to define the indicators for test cases and to define GNSS Minimum performance requirements for rail, especially in terms of safety integrity. Also, the task will provide indicators for T4.2 to ease the ranking of formal methods and tools in terms of their suitability to model and validate required formal properties of moving block system.

Acronyms

Acronym	Explanation
DP	Dangerous Point
ERTMS	European Rail Traffic Management System as defined in EC Decision 2001/260
ERTMS MA	ERTMS Movement Authority
ETCS	European Train Control System; - the control/command and signalling element of ERTMS
EVC	European Vital Computer
FFFIS	Form, Fit, Function Interface Specification
FS	Full Supervision mode
GNSS	Global Navigation Satellite System
LU	Location Unit
MA	Movement Authority
MBS	Moving Block signalling system
NRBC	Neighbour Radio Block Centre
OBU	On-Board Unit which includes EVC
OS	On Sight mode
PHA	Preliminary Hazard analysis
PT	Post Trip mode
RBC	Radio Block Centre
RMS	Route Management system
SH	Shunt mode
SIS	Signal In Space
SR	Staff Responsible mode
SRAC	Safety Related Application Condition
SvL	Supervised Location
TI	Train Integrity
TSI	Technical Specification for Interoperability

List of figures

List of tables

References

[1] BS EN 50126-1:1999 Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Basic requirements and generic process.

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

[3] PD CLC/TR 50126-2:2007 Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS). Guide to the application of EN 50126-1 for safety

[4] UNISIG SUBSET-026 v300 System Requirements Specification - Baseline 3

[5] UNISIG SUBSET-041 Performance Requirements for Interoperability 3.1.0

[6] RSSB – ERTMS – OC Operational Concept for ERTMS, 2014, Rail Safety and Standards Board Limited

[7] EN 50159:2010 Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[8] SUBSET-039 FIS for the RBC/RBC Handover, issue: 3.2.0, date: 17-12-2015.

[9] SUBSET-098, RBC-RBC Safe Communication Interface, issue: 3.0.0, date: 29 February 2012

[10] SUBSET-037, EuroRadio FIS, issue: 3.2.0, date:17 December 2015.

[11] COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009.

[12] SUBSET- 078 Failure Modes and Effects Analysis for the Interface to/from an Adjacent RBC - in Application Level 2, issue: 2.4.0, date 07-04-2009.

[13] SUBSET-120 FFFIS TI – Safety analysis, issue: 0.2.11, date: 27-10-2014.

[14] EN 50159, 2001. Railway applications: communication, signalling and processing systems: safety-related communications in closed (part 1) and in open (part 2) transmission systems. CENELEC European standard (European Committee for Electrotechnical Standardization).

[15] ERA – European Railway Agency, 2009a. Collection of examples of risk assessments and of some possible tools supporting the CSM regulation. ERA reference: ERA/GUI/02-2008/SAF.

[16] Friedemann Bitsch, Ulrich Feucht, and Huw Gough, Safety-Related Application Conditions – A Balance between Safety Relevance and Handicaps for Applications, Springer-Verlag Berlin Heidelberg 2009

[17] Filip, A., 2001. Train control via global navigation satellite system: fiction or reality? In: ITS International Conference, Brno, Czech Republic.

[18] Filip, A., Beugin, J., Marais, J., Mocek, H., 2008. Interpretation of the Galileo safety-of-life service by means of railway RAMS terminology. International

[19] GRAIL, 2007. Enhanced Odometry FMEA Report. Deliverable of the GRAIL project: GNSS introduction in the RAIL sector, issue 1.0., project funded by the EC.

[20] Hänsel, F., Poliak, J., Barbu, G., Schnieder, E., 2006. Safety related usage of satellite-based positioning systems in transportation-concept for Certification.

