Ref. Ares(2019)6773318 - 31/10/2019

D5.4 - Report on the project results/achievements for future Shift2Rail activities

Deliverable ID	**D5.4**
Deliverable Title	**Report on the project results/achievements for future Shift2Rail activities**
Work Package	**WP5**
Dissemination Level	**PUBLIC**
Version	**0.8**
Date	**2019-10-31**
Status	**Final**
Lead Editor	**LINKS**
Main Contributors	**ENAC, ARDANUY, CNR, SIRTI**

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	2019-09-18	LINKS	TOC
0.2	2019-10-01	CNR	Contribution for WP4 chapter
0.3	2019-10-03	ARDANUY	Contribution for WP2 chapter
0.4	2019-10-09	SIRTI	Refinement of WP4 chapter
0.5	2019-10-21	ENAC	Contribution for WP1 chapter
0.6	2019-10-22	LINKS	Contribution for WP3 chapter
0.7	2019-10-24	LINKS	Introduction and Conclusion sections, revision of WP1
0.8	2019-10-31	LINKS	Final revision

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

In the last years, several breakthrough technologies have become available and many of them have a huge potential for the renewal of transportations: as a result, some sectors, especially the automotive one, are rapidly evolving. In the case of railway transport, innovation needs to be introduced at a slower pace, because stricter safety requirements have to be fulfilled. Nevertheless, new paradigms require to be investigated.

The ASTRail project was proposed with the aim of contributing to the investigation of new technological solutions for the railway field. In particular, the ASTRail project has investigated how to improve the technologies for signalling and automation leveraging new applications and solutions, after analysing them in terms of safety and performances. Insights from other fields, such as avionics or automotive, are useful to exploit cutting edge technologies, scientific approaches and methodologies in the railway environment.

The ASTRail rationale and aims are organized into 4 work streams that correspond to its technical Work Packages (WPs. The WPs and their aims are:

1. **WP1** – "*Introducing GNSS technology in the railway sector*". The overall aim of WP1 was to transfer the applicable requirements and solutions from the Aviation domain to the railway domain, in particular for the application of Fail-Safe Train Positioning to Moving Block Signalling. Targets were the analysis and identification of requirements, standards and assumptions for the rail sector and the definition of a GNSS-centric architecture. The final achievement is the development and proposal of a Minimum Operation Performance Standard (MOPS);

2. **WP2** – "*Safety analysis of Moving block signalling system*". The main objective of the WP2 was to examine the safety level of a Moving Block signalling system in view of complete removal of trackside detection. This involved also the preparation of a model suitable for the analysis of the system and to define the use cases to be analysed;

3. **WP3** – "*Automatic driving technologies for railways*". The goal of WP3 was to identify the most suitable automated driving technologies that can be reused in the railway field. After performing a state-of-art survey on automated driving technologies in other application fields, an assessment of the selected technologies was performed to evaluate the suitability of each technology for its deployment in the railways;

4. **WP4** – "*Formal Methods for the railway field*". The objective of this WP was to identify the most promising formal and semi-formal methods and tools for the different development phases of railway. The first objective consisted in reviewing and classifying the main formal modelling and verification languages and tools used in industrial railway applications. The main target of the WP was to qualitatively validate the usage of a set of the selected formal methods through the modelling of the Moving Block signalling system defined within the ASTRail WP2.

1.1 Scope

The aim of this deliverable is to concisely report the main outcomes of each technical WP of the ASTRail project.

The summary of the ASTRail project results wants to provide a synthetic and, at the same time, complete overview to be used for people approaching the ASTRail project for the first time, so to facilitate the exploitation.

Detailed explanations of the work conducted in the ASTRail projects, the complete set of results and related documentation are available in the technical deliverables of each WP. The technical deliverables are all public and they are available on the ASTRail website http://astrail.eu/.

2 Results and main achievements of WP1 "Introducing GNSS technology in the railway sector"

WP1 was split into eight tasks, completed within the timeframe of the ASTRail project.

The first two tasks respectively identified the aviation standards relevant to the studies of ASTRail project (T1.1 – "*Aeronautical Assumptions Review*") and which the relevant assumptions, metrics and requirements from civil aviation standards can be transferred to rail (T1.2 – "*Aeronautical Requirements Transfer*"). Deliverable D1.1 "*Aeronautical Standards Review*" presents the outcomes of the first two tasks.

The third task (T1.3 – "*GNSS Local Error Modelling*") reviewed the existing GNSS channel models for land navigation, identified and described the main signal impairments. A channel model suitable to represent the propagation of GNSS signals in a railway environment was presented and analysed. Outcomes are reported in deliverable D1.2 "*Local GNSS Effects*".

