D2.1 - Modelling of the moving block signalling system

Deliverable ID	**D2.1**
Deliverable Title	**Modelling of the moving block signalling system**
Work Package	**WP2**
Dissemination Level	**PUBLIC**
Version	**2.0**
Date	**2019-01-28**
Status	**Released**
Lead Editor	**SIRTI**
Main Contributors	**ARD, ISMB**

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
0.0	2017-09-15	ARD	First Draft with TOC
0.1	2017-09-29	ARD	First draft of the chapters 1 and 2.
0.2	2017-10-03	ARD	Completion of the draft chapter 1 and 2.
0.3	2017-10-16	ARD, SIRTI, ISMB	Completion of the chapters 1, 2, 3 and draft version of the chapter 5.
0.4	2017-11-06	ARD	Re-arranging of the chapters 1, 2 and 3, draft version of the chapter 4, completion of the chapter 5.
0.5	2017-11-24	ARD, SIRTI	Completion of the deliverable for final internal revision
0.6	2017-11-28	ARD, CNR	Commentaries addressed regarding Moving Block System model
1.0	2017-11-29	ARD	Release of the Final version
1.1	2018-06-01	ISMB	Added legal notice
1.2	2019-01-10	ARD, SIRTI	Correction according to the comments received from the reviewer
2.0	2019-01-28	ARD	Version release

Legal Notice

Table of Contents

1 Introduction

1.1 Objectives

Deliverable 2.1 aims to model the logical functionality of moving block signalling system without trackside detection, as an output of the tasks 2.1 and 2.2 from ASTRail WP2. The system modelling is the first approach to the deployment of evaluation as well as the definition of the system use cases for further hazard analysis. UML state machine diagram will be used in order to visualise the workflow, structure, and behaviour of a system, relationships and interaction of its elements. This model will allow to visualise interfaces between elements and segments of the system and to analyse the sequence “error- faulty state- failure”.

The focus will be put on user segment of GNSS technology; functions and properties of GNSS receiver and localisation unit will be described.

At this stage of analysis (which correspondent to Phase 1 and 2: Concept according to CENELEC 50126-1), it is necessary to develop a level of understanding sufficient to enable its proper Safety analysis, define the system, its mission profile, boundaries and uses cases.

For this purpose, the system architecture and a system model will be elaborated. Modelling represents a simplification of reality but allows to understand the causal relationships, highlight crucial factors and functions enabling the further inductive analysis on events that can trigger hazardous situations.

In parallel with system modelling, the main system use cases will be defined analysing significant system operative conditions. The blueprint of use cases in a range of conditions such a normal operation, degraded operations, transition phases, system initialization, critical failure and recovery from failure will be defined using UML diagrams, taking into account the type of traffic and Grade of Automation of the system being these the external to the system factors.

The main scenarios will be defined in terms of:

- traffic type and density;
- system states;
- environmental conditions;
- Grade of Automation.

This is necessary to be able to allocate safety and performance requirements, to define possible errors and faulty states and analyse their impact on operation.

1.2 Scope

The deliverable D2.1 gathers the results of Task 2.1 and 2.2 which include the modelling of moving block signalling system without trackside detection and the definition of the use cases for further safety analysis.

The interlocking functions are considered out of the scope of the safety analysis. Some of the functions mentioned in the document are only informative and are provided for better understanding of the interface of moving block system to interlocking (Route Management System).

For the train detection function, the focus will be placed on GNSS- based solutions.

1.3 Document structure

Deliverable D2.1 consists of the following parts:

1. Introduction;
2. State of the Art: Moving block, ERTMS level 3, GNSS application in railways;
3. Methodology: Introduction to UML State Machine diagram and UML Sequence Charts;
4. Functional modelling and architectures: moving block signalling system without trackside detection;

5. System Use Cases: classification;
6. System Use Cases: modelling with UML Sequence Charts;
7. Conclusion.

1.4 Related documents

ID	Title	Reference	Version	Date
[RD.1]	Reserved			
[RD.2]	Reserved			
[RD.3]	Reserved			

1.5 Terms and Definitions

Localisation is the determination of the geographical movement state of a certain means of transportation (that means location and speed according to amount and direction in relation to a point of reference of the vehicle) in a spatial reference system.

Navigation is defined as: localisation of a vehicle and its guidance from a location to a destination. Navigation is also defined as the science of getting ships, aircraft, spacecraft or people from place to place; especially: the method of estimating location, course, and distance travelled.

Positioning is a process of putting an object in a place.

Position is the information of a place related to a coordinate system.

Hazard: a condition that could lead to an accident

Reliability: The probability that an item can perform a required function under given conditions for a given time interval.

Availability: The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval assuming that the required external resources are provided.

Maintainability: The probability that a given active maintenance action, for an item under given conditions of use can be carried out within a stated time interval when the maintenance is performed under stated conditions and using stated procedures and resources.

Safety: Freedom from unacceptable risk of harm.

Safety Function: A safety function is defined as a function to be implemented by a safety-related system, this system is an Electric/Electronic/Programmable Electronic system, another technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the Equipment Under Control, in respect of a specific hazardous event. A safety function is not part of machine operation: if such a function fails, the machine can still operate normally, but the risk of injury from its operation increases.

Safety Integrity: The safety integrity is defined as the likelihood of a system satisfactorily performing the required safety functions under all the stated conditions within a stated period of time.

2 State of the Art

2.1 Train detection systems

The general purpose of train detection system is to gain information about the position of each train on the railway network, so the detection systems receive, transmit and evaluate this information.

When it is referred to the detection of rail vehicle the following particular information can be relevant:

1. A train has reached a certain point with its front end (End of Authority, Target\danger point).
2. A train has passed a certain point with its current rear end. This does not necessary imply that the train is complete, so no information of “lost” wagons is given.
3. A particular track section is clear of vehicles.

Important factors in determining the design and the technical efforts of a detection system are the safety requirements, where two groups can be distinguished:

- Safety related purposes are those whose failures can cause accidents (either alone or in combination with other errors). The requirements for the components are very high to ensure safe working in all possible conditions such as different speed f trains, different weather conditions, etc. The safety purposes can be further distinguished in terms of whether the erroneous non-detection or the erroneous detection at the wrong time can cause danger.
- Not safety related purposes are those where errors can result in disadvantages such as delays, wrong information to passengers and economic losses, but cannot cost human life or damage equipment.

The technical components for detection can be divided into two major classes:

1. Track-based detectors where the active elements are installed in or near the track (e.g. axle counters, track circuits).
2. Train-based detectors where the active elements are installed on the train, such as positioning of trains by satellites.

Nowadays, most of the detection systems are class 1 (trackside active elements) system and require fitting the infrastructure with active elements along the lines which is very expensive, particularly for maintenance. The introduction of class 2 (trainborne active elements) detectors would allow to reduce these costs, nevertheless as already highlighted, the safety aspects of detection systems are paramount, so the class 2 detectors shall provide at least the same safety level than track-based detectors.

On the other side, the detection systems can be further divided according to detection continuity:

1. Spot (discrete) detection (e.g. axle counters, virtual balises);
2. Linear (continuous) detection (e.g. track circuits);

The usage of continuous detection system provides some advantages such as easier and more reliable track clear detection, protection of train integrity, transmission of block information, interface to train protection and cab signalling. On the other hand, linear detection requires continuous availability and the risk of hindering failures is greater, also there are some specific requirements to railway superstructure.

In the ETCS level 2 system the train detection is performed by track circuits that transmit occupancy data to Route Management System, additionally, an odometry system is installed on board to provide continuous information of train position and direction to RBC through radio network (each 5 – 7 seconds). So, the train movements are monitored continually by the RBC.

Al this level, the Eurobalises are used as passive positioning beacons or electronic milestones.

In ETCS level 2 and 3, Eurobalises are used for a number of functions. Some of them might still require Eurobalises in the track for safety reasons, but most balises are only used:

- as reference points to allow the train to determine its exact position when passing the balise,

- to allow the train to report its position in reference to that location to the trackside system and
- to allow the trackside system to transmit data describing track conditions as well as movement authorities to the train again using balises as locations reference.

Between two positioning beacons the train determines its position via sensors. The positioning beacons are used in this case as reference points for correcting distance measurement errors. The on-board computer continuously monitors the transferred data and the maximum permissible speed.

The ETCS Level 2 constitutes a continue ATP/ATC with interoperable Cab Signalling and fixed block with block sections.

Odometry measures the position through the number of wheel rotations and systems with Doppler radar via speed and time. In all relative systems, measurements errors (e.g. in odometry by the train slipping and sliding) sum up, therefore the position has to be corrected at absolute control points.

The accuracy of position provided by an Odometer is, according to ETCS System Requirements Specification (SRS) requirement, 5% of the distance from the last reference point (balises group that allows to reset position) +/- 5m.

2.2 Principle of moving block

Traditional signalling systems are based on so called ***fixed blocks*** concept, the railway is divided into sections of track, which are separated by signals. A train is not allowed to enter a given track section (=block) before the preceding train has left it.

This system has some disadvantages, one being its lack of flexibility. Blocks are invariant. Therefore, block size is always the same regardless of train speed or braking performance. For this reason, blocks are determined considering the larger safety distances required by high speed trains, which are imposed on regular trains as well provoking a reduction in track capacity.

Nowadays in some applications a new concept is substituting the traditional signalling systems, it is the moving ***block* concept** which instead of requiring fixed track sections to determine train position, it relies on ***continuous two-way digital communication*** between ***trains*** and a trackside ***control centre***.

In a moving block signalling system, the railway line is usually divided into areas or regions, and each of them is controlled by a computer using the radio transmission system. Each train transmits its identity, location, direction and speed to the computer of the area, which calculates the safe train separation and sends the information to the following train. The radio connexion between trains and computers is continuous. Therefore, a computer constantly knows the location of all the trains in its area. It informs to trains the location of their previous train and provides them a braking curve to enable them to stop before they could reach a train. In effect, it is a ***dynamic distance-to-go system***.

It must be highlighted that in the assumption that all trains were travelling at the same speed and they all had the same braking capabilities, they could theoretically run as close together as a few metres (e.g. about 50 metres at 50 km/h). Railway safety principles require that the distance to go permitted for a train is such that collisions with the preceding trains are excluded. For this reason, it is determined a minimum distance between trains calculated as a full speed braking distance. This ensures that in case of losing the radio connection, the latest data received by the train will ensure that it stops before reaching the preceding train.