[21] Bate, I., Bates, S., Hawkins, R., Kelly, T., McDermid, J.: Safety case architectures to complement a contract-based approach to designing safe systems. In: 21st International System Safety Conference, System Safety Society (2003)

[22] Hartwig, K., Grimm, M., Meyer Zu Hörste, M., Lemmer, K., 2006. Requirements for safety relevant positioning applications in rail traffic – a demonstrator for a train borne navigation platform called ‘‘DemoOrt’’. The 7th World Congress on Railways Research – WCRR, Montreal, Canada.

[23] IEC 62278, 2002. Railway applications – specification and demonstration of reliability, availability, maintainability and safety (RAMS).

[24] IEC 62279, 2002. Railway applications – communications, signalling and processing systems – software for railway control and protection systems.

[25] IEC 62425, 2007. Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling.

[26] Lannoy, A., 2002. A survey of methods and tools for reliability evaluation of SSCs. In: Proceedings of the 3rd International Conference on Mathematical

[27] LOCOPROL, 2001. System safety report. LOCOPROL-low cost satellite-based train location system for signalling and train Protection for Low density traffic railway lines, deliverable D5.1.

[28] Manz, H., Schnieder, L., 2009. Bridging the gap between railway safety and the specification of satellite-based location systems. In: The 9th International

[29] Larsen, K. G., Pettersson, P., & Yi, W., 1997. UPPAAL in a nutshell. *International journal on software tools for technology transfer*, *1*(1-2), 134-152.

[30] Clarke, E. M., Grumberg, O., & Peled, D., 1999. *Model checking*. MIT press.

[31] Kripke, S. A., 1963. Semantical analysis of modal logic - normal modal propositional calculi. *Mathematical Logic Quarterly*, *9*(5-6), 67-96.

[32] Alur, R., & Dill, D. L., 1994. A theory of timed automata. *Theoretical computer science*, *126*(2), 183-235.

[33] Alur, R., Feder, T., & Henzinger, T. A., 1996. The benefits of relaxing punctuality. *Journal of the ACM (JACM)*, *43*(1), 116-146.

[34] Henzinger, T. A., Ho, P. H., & Wong-Toi, H., 1998. Algorithmic analysis of nonlinear hybrid systems. *IEEE transactions on automatic control*, *43*(4), 540-554.

Annex A Hazard log

In the present Annex the Hazard Log table, result of the Moving Block system Hazard analysis is presented.