The fourth task (T1.4 – "*Augmentation System Integrity Assessment*") addressed the various augmentation system options, while the fifth one (T1.5 – "*Hazard Analysis of ERTMS hazards associated with GNSS faults*") identified the ERTMS hazards associated with GNSS faults and defined possible mitigation strategies. Deliverable D1.3 "*The ERTMS hazards associated with GNSS faults*" contains the results achieved in these two tasks.

Task T1.6 – "*GNSS Algorithm Analysis and Design*" was about the definition of a GNSS-centric architecture suitable for the railway environment and the design and implementation in Matlab language of GNSS algorithms. Outcomes of this task are in Deliverable D1.4 "*GNSS algorithms design*".

In task T1.7 – "*GNSS Algorithm Performance Assessment and Verification*", the simulation plan of the algorithms designed in task T1.6 has been defined, followed by the simulation and the performance assessment of these algorithms. Deliverable D1.5 "*GNSS Solutions Report*" provides the details and the results of this task.

Last task (T.1.8 – "*GNSS Minimum Performance Requirements for Rail*") defined a set of minimum performance requirements for the use of GNSS in the railway domain field. Deliverable D1.6 "*Proposed GNSS Minimum Performance Requirements*" reports the outcomes of this task.

The outcomes of WP1 are reported per deliverable in the following of this Section.

2.1 D1.1 – Aeronautical Standards Review

In deliverable D1.1 of ASTRail, the work completed in tasks T1.1 and T1.2 was presented. In task T1.1, the goal was to identify the ASTRail project needs, outline the key assumptions taken by aviation and identify the aviation standards that are pertinent for study. In task T1.2 the objective was to transfer relevant assumptions, metrics and requirements from civil aviation standards to rail through analysis, reporting and by education rail experts to ensure appropriate feedback between partners.

In D1.1, firstly, a review of civil aviation requirements and their relation to railway RAMS requirements was made. Secondly, a thorough review of previous studies of GNSS use in rail was presented. Based on the review of previous projects, two architectures were taken forward, a primary baseline, based on the RHINOS project and a secondary hybridised solution (Brocard). Work on the transfer of assumptions and requirements for the application of GNSS from the civil aviation domain to the rail domain was presented. The philosophy taken was not to apply blindly the civil aviation requirements, specified in terms of the four Signal-In-Space parameters of accuracy, integrity, continuity and availability. Rather, the approach was to use the railway formulation of requirements in terms of Reliability, Availability, Maintainability and Safety with guidance from the experience of civil aviation.

It is noted that in comparison to the reliability and safety of existing railway components, GNSS safety integrity, meaning the trust that the positioning and localisation solution is not subject to dangerous undetected errors, is a function of time. This is as a result of the non-stationary error distributions due to satellite motion. Furthermore, the Safety Integrity Level (SIL) must be achieved under all stated conditions as per the rail

industry standards, this is interpreted to account for the worst-case conditions regarding the impact of a failure and other driving parameters relating to the measurement error model. In fact, what is known, as specific risk in the aviation world should be applied when safety is at stake. The SIL in rail is referenced to a Tolerable Hazard Rate (THR) for a particular function, notably 10-9 per hour for SIL4 the most demanding level. This THR is the total risk during any hour of function. Since the probability distributions for the components are with conventional systems stationary, the designer only has to compare a computed hourly risk to the requirement to check compliance. With GNSS, since the real time risk varies, compliance must be verified in real time, unless it can be guaranteed that the requirement is met whatever the state of the system.

ASTRail WP1 accepted that the virtual balise concept was well established as a means to integrate a GNSS based positioning component to the rail localisation unit (LU) without a complete overhaul of the train architecture. This concept then formed the backbone of the architectures addressed in ASTRail.

2.2 D1.2 – Local GNSS Effects

The objective of task T1.3 was to review and select an appropriate GNSS channel models for land navigation. In deliverable D1.2, the major impairments that can affect the performance of a GNSS receiver in a railway environment were addressed: multipath propagation, Non Line-Of-Sight (NLOS) reception, and Radio Frequency Interference (RFI).
For multipath and NLOS, a channel model present in literature has been selected, adapted to railway environment and analysed. The adaptation led to several advantages with respect to the original channel model:

- Simulation of different scenarios surrounding the train (‘urban’, ‘suburban’, and ‘open-sky’);
- Simulation of complete outages due to the presence of tunnels;
- Support of the RF signal simulation through the use of an RF GNSS signals generator;
- Simulation of an entire GNSS constellation, eased by the employment of the RF GNSS generator;
- Possibility of a direct interface with commercial GNSS receivers to test multipath resilience.