Even this way the introduction of moving block signalling systems results in a safer and more efficient way to manage railway traffic, since what distinguishes moving block from fixed block is that it makes the block locations and lengths consistent with train location and speed, i.e. making them movable rather than fixed. A representation of the two concepts can be seen in the Figure 1.

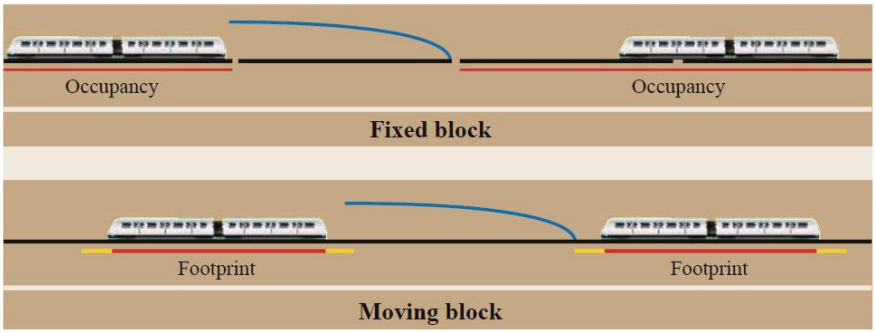


Figure 1 -Fixed block and moving block concepts (Teunissen & Montenbruck, 2017, p. 858)

In general, we have the three cases:

- MA until the entry of the fixed block section occupied by the preceding train
- MA until the current location of preceding train tail ("classical" moving block)
- MA until the future location of the preceding train tail, in case of its sudden braking with maximum efficiency

2.3 ERTMS level 3

An example of a system that contains moving block signalling principle is ERTMS level 3 system.

ERTMS is a system created to substitute the several existing signalling systems currently coexisting in Europe and to provide an economic and technical solution to the railway interoperability. Its objective is to facilitate fast and efficient train traffic across borders in Europe. ERTMS introduces, with its level 2 and 3, radio communication intended to substitute current track to train communication based on optical signals and dedicated systems (like track circuits). Level 3 also includes the use of radio communication (integrated by on-board train integrity confirmation equipment) to send to the control centres train location information permitting the elimination of train detection systems.

ERTMS defines three operation levels to simplify the migration to the new standard where ERTMS level 3 is the most advanced application. In this operation level radio communication replaces the traditional trackside signals, resulting in considerable savings in infrastructure and maintenance costs. Therefore, trains actively report via radio communication their location and their integrity to radio block centers (RBC) periodically. RBC traces the locations of trains, and transmits track descriptions as well as movement authority messages to both Route Management System and trains which are in their area.

ERTMS Level 3 has experienced a significant growth of interest in recent times. The fully integrated advanced level train control system does not use wayside signals, as all the information is transmitted using wireless communications. The Level 3 concept has a potential to make a significant impact on the train control systems, in spite that some pilot lines have been already deployed to prove the technology (e.g. 3inSAT), its applicability for all railway profiles shall still be confirmed.

ERTMS is composed by two basic elements: ETCS (European Train Control System) and GSM-R (GSM for Railways). ETCS is in charge of transmitting permitted speed and movement information to the driver, as well as monitoring constantly the driver's compliance with these instructions. GSM-R is the current radio system used to transmit information between the track and the train that, nevertheless, will be substituted by more advanced IP based communication system that will provide faster connection and greater capacity.

In Figure 2 an scheme of ERTMS level 3 operation is represented, it can be seen the information flow between equipment.

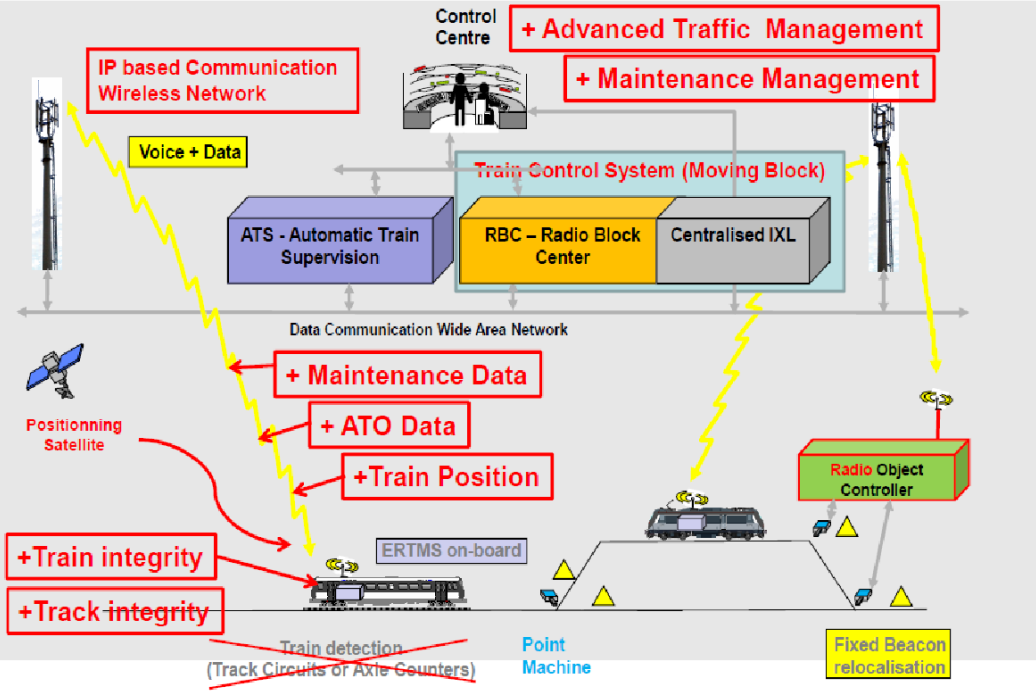


Figure 2 - ERTMS level 3 operation

2.3.1 Description of ETCS Level 3

ETCS is the signalling and control component of the ERTMS (European Rail Traffic Management System) and its development is managed by EC (European Commission) and ERA (European Union Agency for Railways) through the Change Control Management and taking care of political, strategic and legal aspects (TSIs, Deployment plans, etc) to blend ATP (Automatic Train Protection) across numerous European ATP systems. The main purpose of ETCS was to replace incompatible safety systems used by European railways. Subsequently, this standard has been successfully adopted outside Europe.

ETCS is implemented with the standard trackside equipment and the unified controlling equipment in the train. The trackside information is transferred to the driver, without requirement of trackside signals. ETCS Level 3 does not require trackside detection components and does not operate at fixed intervals. It uses the onboard equipment to obtain positioning data signals and achieve continuous line-clear authorization.

ERTMS Level 3 is characterised by the fact that the train determines its own location, using position references transmitted by fixed Eurobalises, its on-board odometry or satellite based navigation systems. It transmits this location data to the Radio Block Centre, which issues movement authorities to the trains under its control.

2.3.2 Functional specification ETCS Level 3

ETCS level 3 requires the implementation of a moving block signalling system which should contain the following components basic functionalities.

Block (i.e. train spacing): when this functionality is performed by a control centre, it must have a track layout, with reference locations that can be used to define position information used in communication between centre and trains.

Train detection: the ability to locate train heads and tails and position them on the representation of the track lay-out (digital track map).

Recognising reference locations: locations must be positioned on the track lay-out used by block systems. The train must be able to recognise them when passing. This can be done in two ways: either installing punctual transmission system on the track, sending the identity of the reference location to the train; or associating the identity of the reference point to a GNSS location and making the train aware of this association (see NGTC deliverable D7.1 on the Virtual Balise concept)

To be noted that in all cases it is important for the train to distinguish the direction in which the reference location has been passed, with reference to the orientation of the track (this means that the orientation of the track is part of the representation of the lay-out used by the centre).

Location of train heads: the train, after passing a reference location, must continuously evaluate the distance of its head. This implies the availability on-board of an odometry system. The odometry system can exploit different technological solutions. If it is not accurate enough, an odometry correction function can be implemented on-board, exploiting reference locations, whose distance is communicated to the trains.

Location of train tails: this location can be evaluated on-board, on the basis of location of the train head, the train length and the confirmation of train integrity.

Communication between centre and trains: all communications between a train and the centre require a shared information about the location of the train and the location of specific positions on the trackside. This implies that the reference locations used in a certain rail system have each a unique identifier, used for train to track communication.

Protection of critical locations: this can be done associating such critical locations to the identity of a reference locations and even without necessary having a reference location placed at the critical location, if the centre knows the distance of these locations with respect to reference locations. Figure 3 shows how they are integrated in the overall signalling and train protection system.

Note: it is assumed that the functionality “Train detection (mobile)” keeps an updated database of position of train heads and tails, in suitable coordinates for the use by other functions.

All functionalities share the access to a track description data base (for the parts that are relevant for them). This data base is configured with all information relevant for MAs (maximum speed, gradients, etc.) In addition, it is assumed that, during operation, this data base can be temporarily modified to introduce speed reductions, included zero speed (i.e. stop locations that trains cannot pass).

According to implementation, the track description data base can use the same coordinates as GNSS, or a simplified coordinate system. In this case, use of GNSS requires that at least for a certain number of reference location the correspondence between GNSS coordinates and track description coordinate is specified. To be as general as possible, in the following functional and safety analysis it will be considered that the location functions communicates to other system functions information subdivided in “elementary elements “ (passed reference position, direction, distance), to analyse separately the effects of errors in each of them.

The scope of the following functional description is not a full specification of all functions, data structure, etc, to implement moving block: the scope is to specify the context where location information generated by GNSS is used, to understand the consequence of GNSS errors and give a functional basis for the causal analysis leading to the specification of safety and performance requirements for GNSS use.