ID		Safety Function	Description	Consequence	Cause	Top Hazard	Initial Risk			Requirement		Mitigation measure	Formal Property	SRACs (Safety Related Application Conditions)	Residual Risk			Responsible	Comments
Nº	Hazard ID						Frequency	Severity	Result	ID	Description				Frequency	Severity	Result		
1	OBU-TI-1	SFSC 01	The train is not complete, but no alarm is triggered.	The system keeps working as if the train was complete but there are decoupled wagon/s left on track	HW or SW error of the train integrity device	Rear collision	OC	CA	IT	RE-TI-1	TI device must be SIL4 device. TI device must immediately send an alarm to OBU in case that TI is not confirmed.	n/a	If TI is not confirmed, TI device sends NOK alarm.	Data verification and validation plan A data verification and validation plan must be defined in each specific application. This plan will specify the foreseen data verification activities and the verification test specification applicable to a specific Operation.	IN	CA	NE	Design	ASTRail assumes that the device is SIL4.
2	OBU-TI-2	SFSC 01	The train is not complete, but no alarm is triggered.	The system keeps working as if the train was complete but there are decoupled wagon/s left on track	TI- OBU communications failure.	Rear collision	OC	CA	IT	RE-TI-2	Communications between TI and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered.	The communication protocol shall be compliant with Subset-119. The protection measures such as time-stamping, authentication protocol, message numbering, message acknowledgment etc. shall be implemented.	If OBU receives NOK alarm from IT device, OBU sends an ACK message to IT device.	If Train Integrity cannot be confirmed within the maximum time limit, the train shall be stopped (transition to TRIP).	IN	CA	NE		
3	OBU-TI-3	SFSC 04	The train is not complete, but no alarm is triggered.	The system keeps working as if the train was complete but there are decoupled wagon/s left on track	HW or SW error in OBU	Rear collision	OC	CA	IT	RE-TI-3	OBU device must be SIL 4 device. Once OBU receives the alarm "TI not confirmed" it must immediately send an alarm to RBC.	n/a	If OBU receives NOK alarm from IT device, OBU sends NOK alarm.	Data verification and validation plan A data verification and validation plan must be defined in each specific application. This plan will specify the foreseen data verification activities and the verification test specification applicable to a specific Operation.	IN	CA	NE	Design	OBU is SIL4
4	OBU-TI-4	SFSC 04	The train is complete, but the alarm is triggered	The system works as if the train where not complete and applies the foreseen measures in case of train integrity failure	TI device wasn't able to complete the TI check	Impact on availability and on "average" safety	OC	MA	UD	RE-TI-4	TI device must be SIL4 device. TI device must provide the level of availability sufficient to avoid occasional triggering of false negative alarms.	n/a	n/a	The level of TI device availability shall be determined for each specific Operation conditions.	IM	MA	NE	Design	
5	RBC-TI-1	SFSC 13	RBC doesn't receive the alarm "TI is not confirmed"	The system keeps working as if the train was complete but there are decoupled wagon/s left on track	The message is lost or corrupted, clock error	Rear Collision	PR	CR	IT	RE-TI-5	Communications between RBC and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered.	The communication protocol shall be compliant with Subset-037. The protection measures such as time-stamping, authentication protocol, message numbering, message acknowledgment etc. shall be implemented.	If RBC receives NOK alarm from OBU, RBC sends an ACK message to OBU device.	If communication between RBC and OBU is lost, OBU must transit in SR mode. For GoA 3 and GoA4 the specific features shall be implemented to allow SR mode circulations.	IN	CR	NE	Design	

ID		Safety Function	Description	Consequence	Cause	Top Hazard	Initial Risk			Requirement		Mitigation measure	Formal Property	SRACs (Safety Related Application Conditions)	Residual Risk			Responsible	Comments
Nº	Hazard ID						Frequency	Severity	Result	ID	Description				Frequency	Severity	Result		
6	RBC-TI-2	SFSC 13, SFSC 11, SFSC 18, SFSC 18 SFSC 14	RBC doesn't take into account "TI is not confirmed" alarm	The system keeps working as if the train was complete, but it is not	HW or SW error in the RBC	Rear collision	RE	CA	UD	RE-TI-6	RBC device must be SIL 4 device. Once RBC receives the alarm "TI not confirmed" it must immediately initiate safe state procedure.	n/a	If RBC receives NOK alarm from OBU, RBC starts safe state procedure.	Safe State procedure in case of receiving alarm "TI not confirmed" shall be foreseen for each specific Operation condition. The train that has produced the initial alarm and the following must transit to degraded mode (TR, SR, OS); estimated affected zone must be delimited (to be calculated regarding the last reported tail position), the MA authorities of other following trains shall be shortened.	IN	CA	NE	Design / Operation	
7	OBU-LU-1	SFSC 03, SFSC 10, SFSC 07	Positioning error exceeds alert limit but is undetected and no alarm is triggered (Integrity Risk).	Error in the MA calculation, the distance to the next SvL/train/danger point is insufficient for safe braking.	GNSS Receiver integrity monitoring system error	Collision / Derailment	PR	CA	IT	RE-LU-1	GNSS Receiver integrity monitoring system must be SIL4 system.	*Different architectures can be implemented to cover the requirement. They will be analysed in ASTRail WP1*	n/a	The positioning error mitigation measure shall be implemented within the user segment. The assumptions on space segment integrity risk level provided by SIS shall be taken for each specific application.	RE	CA	UD	Design	Shall be further analysed within WP1
8	OBU-LU-2	SFSC 03	Positioning error exceeds alert limit but the alarm is triggered exceeding time-to alarm limit (Integrity Risk).	Train is not able to stop in time before the supervised position/ preceding train	Error of position integrity monitoring/ clock error	Collision	PR	CA	IT	RE-LU-2	GNSS Receiver integrity monitoring system must be SIL4 system.	*Different architectures can be implemented to cover the requirement. They will be analysed in ASTRail WP2*	n/a	The positioning error mitigation measure shall be implemented within the user segment. The assumptions on space segment integrity risk level provided by SIS shall be taken for each specific application.	RE	CA	UD	Design	Shall be further analysed within WP1
9	OBU-LU-3	SFSC 03	GNSS positioning system is unable to provide train position within positioning error margin	System will enter safe state mode	Not enough coverage for GNSS	Impact on availability and on "average" safety	PR	CA	IT	RE-LU-3	The SIS availability shall be tolerated by LU, the back-up positioning system (relying on odometrical position or inertial sensors) shall be foreseen.	*Different architectures can be implemented to cover the requirement. They will be analysed in ASTRail WP1*	n/a	The maximum distance/ time during which the SIS unavailability could be tolerated without an impact on safety shall be estimated for each specific application. Previously to authorizing the operation, the predictable SIS availability parameters along the track shall be checked to ensure the maximum distance/time limit will be respected.	RE	CA	UD	Design	Shall be further analysed within WP1
10	OBU-LU-4	SFSC 03	LU calculates ambiguous position	RBC takes into account wrong position	GNSS system and back up positioning system provide different position information	Collision / Derailment	FR	CR	IT	RE-LU-4	Implement internal LU procedure to be able to determine which positioning information is reliable in when position request is generated.	*Different architectures can be implemented to cover the requirement. They will be analysed in ASTRail WP1*	n/a	The maximum distance/ time during which the SIS unavailability could be tolerated without an impact on safety shall be estimated for each specific application. Previously to authorizing the operation, the predictable SIS availability parameters along the track shall be checked to ensure the maximum distance/time limit will be respected.	RE	CR	UD	Design	Shall be further analysed within WP1