Then, a classification of the main types of RFI was reported along with the selection of the most relevant ones for the railway environment. It must be noticed that the employment of the RF GNSS signal generator enables to add an RFI to the generated signal in order to test the overall effect on the tested receiver.

2.3 D1.3 – The ERTMS hazards associated with GNSS faults

Tasks T1.4 and T1.5 addressed the hazard analysis for faults and integrity monitoring implemented within civil aviation’s augmentation systems. For example, in subtask 1.4.1 “Augmentation System Review”, a review of various integrity monitoring options deployed, or under development, within aeronautics both at system (EGNOS) and sensor (RAIM) level, was developed. Studies of the current advances in civil aviation augmentation systems showed that certain techniques may be applicable to the rail application. Namely, the multiple hypothesis approach of Advanced RAIM offers improved local integrity monitoring for the train’s on-board function. Dual frequency positioning and monitoring techniques developed within the next generation GBAS work may help to inhibit some effects of ionosphere whilst reducing through smoothing the multipath. In particular, Task 1.5 identified ERTMS hazards associated with GNSS faults, and at defining possible mitigation strategies for different railway market segments. The work that was carried out covered two main aspects of hazard analysis:

1. Identification of ERTMS hazards for GNSS based positioning system;
2. Identification of the mitigation strategies.

Hazard identification, analysis of its causes and consequences were realised using the HAZOP technique. Those results are related to the impact of main ARAIM threats on ERTMS system performance including the identification of generic mitigation strategies considering aviation sector experience. To quantify the integrity target, the SBAS integrity tree has been analysed and it was concluded that each ranging source corrected measurement may be modelled as a Gaussian error up to 5.33 times the observable standard deviation and that the probability of any exceeding this value is less than 10−7 within 150s. It may be possible to extend this to 0.5×10- 7 within 1 hour since the requirement for lateral guidance in this respect is more stringent but fewer details are published.

2.4 D1.4 – GNSS algorithms design

In task T1.6, the architectural definition was defined employing a baseline GNSS-centric solution, including use of SBAS. Brainstorming between GNSS, rail and aviation experts was used and metrics for setting rail GNSS requirements were defined.

The deliverable D1.4 presented the definition of a GNSS-centric architecture suitable for positioning in rail safety applications, and the selection and design of possible algorithms to enhance the positioning availability and the RFI resilience. In particular, a multi-sensor Virtual Balise reader GNSS-based train positioning system to be integrated to the current ERTMS/ETCS was proposed and outlined.

Three main operational scenarios affected by reduced visibility issues were identified: in the station, in tunnels and in proximity of railway exchanges. In order to improve positioning availability in such scenarios, three main categories of GNSS complementary technologies have been considered: wireless, visual-based and dead-reckoning methods. Thus, a discussion on possible integration approaches has been addressed and a feasible loose-coupling architecture was also proposed.

Finally, after a state-of-art scouting on RFI detection and mitigation techniques, the Adaptive Notch Filter (ANF) has been selected as a versatile and low-complexity solution, able to remove Continuous Wave (CW), Narrow Band (NB) and swept interferers. A specific family of ANFs, namely Frequency-Lock-Loop (FLL)-equivalent ANFs, has been chosen. In particular, two models of FLL-equivalent ANF have been considered: the standard FLL and the exponential filtering FLL. The algorithm description and design of both models has been provided and key performance indicators to be used for the performance evaluation have been also derived.

2.5 D1.5 – GNSS Solutions Report

Simulations performed in Task T1.7 took into account local effects on the GNSS signal propagation. Furthermore, an odometry diagnosis method developed in task 1.6 was defined for the GNSS solution in terms of a test statistic and a threshold set.

The deliverable D1.5 presented the performance evaluation of multiple algorithms, defined and designed in task T1.6. This includes an architecture to diagnose GNSS failures using odometry sensors between physical balises, and the enhancement of both the positioning solution availability and the robustness against RFI.

In particular, a GNSS failures diagnosis scheme comparing measurements of odometry and track geometry with position of GNSS has been provided. Simulations were performed to investigate the effect of choice on GNSS constellation and the advantage of utilizing track geometry information. The results show how the usage of dual-constellation of GPS and Galileo and track geometry are beneficial for the detection of a position failure.