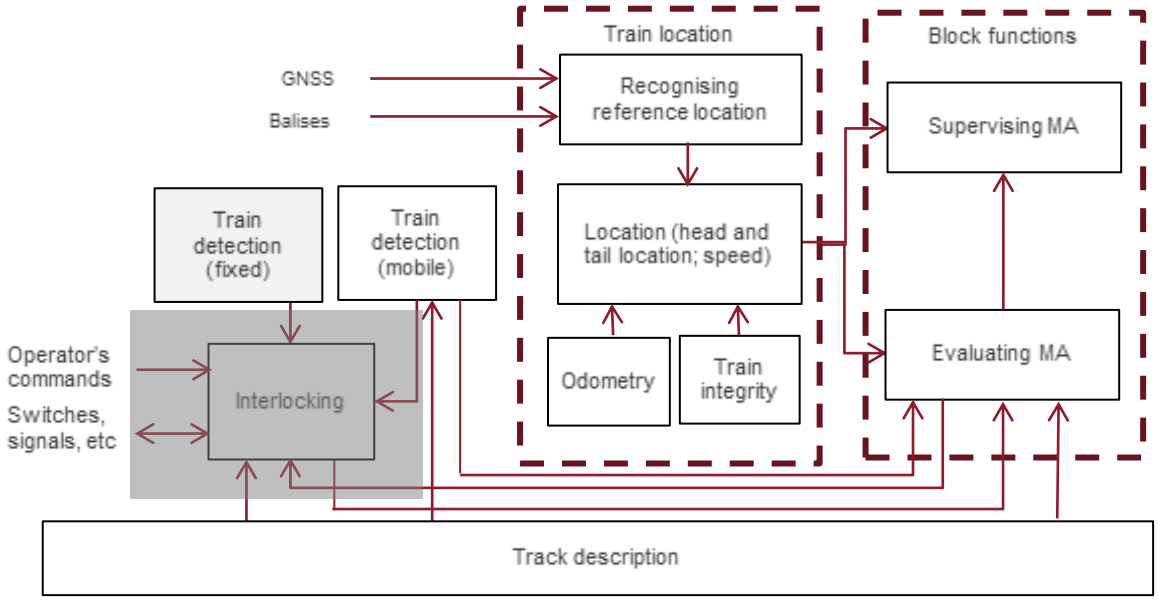


Figure 3 - Overall architecture of train protection system

2.4 Functions of GNSS-based moving block system

The basic functionalities that can be implemented using GNSS are listed in the table below:

Location of train head	Odometry
Location in GNSS coordinates	Measurement of space
Identification of passage on a reference location (including direction)	Correction of measured space
Measuring of distance from the last passed reference location (see odometry)	Measurement of speed

Table 1 - GNSS application functionalities

On the other hand, making reference to the overall architecture for moving block, the GNSS basic functionalities also have impact on the following moving block functions summarized in table below:

General functions	Block functions	Odometry functions	Other protection functions
Updates the trains position	First movement authority to a train	Measurement of distance from the last passed reference location	Stop or reduce train speed before specific locations
Initialisation of train-centre communication when the train knows its position	Extension of a route according to advancement of the train in front		

Initialisation of train-centre communication when the train does not know its location and need to be moved until a reference location is met	Extension of a movement authority into a route, when only one train is permitted in a route	Correction of measured distance Measurement of speed
	Extension of a movement authority into a route, when more train can follow each other in a route	
	Supervision of a movement authority	
	Train moving without movement authority (staff responsible or shunting)	

Table 2 - Moving block system functions

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 3. Moving Block Components Safety functions

2.4.1.1 *ETCS level 3 operational issues*

There are important operational issues related to communication that may affect safety in moving block systems, where train detection systems are not installed:

- No train unable to communicate its position can be permitted to enter and/or move in the rail system, unless appropriate operational procedures are applied (e.g. keeping the non-communicating train inside an area supervised by trackside personnel and defining in the control centre stop locations to prevent other trains to receive authorities inside this area). This procedure can be used to manage degraded situations;
- If, for any reason, the communications between a train and the centre are interrupted, the train must stop at the end of its current movement authority and the centre must consider "occupied" all the tracks from the last reported location of the train tail and the end of the movement authority;
- If a train loses confirmation of its integrity, the centre must consider that the train tail remains at the last reported location;
- If, at start-up, a train is not able to report a location to the centre, it must be permitted to move under operational control until it meets a reference location known to the centre, possibly applying the precautions specified in bullet a above;
- Special precautions must be taken in the centre, in case of trains moving on routes with defective switches or switches not controlled by an Route Management System.

ASTRrail will not perform detailed safety analysis of the above situations, but this will be taken into consideration in the evaluation of the severity of consequences of GNSS errors.

2.5 Other moving block signalling systems

CBTC (Communication Based Train Control) is the only application of moving block signalling currently in operation. This system was developed for urban rail systems and it should be highlighted that despite sharing the same principle and overall architecture, every application is a proprietary solution, where the concrete configuration and implementation method depends on supplier and Urban IM. For this reason, there are low possibility to have an interoperable system based on CBTC solutions.

In this section the common definition and concept design of CBTC system is detailed.

Within the 7FP, NGTC (Next Generation Train Control) project has been developed with the main goal of analysing the commonality and differences of the required functionality of both ETCS and CBTC systems, and determining the level of commonality of architecture, hardware platforms and system design that can be achieved. The project does not seek to develop a system of -one size fits all-, but to make progress in all railway domains in terms of increasing the commonality in system design and hardware, with various benefits such as:

- Increasing economies of scale for suppliers,

- Offering customers the benefit of being able to choose the most competitive supplier, based on standardized functions and interfaces.

In addition, other topics that NGTC will address in detail are:

- Enhanced and unified Moving Block principles
- The usage and development of the IP-based Radio Communications, several possible uses of satellite-related technologies, etc.

The work is based primarily on the practical experience within urban railways, but is taking into account the specifications contained within the ETCS Baseline 3 for ETCS Level 3 systems. Basic assumption applied is that there is no trackside train detection available for the moving blocks. According to the results of NGTC project, by migrating to a moving block system, the system operator gains the following:

- Capability to run trains much closer together resulting in shorter headways;
- Adaptive distance between trains according to actual train speed, which makes efficient use of the infrastructure;
- Reduced wayside equipment, resulting in reduced maintenance & life cycle costs;
- Reduced wayside equipment, resulting in improved reliability;
- Bi-directional operation at much reduced cost.

3 Methodology

3.1 Working plan

During the system modelling phase, great emphasis will be placed on assuring that the system model provides an as accurate as possible representation of reality.

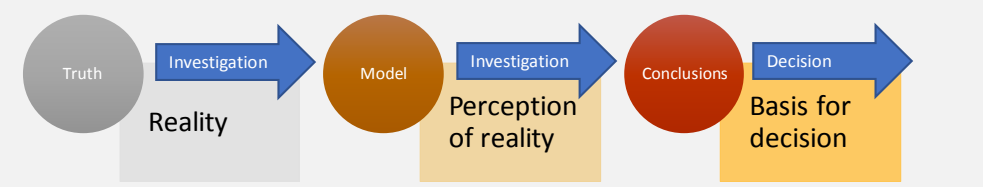


Figure 4 – System modelling workflow

Since any system is made up of parts or subsystems that interact it cannot be simply equal to the sum of its parts, as it is in the physical nature of any part changes-for example by failure: the resulting system will have to undergo a new analysis as a whole. For these reason, it is of utmost importance to use a method that is able to provide the information about system state changes. So, for Moving Block system modelling UML state machine diagram will be used in order to visualise the workflow, structure, and behaviour of a system, relationships and interaction of its elements along with the definition of external boundaries.

This model will allow to visualise interfaces between elements and segments of the system and to analyse the sequence “error- faulty state- failure”. To perform this analysis Inductive method (sometimes described as What If method) will be applied constituting reasoning from individual cases (errors and faults) to a general conclusion (failures). This method is chosen since it can provide a valid and systematic way to identify and correct undesirable or hazardous conditions at the Preliminary stage of system development.

3.2 UML state machine diagram

UML is a standardized object-oriented modelling language used to specify, visualize and produce models of systems using graphic notation, i.e. diagrams. Each diagram defines and graphically visualizes one view or aspect of the modelled system. The aim of UML is to simplify the understanding of complex systems by exploiting visualization representation. The UML conceptual model is created by connecting shapes, which represent an object or class of the modelled system, among them using specific connectors, which identify relationships and the flow of information.

The vocabulary of the UML includes three kinds of building blocks: things, relationships and diagrams. Things are the abstractions of the modelled system, relationships tie things together, diagrams group interesting collections of things. In UML two main categories of diagrams have been identified: structure diagrams and behaviour diagrams. The structural diagrams represent the static model of the system and it defines the stable main structure of the system to be modelled. The behavioural diagrams represent instead the dynamic behaviour of the system and they illustrate how the system changes over time.

Among the behavioural UML diagrams especially the State Machines are suitable for modelling the systems behaviour. Sequence charts and collaboration diagrams describe single cycles inside the system and therefor they are not directly useful for investigation of the whole behaviour. The UML state machine diagram is a behavioural diagram since it determines the various states that an object may be in and the transitions between those states. A state represents a stage in the behaviour pattern of an object, and like UML activity diagrams, it is possible to have initial and final states.

In the present deliverable, Real-Time UML State Machine Diagram is used as a tool to model the analysed system. This variant of UML State Machine Diagram provides an extra information to model real-time systems and allows the detailed specification of quantitative system properties. RT UML State Machine Diagram contains annotations from the SPT (Schedulability, Performance and Time) profile used to add timing information to the state machine. Real-time (RT) as well as performance (PA) stereotypes are introduced.

3.2.1 State Machine Diagrams

State Machine Diagrams capture the behaviour of a system. They can be used to model the behaviour of a class, subsystem, or entire application, and also provide an excellent way of modelling communications that occur with external entities via a protocol or event-based System.

State diagrams represent the behaviour of a system using graph notation. As its name indicates the main elements of this kind of diagrams are states and its transitions, which occur when events are dispatched.

3.2.1.1 States:

States model a specific moment or situation in the behaviour of a system. When an invariant condition holds true. It can represent a static situation or a dynamic situation where the state is actively processing data.

States are shown as a rectangle with rounded corners, and their name is written inside of it. Within the rectangle a state can be divided into compartments as needed. UML defines the following compartments:

- **Name**: shows the name of the state.
- **Internal activities**: shows a list of internal activities that are performed while in the state
- **Internal transitions**: shows a list of internal transitions and the events that trigger them.