ID		Safety Function	Description	Consequence	Cause	Top Hazard	Initial Risk			Requirement		Mitigation measure	Formal Property	SRACs (Safety Related Application Conditions)	Residual Risk			Responsible	Comments
Nº	Hazard ID						Frequency	Severity	Result	ID	Description				Frequency	Severity	Result		
11	OBU-LU-5	SFSC 03, SFSC 10, SFSC 07	Back-up positioning system provides incorrect train position	Error in the MA calculation, the distance to the next SvL/train/danger point is insufficient for safe braking.	SW or HW error	Collision / Derailment	PR	CA	IT	RE-LU-5	Back-up positioning system must be SIL4 system.	n/a	n/a	Data verification and validation plan A data verification and validation plan must be defined in each specific application. This plan will specify the foreseen data verification activities and the verification test specification applicable to a specific Operation.	IM	CR	TO	Design	
12	OBU-LU-6	SFSC 03, SFSC 10	LU is unable to send position information to the OBU, and OBU doesn't generate an alarm	RBC has no information regarding train position, and considers the train is not moving	LU- OBU communications failure.	Collision / Derailment	PR	CA	IT	RE-LU-6	Communications between LU and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered.	The communication protocol shall be compliant with Subset-119. The protection measures such as time-stamping, authentication protocol, message numbering, message acknowledgment etc. shall be implemented.	If OBU receives train position from LU, OBU sends an ACK message to LU device.	If train position cannot be received within the maximum time limit, the OBU shall generate an alarm and must transit to degraded mode (TR, PT, SR, OS). For GoA 3 and GoA4 the specific features shall be implemented to allow restricted mode circulations.	IN	CA	NE	Design	
13	OBU-LU-7	SFSC 10, SFSC 07, SFSC 08, SFSC 12	OBU provides incorrect information regarding train direction	Error in the MA calculation, the distance to the next SvL/train is insufficient for safe brake.	GNSS receiver is unable to detect the direction of movement because the speed of train is too low.	Collision	PR	CA	IT	RE-LU-7	GNSS receiver shall provide train direction whenever possible. If train direction is not detected an alarm shall be triggered/ back up positioning system shall be engaged	Back-up positioning system can be used to provide information regarding train direction during low speed operation	n/a	An operational procedure must be set to manage train direction detection.	RE	CA	UD	Design	A specific analysis shall be provided for each specific application.
14	OBU-LU-8	SFSC 03, SFSC 10, SFSC 07, SFSC 12	LU provides ambiguous information regarding the track on which the train is located	Error in the MA calculation, the distance to the next SvL/train is insufficient for safe brake.	GNSS receiver is unable to discriminate the tracks	Collision	FR	CA	IT	RE-LU-8	LU must be able to provide unambiguous information for track discrimination.	Additional mitigation measures shall be foreseen to protect the switches.	n/a	A specific safety analysis must be performed to prove the ability of system to discriminate track.	PR	CA	IT	Design	For the current situation is unlikely that GNSS system standalone is able to provide the accuracy needed for track discrimination
15	RBC-LU-1	SFSC 09, SFSC 05, SFCS 16, SFCS 17, SFCS 14, SFSC 07, SFSC 08, SFSC 12	RBC receives incorrect train position	Error in the MA calculation, the distance to the next SvL/train/danger point is insufficient for safe braking.	The message is lost or corrupted, clock error	Collision / Derailment	PR	CA	IT	RE-LU-9	Communications between RBC and OBU must be safe and continuously supervised, if the connection is lost an alarm must be triggered.	The communication protocol shall be compliant with Subset-037. The protection measures such as time-stamping, authentication protocol, message numbering, message acknowledgment etc. shall be implemented.	If RBC receive train position from OBU, RBC sends an ACK message to OBU.	If communication between RBC and OBU is lost, OBU must transit to degraded mode (TR, PT, SR, OS). For GoA 3 and GoA4 the specific features shall be implemented to allow restricted mode circulations.	IN	CR	NE	Design, Operation	