To enhance the PVT availability in presence of local channel impairments, a loosely coupled integration of GNSS receiver, Doppler radar and wheel odometer has been presented. The performed tests demonstrated the advantages of the data fusion, overcoming the limitations shown by each technology alone. Finally, a performance comparison of two FLL-equivalent ANFs in case of jamming signals has been presented, showing promising results.

2.6 D1.6 – Proposed GNSS Minimum Performance Requirements

In Task T1.8 a skeleton analysis and presentation of a set of minimum performance requirements for the use of GNSS (and other sensors) in rail was concluded. This work was captured in D1.6 that summarized the characteristics of GNSS-based location system and defines the performance requirements in railway scenarios. The situations that are challenging for the GNSS-based location system were identified, highlighting the main positioning issues. The main operational performances of a GNSS-based location system were described identifying the environment classes that influence the performances of the system.

The main solutions that allowed the use of GNSS for train operations in a Moving Block signalling system without trackside train detection were outlined. It suffices to say that the specification of requirements and recommended practices or operating procedures for GNSS based equipment to be employed for safe train localisation is at this stage greatly limited by the lack of knowledge and an agreed solution to the impact of local errors. Before an appropriate methodology is defined for these effects, it becomes very difficult to confidently restrict the architecture to be employed. The approach of D1.6 was to attempt to innovate in other areas. The different environments were classified, although it is too early to categorically proclaim the approach taken is optimal. The method proposed was based on some analyses of the constellation geometry obtained taking into consideration the local terrain and topography, including building elevation data.

Furthermore, one of the challenges identified within ASTRAIL has been the difficulty of requirements setting and the wide range of results from previous studies. In this work, an alternative to setting alert limits was proposed, instead relying upon the computation of a variable protection level that is used by the on-board system to determine what speed (with respect to the appropriate braking curve) may the train move at safety. One aspect, which will have to be investigated in future, if this idea is to be employed, is the prediction of protection levels. This might be necessary to avoid some sharp emergency braking protocols if the protection level were to jump abruptly. This work is based on the use of topographic height data, which it is intended to use (potentially a similar source such as LIDAR or camera) as a basis for characterising the local environment along the rail route network. This might feasibly be done in real time in future solutions, here though it is based on offline processing which allows both an error model to be defined for that location and also a means to determine the receiver mode. Three receiver modes have been defined which account for the variable environments, taking care to appease the needs for legacy compliance and backward compatibility. We've concluded that, to satisfy the needs for train operations and traffic management, the GNSS-based location system shall be integrated with complementary positioning systems when in enhanced odometry mode and physical balises to support the legacy mode and between virtual balise sections.

3 Results and main achievements of WP2 "Safety analysis of Moving block signalling system"

This section summarizes the main outcomes of WP2 whose focus was to analyse the safety level of a Moving Block signalling system.

This WP is break-down in four tasks. The first task (T2.1 – "*Modelling of the moving block signalling system*") tackled the modelling of the logical functionalities of the Moving Block signalling, while in the second task (T2.2 – "*Definition of the system use cases*") the use cases for the safety analysis are introduced.
Deliverable D2.1 "*Modelling of the moving block signalling system*" reports the outcomes of the first two tasks.

The safety assessment of a Moving Block signalling system has been investigated in the third task (T2.3 – "*Hazard identification and risk analysis and evaluation*"). The fourth task (T2.4 – "*Safety Related Application Conditions for operational procedures*") dealt with the definition of the operational procedure to be applied in normal or degraded conditions considering the different identified use cases.
Deliverable D2.2 "*Moving Block signalling system Hazard Analysis*" reports the outcomes of tasks T2.3 and T2.4.

3.1 D2.1 – Modelling of the moving block signalling system

3.1.1 Model assumptions

The Moving Block System (MBS) without trackside detection model has been performed with the following assumptions:

- 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.

3.1.2 Functional model results

MBS has been modelled using UML State Machine Diagrams. In Table 1, the regions identified are listed and the pseudo-states that can be found in each region as well as a brief description of the modelled function within the region. Subsequently, can be found the respective diagrams for each function and region as well as the events that trigger these function and transitions from one pseudo-state to the next one.

ID	Region	Pseudo-state	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	The On-board Unit sends the location request to the Location Unit.
		Full	
LU 3	Processing location request and calculating location by Location Unit	Idle	Once the Location Unit has received the location request, it processes it and calculates the location.
		Busy	
TCOM 4	Sending location from Location Unit to on-board Unit	Empty	The Location Unit sends location to On-board Unit.
		Full	

ID	Region	Pseudo-state	Description
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 1 – Summary of regions and pseudo-states modelled.