A state can be either *activate* or *inactivate.* It is considered active as soon as it is entered through some transition. Similarly, it is considered inactivate immediately after leaving the state. In addition, a state can include several regions. A state with one or more regions is called a composite state. Regions are represented using a dashed line dividing the composite state. Each region may be named within the region's area. Furthermore, each region has its own *initial pseudostate* and *final state.* A transition to a composite state is a transition to the initial *pseudostate* in each region. Each region within a composite state executes in parallel, and it is perfectly acceptable for one region to finish before another. A transition to the final state of a region indicates completing the activity for that region. Once all regions have been completed, the composite state triggers a completion event and a completion transition (if one exists).

3.2.1.2 Transitions

A transition shows the relationship, or path, between two *states* or *pseudostates.* It represents the actual change in the configuration of a system as it heads from one state to the next. Each transition can have a guard condition that indicates if the transition can be considered (*enabled)*, a trigger that causes the transition to execute if it is enabled, and any effect the transition may have when it occurs. Transitions are shown as a line between two states, with an arrowhead pointing to the destination state. The details of the transition are specified using the following syntax:

Trigger [guard] / effect

where:

- *trigger:* indicates what condition may cause this transition to occur. The trigger is typically the name of an event, though it may be more complex.
- *guard:* is a constraint that is evaluated when an event is fired to determine if the transition should be enabled. Guards should not have any side effects and must be evaluated with a Boolean. Guards will always be evaluated before a transition is fired. The order in which multiple guards are evaluated isn't defined. A guard can involve tests of states in the current system.
- *effect:* specifies an activity that is executed when a transition happens. This activity can be written using operations, attributes and links of the owning classifier as well as any parameters of the triggering event. An effect activity may explicitly generate events such as sending signals or invoking operations.

3.2.1.3 Activities

An activity represents some functionality that is executed by a system. A state can have activities that are triggered by transitions to and from the state or by events raised while in the state. A state's activities execute only if the state is active.

Each activity has a label showing when the activity executes, and an optional activity expression:

Label / activity expression

The activity expression can be written using pseudocode or natural language. The slash may be omitted when the activity expression is not shown.

UML reserves three activity labels:

- *Entry:* triggers when a state is entered. The entry activity executes before anything else happens in the state.
- *Exit:* triggers when leaving a state. The exit activity executes as the last thing in the state before a transition occurs.
- *Do:* executes as long as a state is active. The *do* activity executes after the entry activity and can run until it completes, or as long as the system is in the state.

3.2.1.4 Stereotypes

A stereotype is one of three types of extensibility mechanisms in the Unified Modeling Language (UML), the other two being tags and constraints. They allow designers to extend the vocabulary of UML in order to create new model elements, derived from existing ones, but that have specific properties that are suitable for a particular domain or otherwise specialized usage.

RT UML State Machine Diagrams contain real-time (RT) and performance (PA) sterotypes. Several sterotypes can be found classiffied within these two groups. Nevertheless, in this deliverable Rtdelay, RTevent and Pastep are used with their respective tags which are briefly described in Table 4.

Stereotype	Definition	Tags
RTdelay	This models a pure delay action.	RTduration = *(value, units)* or *(distribution, parameter, units)*
RTevent	This models any event that occurs at a known time instant.	Rtat = *(value, units)*
PAstep	This models a step in a performance analysis scenario.	Paprob = *probability to dispatch the activty once it is enabled.*

Table 4 - Used Stereotypes

3.3 UML Sequence Charts

UML Sequence Chart is the most common kind of interaction diagram, which focuses on the message interchange between a number of lifelines.

Sequence diagram describes an interaction by focusing on the sequence of messages that are exchanged, along with their corresponding occurrence specifications on the lifelines.

The following nodes and edges are typically drawn in a UML sequence diagram: lifeline, execution specification, message, combined fragment, interaction use, state invariant, continuation, destruction occurrence

UML state machines and UML Sequence Charts are both behavioural diagrams and their modelling represents the steps in a process. UML state machines are quicker to create and at more of a 'high level', showing the information flow, but not when or in what order the information flows.

Sequence Charts take the classes with their data and operations, plus the general behaviour modelled in the activity diagrams, and show how it all fits together.

Lifelines (dashed vertical lines) with associated rectangles are used to represent the system components participating in the process (Location unit, On-board Unit (EVC) or RBC).

A rectangular activation box is placed over the lifeline (or on top of another activation box) to indicate when and how long something is being done.

Time in a sequence diagram is all a about ordering, not duration. The vertical space in an interaction diagram is not relevant for the duration of the interaction.

The messages exchanges between actors are represented with arrows, where dashed arrow represents the reply to previous message.

USC allows to introduce the actors external to the system (e.g. Driver/ATO), and alternative options (e.g. position is available/ position is unavailable).

This tool is recognized to be an adequate tool for Use Cases modelling.

4 Functional modelling of the moving block system

4.1 Assumptions

The Moving block system without trackside detection model has been performed with the following considerations:

- The model shall be applicable for each possible use cases, thus only common features have been represented. Numerical parameters of performance can be adjusted to the chosen line type since the speed and the density (the distance between the trains) will be principally impacted by the update rate of positioning information and the maximum time to receive valid MA.
- RBC and OBU (EVC) are highly reliable devices already developed and proven in numerous railway applications. It is assumed that they are SIL4 devices compliant with all RAMS requirements.
- The “location unit” is a device installed on-board that provides positioning information according to Virtual Balise principles, so the ERTMS/ETCS system functions stay unchanged. Location unit can provide positioning data whenever required thanks to odometer functions.
- The radio communication link is established through a new generation IP based communication system and are compliant with the new mission critical specifications proposed by 3GPP. This system will be a GSM-R substitute, since GSM-R is close to be obsolete system and it is insufficient to cope with the growing demand of digital applications in Railways.
- The numerical values in the Table 8 are given based on existing requirement specifications for the parts of the system, assuming the components shall be compliant with them before the integration.

4.2 Virtual Balise principle

The possible solution for the train accurate positions is to replace existing physical balises, that provide the reference location, by GNSS- based virtual balises that will perform the same function. The system shall detect when the train reaches a virtual balises previously identified and recorded in the map database. Nevertheless, this approach requires additional study on accuracy and availability of virtual balise concept, the issue that does not exist with physical balises.

The requirement to minimize the impact to ETCS when applying GNSS led to the concept of “virtual balises”, which are predefined reference locations similar to balises, but without an actual Eurobalise installed. This is achieved through:

- The installation of a GNSS based onboard unit, subsequently called “virtual balise reader” continuously determines the train’s position in GNSS coordinates,
- it continuously compares this position to a list of reference points which are known to the virtual balise reader with their GNSS location coordinates
- it then indicates to the ETCS onboard system a balise passage by reporting the respective “virtual balise” information each time one of these locations has been reached. The “virtual balise” information includes the maximum estimated balise location error, or an information to compute such an error.

From that point, all ETCS functions and processes shall remain unchanged.

A number of safety related issues must be analysed in relation to Virtual Balise concept:

- Whether it is possible to achieve SIL4 level for all the applications (safety of GNSS positioning is proven so far in a less critical environment, with lower accuracy requirements);
- Robustness against environmental impacts (e.g. multipath effect);
- Backup system if GNSS signal is not available.

These issues will be further investigated in ASTRail WP1.

In the present document it is assumed that “location unit” provides positioning information according to Virtual Balise principles, so the ERTMS/ETCS system functions stay unchanged.

4.3 User requirements for railway GNSS applications

To investigate the performance and quality levels of GNSS positioning as required for railway applications, the European Rail Advisory Forum has proposed three main classes of applications, safety, operational, and professional. A summary of these applications and their positioning specifications is presented in Table 5.

Application	Requirement							
	Horitzontal accauracy[a] (m)	Integrity alert limit[b] (m)	Integrity max. time to alarm[c] (s)	Availability[d] (%)	Service interrupt (s)	Continuity[e] (%)	Coverage[f]	Fix rate (s)
Safety-related applications								
ATX on high density lines	1	2,5	<1,0	>99,98	<5	>99,98	ELM	1
Train control on medium density lines	10	20	<1,0	>99,98	<5	>99,98	ELM	1
Train control on low density lines	25	50	<1,0	>99,98	<5	>99,98	ELM	TBD
Mass commercial/information and management – operational applications								
Tracking and tracking of vehicles	50	125	<10	99,9	TBD	TBD	ELM	TBD
Cargo monitoring	100	250	<30	99,5	TBD	TBD	ELM	TBD
Dispatching	50	125	<5	99,9	TBD	TBD	ELM	TBD
Passenger information	100	250	<30	99,5	TBD	TBD	ELM	TBD
Infrastructure and civil engineering, professional application								
Positioning of machines	0,01	TBD	<5	99,5	TBD	TBD	Operating area	TBD
Infrastructure survey	0,01	10^{-3}	<10	99	TBD	TBD	ELM	TBD
Fix point applications	0,005	TBD	<30	99	TBD	TBD	ELM	TBD

a Accuracy is specified as the position error at 95% confidence level.
B Threshold value or alert limit – the maximum allowable error in the measured position before an alarm is triggered.
C Time-to-alarm – the maximum allowable time between an alarm condition occurring and the alarm being present at the output.
D Defined as intrinsic availability: This is the Probability that a system or equipment is operating satisfactorily at any point in time when used under stated conditions, where the time considered is operating time and active repair time.

E Continuity is defined as the probability that the location unit will be able to determine its position within the specified accuracy and is able to monitor the integrity of the determined position over the mission time, in all points of the route within the coverage area.
F The coverage is defined as the surface area or volume of space where the SIS service is sufficient to permit the user to determine its position with the specified accuracy and to monitor integrity of the determined position.

Table 5 – GNSS positioning requirements for different classes of railway applications (TBD: to be defined; ELM: European Land Mass) (Teunissen & Montenbruck, 2017)

The required navigation parameters for a railway locator are defined as Coverage, Accuracy, Integrity and Availability:

Integrity

Integrity is the parameter, which describes safety. The integrity function is ensured by providing a protection level value, if no feared events are detected in the system. The protection level bounds the position instantaneous error with required probability. This probability comes from an apportionment of safety requirements.