ID		Safety Function	Description	Consequence	Cause	Top Hazard	Initial Risk			Requirement		Mitigation measure	Formal Property	SRACs (Safety Related Application Conditions)	Residual Risk			Responsible	Comments
Nº	Hazard ID						Frequency	Severity	Result	ID	Description				Frequency	Severity	Result		
16	RBC-LU-2	SFSC 09, SFCS 16, SFCS 17, SFCS 14, SFSC 08	RBC does not receive train position	RBC has no information regarding train position	RBC HW failure	Collision / Derailment	PR	CA	IT	RE-LU-10	Install a redundant system to ensure the required availability and reliability. Implement monitoring system to observe and detect communications loss. In case of communications loss enter in the safe state.	In case of communication loss enter in safe state mode.	If communication loss is detected, system enters in safe state.	If communication between RBC and OBU is lost, OBU must transit to degraded mode (TR, PT, SR, OS). For GoA 3 and GoA4 the specific features shall be implemented to allow restricted mode circulations.	IN	CR	NE	Design, Operation	
17	RBC-LU-3	SFSC 10, SFCS 16, SFCS 17, SFCS 14, SFSC 08	OBU is unable to send position information to RBC	RBC has no information regarding train position, and considers the train is not moving	Communications loss	Collision / Derailment	PR	CR	IT	RE-LU-11	Implement monitoring system to observe and detect communications loss. In case of communications loss enter in the safe state.	In case of communication loss enter in safe state mode.	If communication loss is detected, system enters in safe state.	If communication between RBC and OBU is lost, OBU must transit to degraded mode (TR, SR, OS). For GoA 3 and GoA4 the specific features shall be implemented to allow restricted mode circulations.	IN	CR	NE	Design, Operation	
18	RBC-LU-4	SFSC 09, SFSC 05, SFSC 07, SFSC 08, SFSC 02	RBC is not able to detect the direction of train movement	Error in the MA calculation, the distance to the next SvL/train is insufficient for safe brake.	RBC is not capable to interpret the data coming from train	Collision	PR	CA	IT	RE-LU-12	The appropriate procedures must be foreseen to allow RBC to interpret correctly the direction of train.		n/a		IN	CR	NE	Design	
19	OBU-SM-1	SFSC 17, SFSC 19, SFSC 06	Train that circulating in restricted modes overrides Dangerous point	Train override a switch in movement/ invades the route reserved for another circulation	Positioning information is not available without trackside detection	Collision/ Derailment	PR	CA	IT	RE-SM-1	The positioning error must be taken into account when transmitting speed restriction in SR mode.	To foresee necessary protection level for section with speed restrictions.	n/a	The Railway Authority must implement traffic control measures in SR mode and define the SR zones and speed restrictions in these zones.	IM	CA	TO	Operation	
20	OBU-SM-2	SFSC 17, SFSC 19, SFSC 02, SFSC 06	Train that circulates in restricted modes doesn't receive information about speed restrictions	Train circulates at excessive speed	The train position is undetected and the data regarding speed restrictions cannot be transmitted.	Derailment	PR	CA	IT	RE-SM-2	All trains in SR mode must be given speed restriction information as part of the permission to proceed.		n/a	Drivers must be aware that the speed restrictions may not be transmitted by ERTMS. For GoA3 and GoA4 the specific procedures shall be established to manage the speed restrictions without ERTMS supervision.	IN	CA	NE	Operation	
21	RBC-SM-3	SFSC 17, SFSC 19, SFSC 02, SFSC 06	Train that circulates in restricted modes stops to receive information about speed restrictions	Train circulates at excessive speed	The communication with RBC failed	Derailment	RE	CA	UD	RE-SM-3	All trains in SR mode must be given speed restriction information as part of the permission to proceed. The most restrictive data shall be taken into account.		n/a	The drivers of fitted trains must be made aware of the possibility of divergence between the speed related information received ERTMS DMI and that provided at the lineside for unfitted trains. For GoA3 and GoA4 the specific procedures shall be established to manage the speed restrictions without ERTMS supervision.	IN	CA	NE	Operation	