3.1.3 Conclusions and recommendations

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. 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.
The next section will summarize the main results and achievements of the MBS hazard analyses.

3.2 D2.2 – Moving Block signalling system Hazard Analysis

3.2.1 Preliminary Hazard Analysis (PHA) main results

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. 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 and the inductive analysis will be used to identify the hazards that could prevent system from complying its functions The results of preliminary Hazard Analysis were included in D2.2.

3.2.1 Operation and maintenance procedures for Moving Block System

3.2.1.1 Operation procedures (Operational Hazards)

The hazards associated to specific operational procedures derived from four Use Cases defined in the deliverable D2.1 are summarized in Table 2. This analysis is separated from the PHA since the mitigation measures applicable are out of scope of ERTMS/ETCS system (technical mitigation is not possible).

The Hazard Analysis procedure performed is depicted in Figure 1.

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-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 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	
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**	

Table 2 – Summary of Operational Hazards.

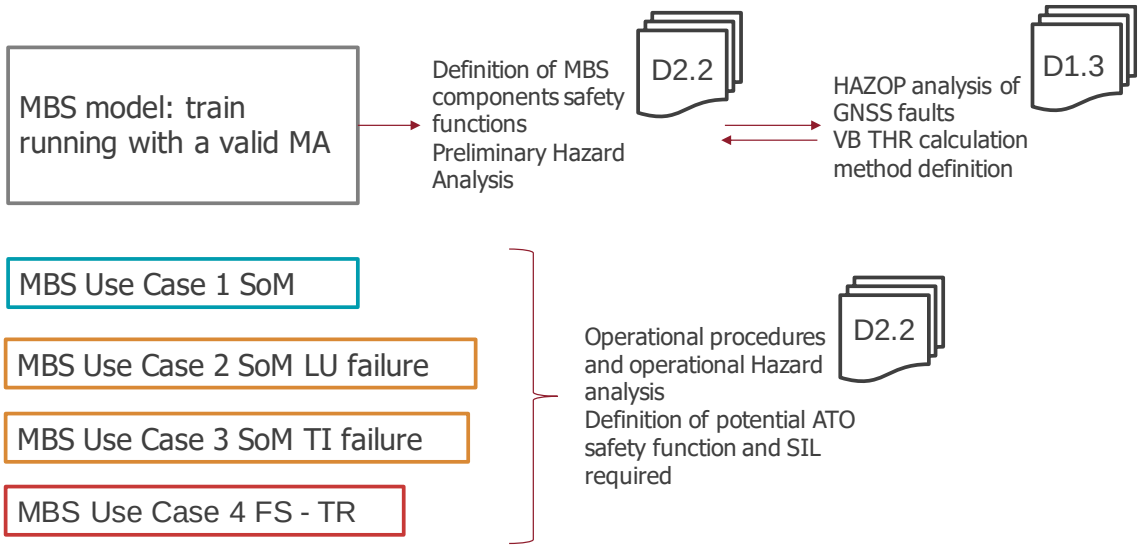

Figure 1 – MBS Hazard Analyses

3.2.2 Conclusions and recommendations

To perform the PHA, the MBS system safety functions have been defined implementing the top-down analysis that has been derived from the most common type of railway accidents and the scenarios that 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 that 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. 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 since they are already covered in other reference sources.

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 are 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 task 2.3 have provided hints to 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. In addition, the task has fed also task 4.2, by easing the ranking of formal methods and tools in terms of their suitability to model and validate required formal properties of moving block system.

4 Results and main achievements of WP3 "Automatic driving technologies for railways"

In this Section, the main outcomes of WP3 are illustrated. This WP is organized in three tasks. The first task (T3.1 – "*Automated driving technologies in the automotive and in other application fields*") dealt with a survey of the state-of-art technologies for automated driving that have been introduced in different application fields. Deliverable D3.1 "*State of the Art of Automated Driving technologies*" reports the results of the survey

In the second task (T3.2 – "*Analysis of Automatic Train Operations: operation conditions and implementation characteristics*"), an evaluation of the main characteristics of ATO was performed to understand which implementation characteristics and operation conditions are required in a scenario where ATO is introduced.
The third task (T3.3 – "*Assessment of automated driving technologies for railways*") performed an evaluation of the technologies identified in the first task in order to define which of the currently available automatic driving technologies can be reused in the railway domain.
The outcomes of these two tasks is provided in deliverable D3.2 "*Automatic Train Operations: implementation, operation characteristics and technologies for the Railway field*").