The protection level can be provided as horizontal protection level or as longitudinal protection level, at it is time-dependant value.

Coverage

The fundamental parameter that determines the quality of service to be obtained from a GNSS based positioning system is the coverage obtained from the satellite constellations;

Accuracy

Accuracy is a part of the performance requirement and is relevant to safety when the inaccuracy present at any time could cause the safety margins (position and speed information) to be exceeded.
Accuracy can be expressed as horizontal accuracy (a radius with centre in the estimated position where the true position should be within the circle with 95% probability), or as longitudinal accuracy (accuracy is a half of the interval with centre in the estimated position where the true position should be with 95% probability in this interval).

Accuracy is time-dependant value.

Availability

If the protection level of position/velocity exceeds the corresponding alert limit, or it is not possible to determine the protection level of position/velocity, the service is declared as unavailable.

Availability is expressed as a percentage of time, when the service provides at least the required minimal performance, i.e. when the protection level is below the corresponding alert limit over the interval of interest.

4.4 Functional model

Moving Block has been modelled using UML State Machine Diagrams described in Methodology. It has been considered that moving block is constituted by several regions, each of them models a function or process performed in the system. Functions can be classified in two groups depending on the nature of the process. Some function aim sharing data and information between units, however some other functions process the data and lead to some calculations.

In Table 6 the regions identified are listed and the pseudostates that can be found in each region as well as a brief description of the modelled function within the region. Subsequently in Table 7 can be found the respective

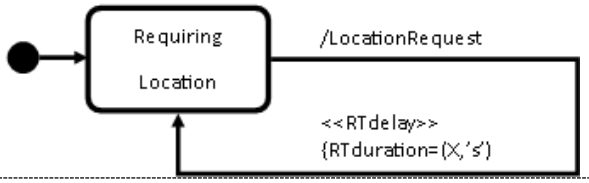
diagrams for each function and region as well as the events that trigger these function and transitions from one pseudostate to the next one.

ID	Region	Pseudostate	Description
OBU 1	Generation of location request	Requiring location	Every fixed interval of time the On-board Unit generates a request of its location.
TCOM 2	OBU sends location request to Location Unit	Empty Full	The On-board Unit sends the location request to the Location Unit.
LU 3	Processing location request and calculating location by Location Unit	Idle Busy	Once the Location Unit has received the location request, it processes it and calculates the location.
TCOM 4	Sending location from Location Unit to on-board Unit	Empty Full	The Location Unit sends location to On-board Unit.
RCOM 5	Sending location from on-board unit to RBC	Empty Full	Once the On-board Unit receives its location it sends it to RCB.
RBC 6	Processing information and calculation of movement authorities by RBC	Idle Busy	Once the RCB receives the location of the trains it processes the information and calculates Movement Authorities.
RCOM 7	Sending movement authority to train	Empty Busy	RBC sends Movement Authorities to On-board Units.
CON 8	Controlling	Counting Stopped	On board Unit controls the reliability of the MA and activates the emergency stop when the MA available becomes too old.

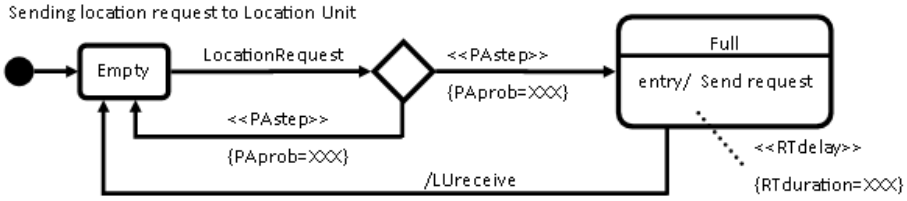
Table 6 – Summary of regions and pseudostates modelled

Moving Block

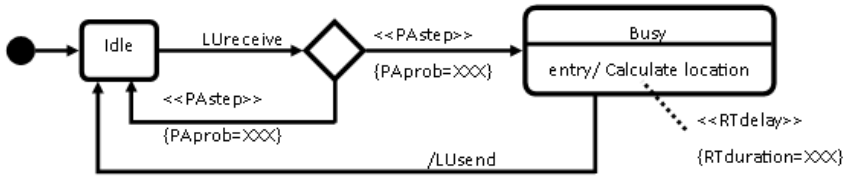
Generation of location request



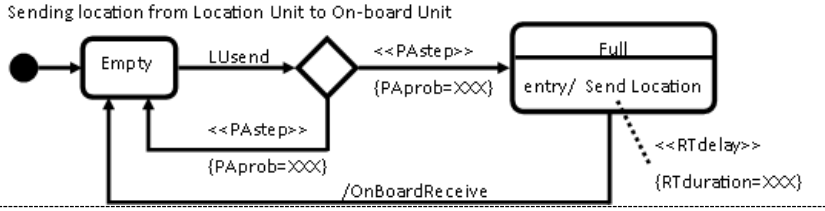
Sending location request to Location Unit



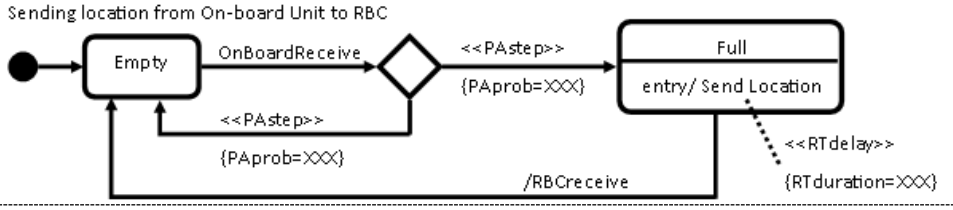
Processing location request and calculating location by Location Unit



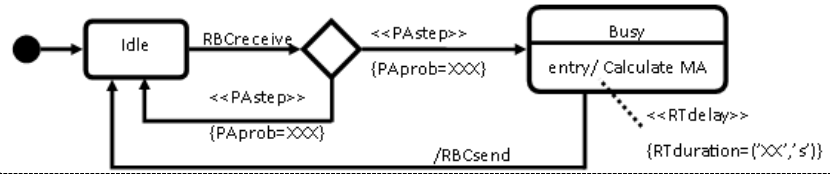
Sending location from Location Unit to On-board Unit



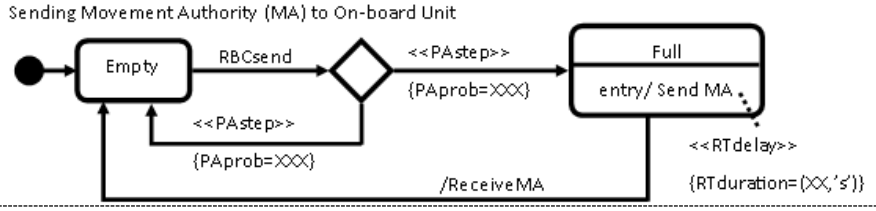
Sending location from On-board Unit to RBC



Processing information and calculation of Movement Authorities by RBC



Sending Movement Authority (MA) to On-board Unit



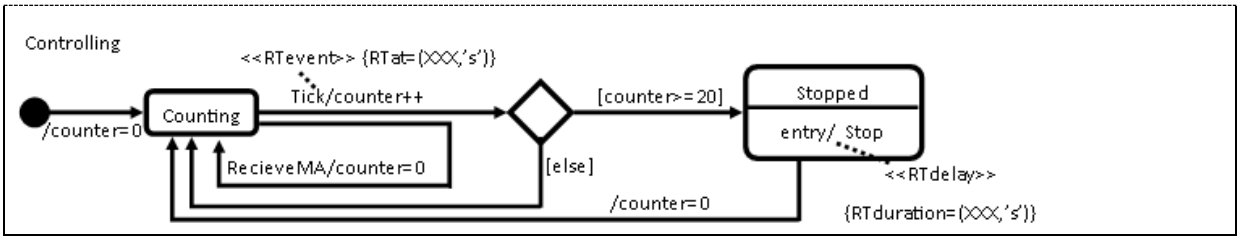


Table 7 – UML State Machine Diagrams for Moving Block

Within the processes described in the Table 7 the MA is extended automatically to the train, it shall be noted that when the train initiates its trip for the first time On-board Unit shall request the MA to the RBC. Nevertheless, the objective is to run in FS whenever possible, and the system must be designed to achieve this at the earliest opportunity. The train will automatically receive new ERTMS Mas as required, as long as it is safe to provide them.

4.4.1 Performance parameters

From the moving block functional model the following performance parameters can be deduced:

Stereotype	Component	Function	Range	Note
Rtdelay	Location Unit	Generation of location request	Rtduration = *1 update each 5 second*	Standard rate of update in MBS. In some lines this rate can be lower (e.g. 7 second in Italian Railways)
Pastep	Location Unit	Probability that LU will be able to answer the request	Paprob= 99,99%	Maximum achievable reliability in line on sight conditions
Rtdelay	Location Unit	Processing and answering location request	Rtduration = *1 update/sec (1 Hz)*	1 Hz is a standard rate for GNSS/GPS receivers Nevertheless, it can be upgraded to 5Hz
Pastep	On-board Unit	Probability of correct processing of positioning information	Paprob = 99,9999%	ERTMS/ETCS SRS

Stereotype	Component	Function	Range	Note
Rtdelay	On-board Unit	Processing of data received and report elaboration	Rtduration = 0,5 sec	
Rtdelay	Radio communications	Maximum delay for critical communications	Rtduration= 0,1 sec	Quantitative Mapping of service and QoS attributes (3GPP) Ref. [3GPP TR 22.889, 2018]
Pastep	Radio communications	Minimum Reliability of critical communications	Paprob = 99.9999%	Quantitative Mapping of service and QoS attributes (3GPP) Ref. [3GPP TR 22.889, 2018]
Pastep	RBC	Probability of processing correctly the report received and calculate MA	Paprob = 99,9999%	ERTMS/ETCS SRS
Rtdelay	RBC	Processing of data received and MA emission	Rtduration = 0,5 sec	
Rtdelay	Radio communications	Maximum delay for critical communications	Rtduration= 0,1 sec	Quantitative Mapping of service and QoS attributes (3GPP) Ref. [3GPP TR 22.889, 2018]
Pastep	Radio communications	Minimum Reliability of critical communications	Paprob = 99.9999%	Quantitative Mapping of service and QoS attributes (3GPP) Ref. [3GPP TR 22.889, 2018]
Pastep	On-board Unit	Probability of correct processing of MA received	Paprob = 99,998%	

Stereotype	Component	Function	Range	Note
RTevent	Counter	Counts ticks each RTat time	RTat=0,75 sec	Maximum number of ticks = 20 (15 sec deadline)
RT delay	Counter	Time when controlling function is inactive (emergency breaking)	RT duration=900 sec	

Table 8 – Moving Block system model performance parameters

5 System Use Cases

Moving block signalling system without trackside detection is characterized by the necessity to obtain reliable information about track location and integrity, monitor track status, detect faults (and infer their causes), maintain normal operation and carry out actions to assure safe operation in degraded situations, and improve network efficiency and application performance.