Table 17. RBC – OBU interface

ID		Description	Consequence	Cause	Top Hazard	Initial Risk			Requirement/Action		SRACs (Safety Related Application Conditions)	Residual Risk			Responsible	Comments
Nº	Hazard ID					Frequency	Severity	Result	ID	Description		Frequency	Severity	Result		
1	NRBC-LU-1	MA is incorrectly shortened to RBC-RBC border	The train will not able to cross the border as the related resources are blocked in the Accepting RBC	The positioning error has not been foreseen for shortened MA calculation	Collision/ Impact on availability	PR	CA	IT	RE-NRBC-1	The positioning error must be taken into account during shortened MA calculation.	Specific procedures shall be established for RBC-RBC border zone delimitation.	IM	CR	TO	Design/ Operation	
2	NRBC-LU-2	Handing over RBC considers train overpassed the border, but it is not	The train will not able to cross the border as the related resources are blocked in the Accepting RBC	The reported train position is incorrect/The positioning error has not been foreseen	Collision/ Impact on availability	PR	CA	IT	RE-NRBC-2	The positioning error must be taken into account. GNSS Receiver integrity monitoring system must be SIL4 system.	Specific procedures shall be established for RBC-RBC border zone delimitation.	IM	CR	TO	Design/ Operation	
3	NRBC-LU-3	In the meantime, the train passes the RBC border while the Accepting RBC intends to have the train be in rear of the border.	Exceedance of safe speed /distance by train	The reported train position is incorrect/The positioning error has not been foreseen	Collision	PR	CA	IT	RE-NRBC-3	The positioning error must be taken into account. GNSS Receiver integrity monitoring system must be SIL4 system.	Specific procedures shall be established for RBC-RBC border zone delimitation.	IM	CR	TO	Design/ Operation	

Table 18. RBC – NRBC interface