The results and main achievements of WP3 are described in the following of this Section.

4.1 D3.1 State of the Art of Automated Driving technologies

Deliverables D3.1 reports the results of the survey conducted in task T3.1. This task has been devoted to the identification of the technologies that are currently employed or under development in the automotive, in the railway and in other application fields, such as agriculture, maritime and industrial. Scientific literature, industrial and market solutions have been analysed to provide an overview of all cutting-edge technologies that are available.

The survey focused in particular on the technological solutions for the "*Navigation"* functionality of the automated driving. This functionality concerns especially the localization of the vehicle in the driving environment and the perception of objects in the surroundings of the vehicle.

The vehicle's localization is usually achieved using satellite positioning techniques that are complemented by dead reckoning methods (mainly odometry and inertial navigation) to improve the accuracy in the vehicle's localization. Significant research effort is also devoted to employ visual sensors, i.e. camera, and other perception sensors, such as RADAR or LiDAR, to identify particular features of the driving environment and to create a virtual representation. These approaches are used for a map-based localization.

The detection of objects can be achieved using several perception sensors, i.e. cameras, RADARs, LiDARs. Typically, different types of sensors are used together since most of them are complementary for characteristics in different working conditions, such as bad weather or low lighting conditions.

Surveying the different application fields, it has been observed that most of the technologies, which are employed for the navigation task, are nearly the same in all application fields.
Furthermore, the joint use of several sensors is also a common feature in autonomous driving for both localization and obstacle detection tasks. Fusing data from different sensors can indeed provide high reliability, robustness and it can improve the results accuracy.

4.2 D3.2 Automatic Train Operations: implementation, operation characteristics and technologies for the Railway field

The analysis of implementation and operation characteristics of autonomous driving road vehicles and of ATO is described in deliverable D3.2. This analysis had the objective to understand which the main requirements are to implement ATO for different grade of automation considering the needed applications and leveraging on the basic characteristics of the automotive sector technologies.

The comparison between the characteristics and conditions for autonomous driving of these two sectors created indeed a knowledge basis that was helpful to better assess the suitability of autonomous driving technologies in the railway sector.

Deliverable D3.2 reports as well the evaluation of the selected technologies in order to identify which of them are most likely to be reused in the railway sector for ATO.
The approach for the evaluation has been to perform a qualitative analysis since currently available sensors of the selected technologies have been designed to satisfy conditions and requirements different from the ones of the railway sector.

The evaluation of the autonomous driving technologies has been performed assessing the suitability of the technologies to satisfy specific requirements of ATO functions (e.g., precise localization, detection of obstacles, trackside signal detection …).

The requirements of the selected ATO functions have then been specified considering their employment in particular railway use cases of interest. Some of the use cases are, for example, "*Approaching a station*", "*Plain line running*" and "*Level crossing*". Each use case requires a given ATO function to satisfy specific needs. These requirements have been identified and technologies have been evaluated versus each of these requirements.

The results and the analysis of the technologies highlighted that several technologies may be well suited to satisfy railway-specific requirements. However, it seems difficult that only one technology can guarantee an effective and reliable solution for all operation conditions and needs. The development of multi-sensors data fusion system seems to be the only viable perspective to properly satisfy autonomous driving requirements. Indeed, each sensor presents strengths and weaknesses and the multi-sensors data fusion system can take advantage on the specific strengths of a sensor to overcome weaknesses of other sensors.

The technologies assessment presented in D3.2 concluded that technologies for autonomous driving can be reused in the railways, however a specific design of the sensors has to be performed to take into account the peculiar characteristics of the railway sector such as speed, braking distance and railway environment.

5 Results and main achievements of WP4 "Formal Methods for the railway field"

WP4 is structured into four main tasks, oriented to identify the most appropriate formal methods and tools to be adopted in the railway field. The first two tasks (T4.1 – "*Benchmarking*" and T4.2 – "*Ranking*") are oriented to survey literature, practitioners and tools to provide structured information for the selection of formal methods and tools. Outcomes of these two tasks is provided in deliverable D4.1 "*Report on Analysis and on Ranking of Formal Methods*".

The third task (T4.3 – "*Trail Application*") aims at experimenting the usage of a set of selected formal methods through the modelling of the moving-block system. Results of task T4.3 are reported in deliverable D4.2 "*Preliminary Trial Report*".

The final task (T4.4 – "*Validation*") aims at validating the usage of the selected formal methods by integrating the moving-block model with automated driving technologies. The deliverable D4.3 "*Validation Report*" reports the result of the Validation task.