Basically, signalling system application periodically collects information from a set of managed elements, it processes the collected data, and then send commands to the elements (including trackside elements and trains). All the elements and the system itself, however, have different limitations, parameters and requirements. They might also need to work in diverse environments with advanced safety and security requirements and unfavourable external conditions which can derive in additional hazard and, consequently, in more demanding requirements for precision, accuracy, reliability, availability and integrity.

This chapters aims to understand use cases for the applications of Moving block signalling system without trackside detection. It lists and discusses diverse use cases from the network as well as from the application point of view.

The list of discussed use cases is not an exhaustive one since other scenarios, currently unknown to the authors, are possible. The application scenarios discussed aim to show where moving block signalling system are expected to be deployed. For each application scenario, the characteristics are briefly described followed by a discussion on how the safety functions can be performed, and which priority shall be given to the main system parameters.

The following scenarios are taken into account:

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 Degraded operation	The train know its location and is able to report. The train does not know its location.	GoA1 GoA2 GoA3 GoA4	Open Sky Environment Restricted environment Urban environment

Table 9 - Use cases scenarios

5.1 Railway profiles

According to the CEN, there exist 5 categories of the rail traffic lines based on the services they accommodate.

a) Mixed traffic lines for passenger trains, speed 80-120 km/h;

b) Mixed traffic lines for passenger trains, speed 120-200 km/h;

c) Mixed traffic lines for passenger trains, speed higher than 200 km/h;

d) Mixed traffic lines for passenger trains incorporating special design characteristics;

e) Dedicated passenger lines for passenger trains, speeds greater than 250 km/h.

Apart from speed, the core parameters that shall be considered are: number of trains per time interval and the heterogeneity of different running times for different train types.

The density parameters considered correspond to:

- Low density line: less or equal to 2 trains/hour in both directions.
- Medium density line: 3 -11 trains/hour in both directions
- High density line: more than 11 trains trains/hour in both directions

Regarding the type of the line, the following can be distinguished:

- Mainline Rail (MR) is a track that is used for a high variety of trains and often is the principal artery of the system from which branch lines, yards, sidings and spurs are connected. It generally refers to a route between towns, as opposed to a route providing suburban or metro services. For capacity reasons, main lines in many countries have at least a double track and often contain multiple parallel tracks. The operation speeds correspond to types b to c, and the density is medium to high, the time intervals between running trains are not heterogeneous.
- Regional Rail (RR) also known as local trains and stopping trains are passenger rail services that operate between towns and cities. These trains operate with more stops over shorter distances than inter-city rail, but fewer stops and faster service than commuter rail. The operation speeds correspond to types a to b, and the density is low to medium, the time intervals between running trains are quite heterogeneous.
- High-speed Rail (HSR) is a type of rail transport that operates significantly faster than traditional rail traffic, using an integrated system of specialized rolling stock and dedicated tracks. The traffic control and signalling system must guarantee maximum safety and reliability. The main characteristic of these lines is the speed (types c and d), while the density could vary depending on the demand, the time intervals between running trains are quite heterogeneous.

5.2 Grade of Automation

Concerning operation mode regarding the Grade of automation of trains, it refers to the process by which responsibility for operation management of the trains is transferred from the driver to the train control system.

There are several grades of automation (GoA), which are defined according to the basic functions of train operation that are the responsibility of staff, and the basic functions that are the responsibility of the system itself.

GoA takes values between 0 and 4. Grade of Automation 0 would correspond to on-sight operation. Grade of Automation 4 would refer to a system in which vehicles are run fully automatically without any operating staff onboard. The Table 10 - Grades of AutomationTable 10Table 10 illustrates the main characteristics of each possible grade of automation.

Basic functions of train operation		GoA0	GoA1	GoA2	GoA3	GoA4
		On-sight train operation	Non-automated train operation	Semi-automated train operation	Driverless train operation	Unattended train operation
Ensuring safe movement of trains	Ensure safe route	X (points command/control in system)	system	system	system	system
	Ensure safe separation of trains	X	system	system	system	system
	Ensure safe speed	X	X (partly supervised by system)	system	system	system
Driving	Control acceleration and braking	X	X	system	system	system
Supervising guideway	Prevent collision with obstacles	X	X	X	system	system
	Prevent collision with persons on track	X	X	X	system	system
Supervising passenger transfer	Control passengers' doors	X	X	X	X	system
	Prevent person injuries between cars or between platform and train	X	X	X	X	system
	Ensure safe starting conditions	X	X	X	X	system
Operating a train	Set in/ set off operation	X	X	X	X	system
	Supervise the status of the train	X	X	X	X	system
Ensuring detection and management of emergency situations	Perform train diagnostic	X	X	X	X	System and/or staff in OCC

Table 10 - Grades of Automation

According to IEC 62290, operation of trains without crews includes both unattended and driverless train operations. With unattended train operations (UTO or GoA-4), there would normally be no crew member onboard the train. With driverless train operations (DTO or GoA-3), there may be a crew member onboard the train, but normally not in the driving cab. This crew member, if present, would normally have no responsibility for operation of the train except for failure recovery.

In addition, ATO-equipped trains should be capable of operating in various modes, depending on the operational status of the train-borne and/or wayside equipment.

5.3 System states

The use cases related to the system states are described using UML Sequence Charts (UUSC), based on the architecture at general functional level avoiding specific implementation assumptions.

According to this principle, the USCs have been specified as far as necessary to identify the information that must be generated and used in the different operational situation. The analysis of the role of such information and of the possible errors affecting it, will permit a structured and systematic safety analysis.

To identify the system, use cases related to the moving block functions listed in Table 2 has been analysed and the results are reported in the Chapter 6 of the deliverable. The description is performed by means of USC with notes and explanations where necessary.

The analysis of the failure modes and their consequences will take into account all the conditions associated to the different scenarios.

5.4 Environmental conditions

Environment type	Characteristics
An open sky environment	Good satellite visibility Continuous presence of the total number of satellites with rare interruptions
Restricted environment	Frequent interruptions of satellite visibility, Significant reduction of the number of available satellites. GNSS signal multiple reflexions (multipath) Possible NLOS reception (No Line of Sight) SBAS (EGNOS) sporadic visibility Presence of natural obstacles
Urban environment	Frequent interruptions of satellite visibility, Significant reduction of the number of available satellites High probability of multipath and NLOS, due to reflections and obstructions SBAS (EGNOS) sporadic visibility Presence of man built obstacles

Table 11 - Environmental conditions

6 Use Cases representation with UML Sequence Charts

The use cases that identify the system in terms of moving block functions have been analysed and are shown below, according to the functions in the Table 3.

Each train reports cyclically its location, “Train detection (along with train integrity)” function updates the locations of heads and tails on the track description, for use by “Route Management System” and “RBC” functions.

The locations stored are therefore “old”, with respect to the current locations, if the train is moving. If a train can only move forward and cannot exceed the received MA, the following will be not considered as a safety issue:

- the head will remain in any case within the MA, that must be considered as “not at disposal of any other MA”;

- the tail position received is less advanced than in reality, therefore the MA of following trains will be shorter, with a possible system performance problem, but no safety risk.

The situations to be further analysed and managed through appropriate operational rules are:

- movement of trains without MA (on-sight), especially when the train is not able to report its location (degraded situation);

- backward movements (shunting);

-during the mission the system version number X of a received balise telegram is greater than the highest version number X supported by the on-board equipment

According to the abovementioned, two main uses cases can be considered:

- the train know its location and is able to report (and train integrity is confirmed);

- the train does not know its location (or train integrity is not confirmed).

The USC refer to initialization, they are however cyclically repeated to keep the data base up-to-date.

The case of a train not knowing its location is especially critical either if there is a train entering the system from a depot not covered by moving block functionality or there is a train already in the area covered by moving block that has been switched off at the end of its mission. In this case, the train is known to the trackside data base, that keeps its last reported head and tail locations. In this case special operational procedures are necessary, to record the new locations communicated by the train and delete the old ones.