In the following of this Section, for each deliverable of WP4 we list the main results and achievements.

5.1 D4.1 – Report on Analysis and on Ranking of Formal Methods

A set of activities were carried out within the tasks named T4.1 – "*Benchmarking*" and T4.2 – "*Ranking*", aimed at supporting the identification of the most suitable formal and semi-formal methods to be used for railway systems development.

Specifically, a systematic literature review was conducted to categorise 114 scientific publications on formal methods and railways according to features such as the type of system and the phase of the development process addressed by the experience considered in the publication. The literature review was complemented with a project review and a survey with practitioners, to identify the most mature formal and semi-formal methods and tools to be used in a railway context.

This analysis has shown a dominance of the UML modelling language for high-level representation of system models, and a large variety of formal tools used, with a dominance of the tools associated to the B family (ProB and Atelier B), followed by several other tools, including Simulink, NuSMV, Prover, SCADE, IBM Rational Software Architect, Polyspace, S3, SPIN, CPN Tools, etc. The project review and the survey with practitioners confirmed this scattered landscape.

According to the survey with practitioners, one of the most relevant features that a tool should support was considered formal verification, and, therefore, a set of tools supporting both modelling and formal verification was considered for accurate experimentation and evaluation. A set of 14 tools, considered as the most promising, was carefully reviewed by means of a systematic evaluation based on a set of 34 evaluation features.

The final product of these activities is a set of informative documents to support the ranking and selection of formal and semi-formal methods for railways, based on (a) the information retrieved from the literature, summarised in a Tool Selection Support Matrix, (b) the information available from the tools' evaluation and (c) a Ranking Matrix, which allows users to weight the different evaluation criteria, and come to a fine-grained selection of the most appropriate formal methods and tools, suitable to their needs.

5.2 D4.2 – Preliminary Trial Report

The objective of task T4.3 – "*Trail Application*" is twofold: firstly, we aim to model the initial design of the moving-block system with different formal/semi-formal tools, to evaluate their usability and their specific peculiarities; secondly, we want to refine and consolidate the initial requirements of the moving-block system to provide a stable version of such requirements.

To address the first objective, we select a set of formal methods and tools, which will be subject to the trial, based on the results of the analysis of the state-of-the-art and state-of-the-practice carried out in the previous tasks. Eight tools in total are selected, namely Simulink, SCADE, UPPAAL, NuSMV, SPIN, ProB, Atelier B, UMC. Each tool is used to develop a model of the moving-block system. The models are showcased to 9 industrial railway experts, and the widely adopted system usability scale (SUS) questionnaire is used to assess the usability of the tools.

The results show that commercial tools with powerful user interface, such as Simulink and SCADE, are considered to be the most usable by the railway experts. However, besides usability, other factors need to be taken into account when selecting a tool and each tool is appropriate for a specific context:

- Simulink and SCADE are appropriate for both early prototyping and detailed design towards code generation, other tools need to be used when aiming at formal verification.
- UMC is appropriate for initial prototyping, when one wants to adopt a design based on UML state machines to facilitate communication with different stakeholders, but wants also verification capabilities as the ones provided by UMC.
- UPPAAL is appropriate when one needs to focus on the verification quantitative, real-time properties and probabilistic aspects.
- NuSMV and SPIN are appropriate when the system, or composition of systems, has a large state space, and one needs to verify temporal logic properties.
- Atelier B and ProB are the right choice for top-down development (i.e., from initial design to code) of single systems, and have somewhat complementary verification capabilities, with Atelier B supporting invariants checking, and ProB supporting model checking.

Other tools, although not widely used in railways, such as CADP and FDR4, have been also experimented in the context of the project and demonstrated their appropriateness for the modelling and verification in the context of large scale, systems of systems.

To address the second goal, which is refining and consolidating the initial moving-block requirements, we rely on an automated quality analysis based on natural language processing (NLP) technologies, and on iterations of brainstorming among industrial and academic partners. A final set of requirements for the moving-block system was produced as output of the task.

5.3 D4.3 – Validation Report

Task T4.4 – "*Validation*" concerned the validation of the choices of formal tools for the development of railway systems, based on the formal specification of the Moving-block system integrated with Automated Driving Technologies (ATO, Automatic Train Operation).

Within the task, we have first defined a formal process to be applied in the concept phase of the system development. The formal process consists of:

1. a requirements elicitation and simulation phase;
2. a phase of mapping towards formal languages;
3. a phase of formal verification.

In the first phase, the Simulink-Stateflow tool was applied to model and simulate the requirements provided by the railway experts, in order to produce a stable requirements specification document, together with an executable Simulink-Stateflow model of the integrated system including Moving-block and ATO. In the second phase, the requirements specification document and the Simulink-Stateflow model were used as input to produce a UML model, which focused on relevant abstraction of the system, and enabled a translation into the Event B formal language. In the third phase, the requirements produced were translated into logic formulae to formally verify the Event B model by means of the ProB tool. Most of the requirements could be verified by means of the tool.

The summarised process demonstrates the feasibility of using formal methods in the concept phase of the development, and demonstrates the suitability of the choices made throughout the ASTRail project. Specifically, we observed that modelling and simulating early requirements enables the discovery of

incomplete or too generic requirements, and it is an appropriate approach to provide an initial refinement and consolidation of the requirements. The graphical language used by Simulink-Stateflow could be interpreted by the domain experts with limited guidance, and was therefore an appropriate means to communicate between formal methods experts and domain experts. The usage of UML enabled the definition of an abstract specification oriented to model nondeterministic behaviour, which could not be modelled with Simulink-Stateflow. Further, translating the UML model into Event B enabled the discovery of incorrectness in the original UML model. Similarly, the translation of requirements into temporal logic formulas, and their verification by means of the ProB tool enabled further reflections on the modelled system, and further adjustments towards the consolidation of the requirements.

A final requirements specification that integrates moving-block and ATO is produced as output from the task. The output of the task also includes the Simulink-Stateflow models, the Event B models, and UML models.

5.4 Final Remarks

The plenty of available formal tools, frequently with complementary attitudes and capabilities, is a consequence of the heterogeneity of the needs that must be addressed when designing and developing a product for railways. The wide variety of the applicable solutions suggests that there is no preferable choice, except by virtue of the particular need, as also results from our survey. Based on the parameters you might select, you could get a different ranking of the tools. Choosing the suitable tools, identified by one unique path, could be an hard task when not strictly related to a specific cost-benefit analysis. This point could be investigated by further projects.

6 Conclusions

The ASTRail project has contributed to reason on possible solutions to enhance signalling and automation system, leveraging cutting-edge technologies from different sectors and taking in particular care the safety and performance issues. The rationale behind ASTRail project has been to create a technological base on which to develop innovation, based on what available from different transportation sectors and other application fields, carefully highlighting the gaps to be filled.

The ASTRail project has further analysed and evaluated the identified technologies in order to recommend to the S2R JU the most suitable solutions to be considered for the development of the planned technical demonstrators described in the S2R MAAP.

Main outcomes of WPs are:

- WP1 provided a report on the transfer of assumptions and requirements from aeronautical standards and it proposed a set of Minimum Performance Requirements for GNSS;
- WP2 defined a model of Moving Block System and performed a Preliminary Hazard Analysis of the defined model;
- A state-of-art survey on automatic driving technologies is provided by WP3, furthermore, it performed an assessment of the identified technologies for their reusability in the railway domain, recommendations on automatic driving for railways are provided as well;
- WP4 provided a ranking of the formal and semi-formal methods and developed and validated a model of the Moving Block System based on the output of ASTRail WP2.

The results of the different WPs show, all in all, that the transfer of technological solutions from application domains other than railways can foster and ease the technological innovation also in the railway domain.

The studies and results of ASTRail have been performed as a preliminary and purely conceptual investigation. The outcomes motivate deeper studies to enhance the level of technology readiness of the identified innovative solutions and so to bring them to a higher maturity grade, moving forward and paving the way to test them on field.

Acronyms

Acronym	Explanation
ATO	Automatic Train Operation
EGNOS	European Geostationary Navigation Overlay Service
ERTMS	European Rail Traffic Management System
GNSS	Global Navigation Satellite System
GoA	Grade of Automation
HAZOP	Hazard and Operability Study
LU	Localisation Unit
MAAP	Multi-Annual Action Plan
MBS	Moving Block System
MOPS	Minimum Operation Performance Standards
NLOS	Non-Line-Of-Sight
OBU	On-board Unit
OPH	Operational Hazard
PHA	Preliminary Hazard Analysis
RAIM	Receiver Autonomous Integrity Monitoring
RAMS	Reliability, Availability, Maintainability, and Safety
RBC	Radio Block Center
RFI	Radio-Frequency Interference
SBAS	Satellite-Based Augmentation System
S2R	Shift2Rail
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate
WP	Work Package

List of figures

List of tables