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

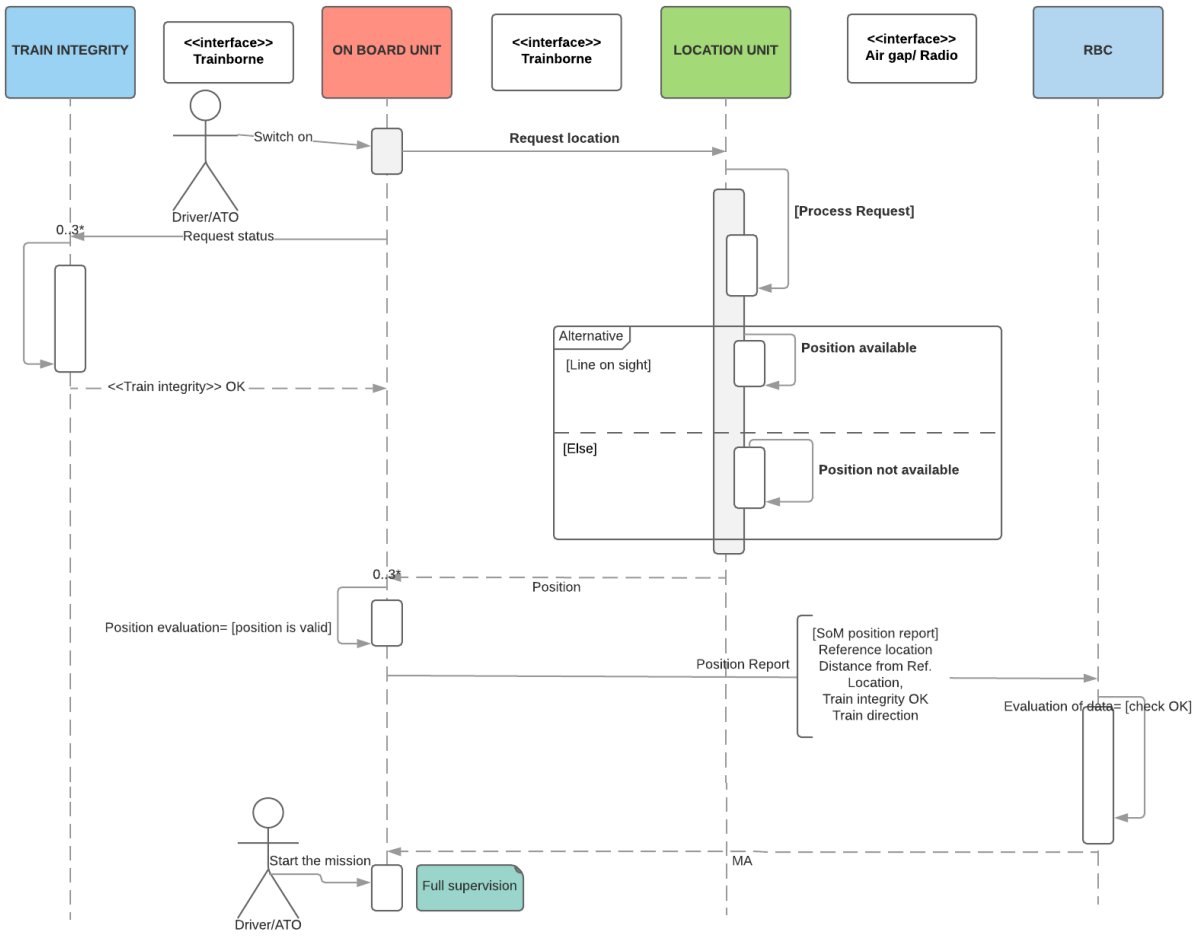


Figure 5 – USC Start of Mission when the train position is valid

The Sequence Chart corresponds to the case when the system is performing correctly with the 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**	GoA1 GoA2 GoA3 GoA4	Open Sky Environment
High density lines High speed lines	Normal operation	The train knows its location and is able to report.		

Medium density lines Low density lines Regional lines		.		

Table 12 - 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).

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

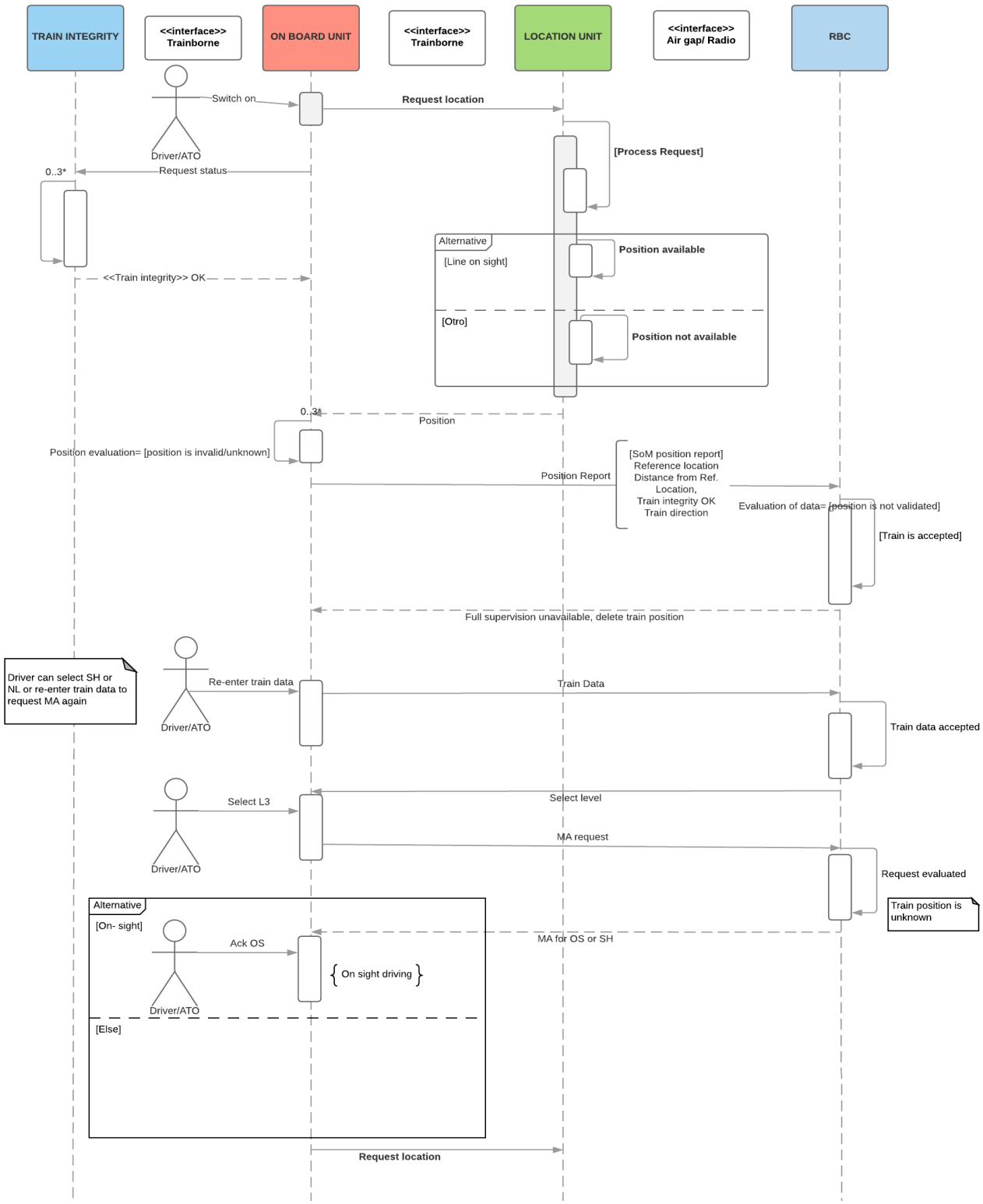


Figure 6 - Start of Mission when the train position is invalid/ unknown

The Sequence Chart 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);
- 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 13 - 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 or unknown and GNSS positioning information is out of range (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).

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 (according to the probability of encountering a train while moving on-sight).

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 and evaluation functions are required and are safety related.

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

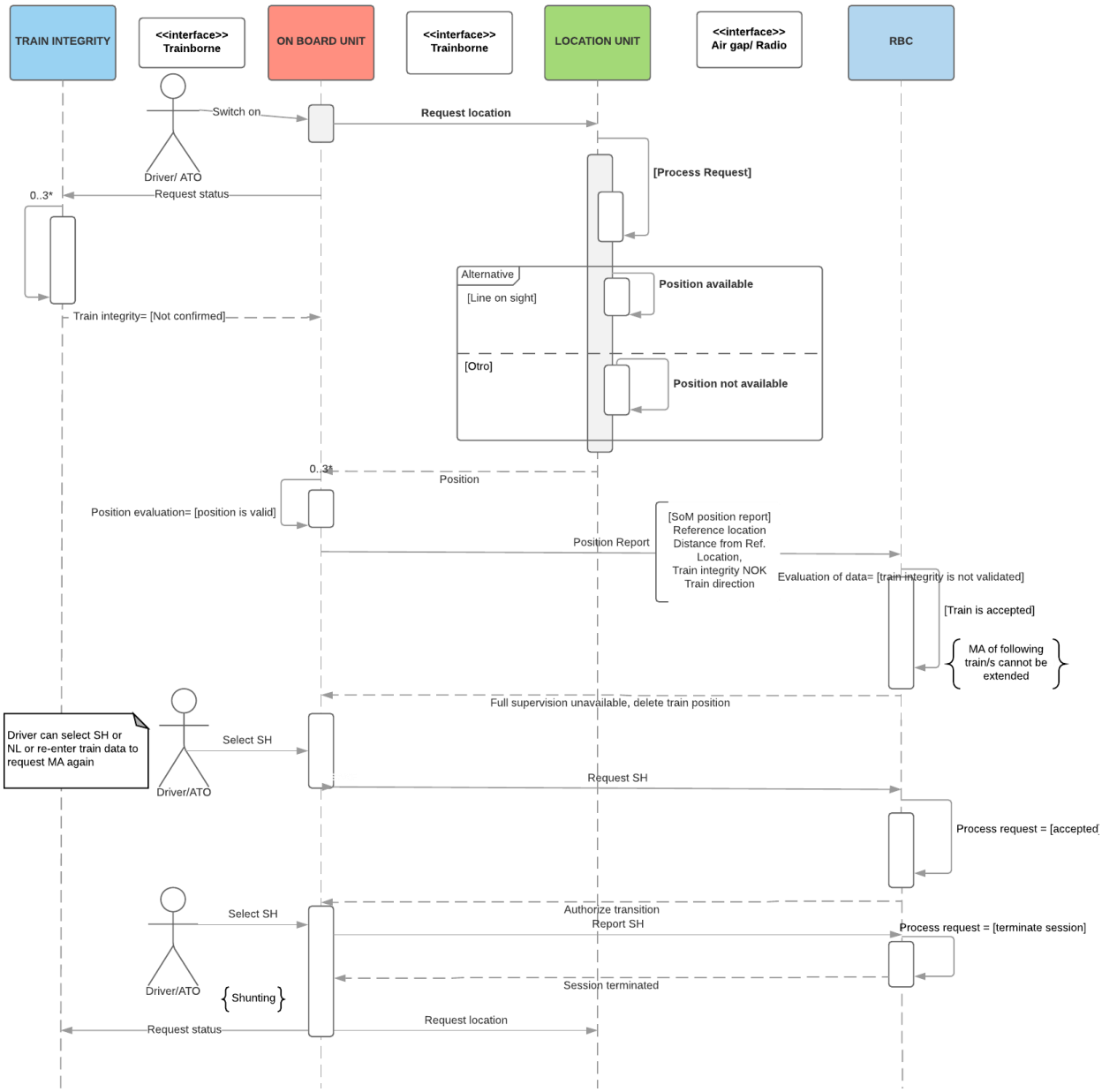


Figure 7 - Start of Mission when train integrity is not confirmed

The Sequence Chart 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 14 - 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.

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

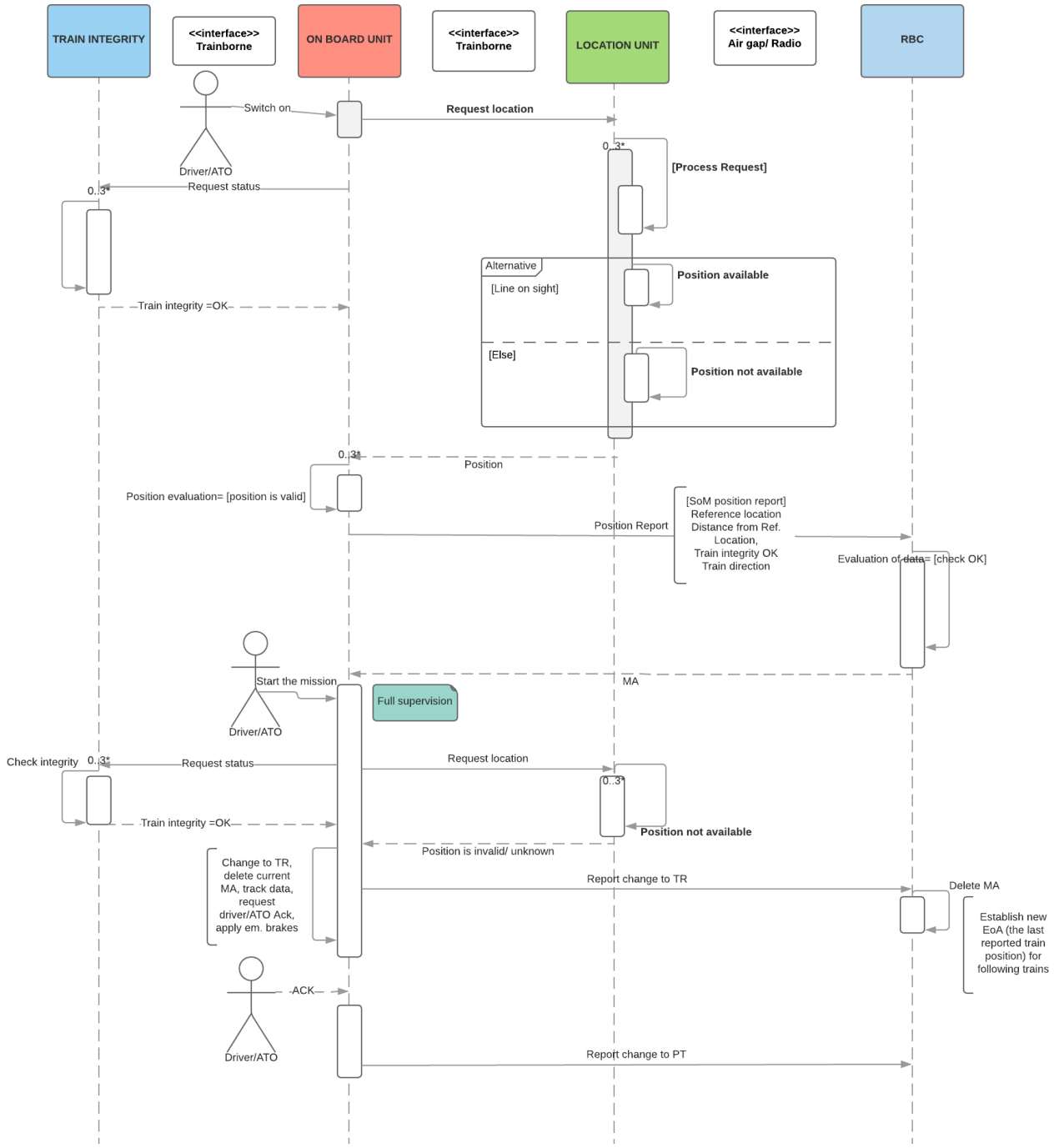


Figure 8 - Start of Mission when train integrity is not confirmed

The Sequence Chart 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 6.1).

In case the positioning function is not available, driver/ATO also can select Start to trigger MA request to RBC (Use case 6.2). 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.

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.

7 Conclusion

To develop a level of understanding of the Moving Block system without trackside detection sufficient to enable its proper Safety analysis, and then to define the system main components and functions, its mission profile, boundaries and uses case, the system architecture and a system model have been elaborated.

Firstly, the ERTMS Level 3 overall architecture was investigated to better understand the scope and interfaces of the Moving block system. The existing train detection systems functions were analysed and classified with the aim to study how they interact with moving block system components.

Based on the information so achieved, the system model has been developed applying semi-formal method UML state machine diagrams for the representation of the system, and then four Use Cases were derived and depicted with UML sequence diagrams to analyse operational impact.

These models will provide the base for the further development of the Hazard Analysis and will be used for the validation in the ASTRail WP4. For this reason, it is important to highlight that according to the results of Hazard Analysis and Validation, further modifications could be introduced in the model during the official revisions of the D2.1 on M13 and on M19. The possible inputs that will come from ASTRail WP1 and X2Rail-1 project will be considered also during these revisions to assure the continuity of the work within the project.

In parallel with system modelling, the System Use Cases have been defined analysing significant system operative conditions.

The main scenarios that has been defined correspond to the system states, modes of operation and operational conditions. The system states have been represented using the method of UML Sequence Charts (Chapter 6). This method offers another point of view on the main system functions and will be exploited in the Hazard Analysis.

Other factors such as traffic type and density (main parameters: speed and headway), environmental conditions (main parameters: GNSS availability, local effects) and Grade of Automation (main parameter: Driver and system responsibility) will be assessed during the Hazard Analysis phase using the inputs coming from ASTRail WP1 and WP3.

The definition of the system model allows to visualise the interaction between its elements and to understand how the fault of a component might impact other components and the overall system, which is a necessary step to determine how GNSS fault (Location Unit fault/ failure) can contribute to ERTMS hazards. The analysis will be provided in the Task 1.5 of the WP1.

Acronyms

Acronym	Explanation
LX	Level Crossing
LoA	Limit of Authority
MA	Movement Authority
FS	Full Supervision Mode (ERTMS mode)
SvL	Supervised Location
GNSS	Global Navigation Satellite System
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
CBTC	Communications-based train control
RBC	Radio Block Centre
ROC	Radio Object Controller

List of figures

8 List of tables

References

Baar, T., Strohmeier, A., & Moreira, A. (2004). *<<UML>> 2004 - The Unified Modeling Language.* Lisbon: Springer.

Bernardi, S., Flammini, F., Marrone, S., Mazzoca, N., Merseguer, J., Nardone, R., & Vittorini, V. (2013). *Enabling the usage of UML in the verification of railway systems: The DAM-rail approach.* Elsevier.

Bernardo, M. (2005). *Formal Methods for Mobile Computing.* Bertinoro: Springer.

Bin, N., Tao, T., Min, Q., & Hai, G. (2006). *CBTC (Comminication Based Train Control): system and development.* Bejing Jiaotong University, School of Electronics and Information Engineering. WIT Press.

Damy, S. (2016). *A Novel GNSS-based Positioning System to Support Railway Operations.* London: Imperial College London.

ERTMS Platform . (2008). *ETCS Implementation Handbook.* París.

FIlip, A. (2017). *Travelling Virtual Balise for ETCS.* University of Pardubice, Faculty of Electrical Engineering and Informatics. WIT Press.

Jabri, S., EL Kouris, E., Lemaire, E., & Bourdeaud'huy, T. (2009). *A generation method of test scenarios based on models: application to the ERTMS/ETCS system.* Ecole Centrale de Lille, National Institute for Transport and Safety Research , Lille.

Leue, S. (2003). *Scenarios: Models, Transformations and Tools.* Dagstuhl Castle: Springer.

Marais, J., Beugin, J., & Berbineau, M. (2017). *A Survey of GNSS-Based Research and Developments for the European Railway Signaling .* Lille: IEEE.

Novatel. (2017, October 3). Retrieved from https://www.novatel.com/an-introduction-to-gnss/

Pilone, D., & Pitman, N. (2005). *UML 2.0 in a Nutshell: A Desktop Quick Reference.* O'Reilly.

Selic, B., Moore, A., Woodside, M., Watson, B., Bjorkander, M., Gerhardt, M., & Petriu, D. (2001). *Response to the OMG RFP for Schedulability, Performance, and Time.* OMG.

Teunissen, P., & Montenbruck, O. (2017). *Handbook of Global Navigation Satellite Systems.* Wessling: Springer.

Trowitzsch, J., & Zimmermann, A. (2005). *Real-Time UML State Machines: An Analysis Approach.* Technical University Berlin, Real-Time Systems and Robotics Performance Evaluation Group.

Trowitzsch, J., & Zimmermann, A. (2006). *Using UML State Machines and Petri Nets for the Quantitative Investigation of ETCS.* Technische Universität Berlin, Real-time Systems and Robotics, Pisa.

Ulianov, C., Hyde, P., & Shaltout, R. (2017). *Railway Applications for Monitoring and Tracking Systems.* Newcastle University, NewRail Centre for Railway Research. Newcastle: Springer.

Verma, A., Pattanaik, K., & Goel, P. (2014). *Mobile Agent based CBTC System with Moving Block Signalling for Indian Railways.* Indian Institute of Information Technology and Management Gwalior. Civil-Comp Press.

Xie, G., Xinhong, H., Hiroshi, M., Sei, T., & Hideo, N. (2013). *Safety and Reliability Estimation of Automatic Train Protection and Block System.* John Wiley & Sons.

Zimmermann, A., & Hommel, G. (2004). *Towards modeling and evaluation of ETCS real-time communication and operation.* Technische Universität Berlin, Real-Time Systems and Robotics Group. Berlin: Elsevier Inc.