ASTRail

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

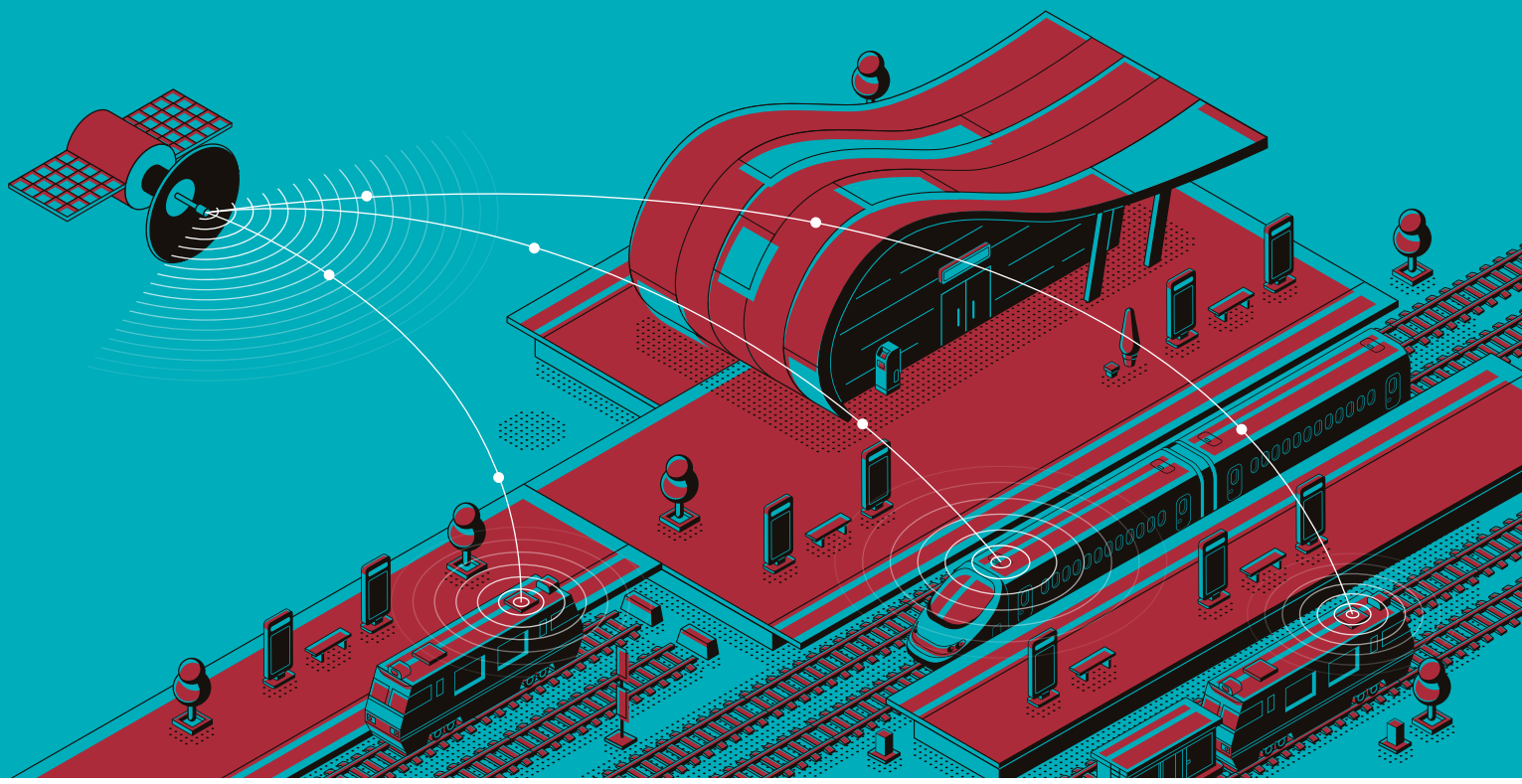
FOREWORD

Newsletter October 2019

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. However, it is time to investigate new paradigms.

To the purpose, the ASTRail project has contributed 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 innovations, based on what available from different transportation sectors and other application fields, and exploring those solutions and technologies that are promising also in the railway sector. 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.

Enhancing the ERTMS with Moving Block System, Automatic Train Operations and GNSS positioning can indeed ensure the competitiveness of the European railway industry, and, in the meanwhile, guarantee a concrete improvement in the quality of the European railway transport system, solving the problem of increasing demand on high density lines.



This project has received funding from the European Union`s Horizon 2020 research and innovation under grant agreement No: 777561. The content of this publication reflects only the author's view and that the JU is not responsible for any use that may be made of the information it contains.

PROJECT STRUCTURE & INTERACTION WITH SHIFT2RAIL

The ASTRail project aims to improve technologies for signalling and automation investigating new applications and solutions that must be carefully analysed in terms of safety and performances.

Insights from other fields, such as avionics or automotive, are necessary to exploit cutting edge technologies, scientific approaches and methodologies in the railway environment.

The ASTRail rationale and aims are split into 4 main technical work streams (WSs):

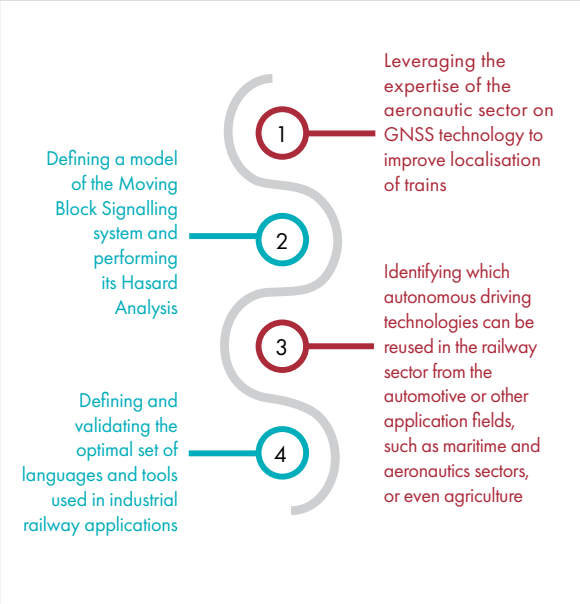


Figure 1. ASTRail technical objectives

The WS-es are only seemingly separate and, on the contrary, have strong interactions. In fact, the understanding of GNSS performance in railways will be crucial for its adoption, particularly in the new moving block signalling and for its integration within the solutions for the Automatic Train Operation; formal methods will be crucial to perform the hazard analysis of new signalling methods.

ASTRail contributes to the achievement of the Master Plan and the Multi-Annual Action Plan (MAAP) roadmap -in particular in the Innovation Programme 2. Through the involvement of JU Members, ASTRAIL constitutes a good way of achieving the long-term technological demonstration programme within the Shift2Rail JU.

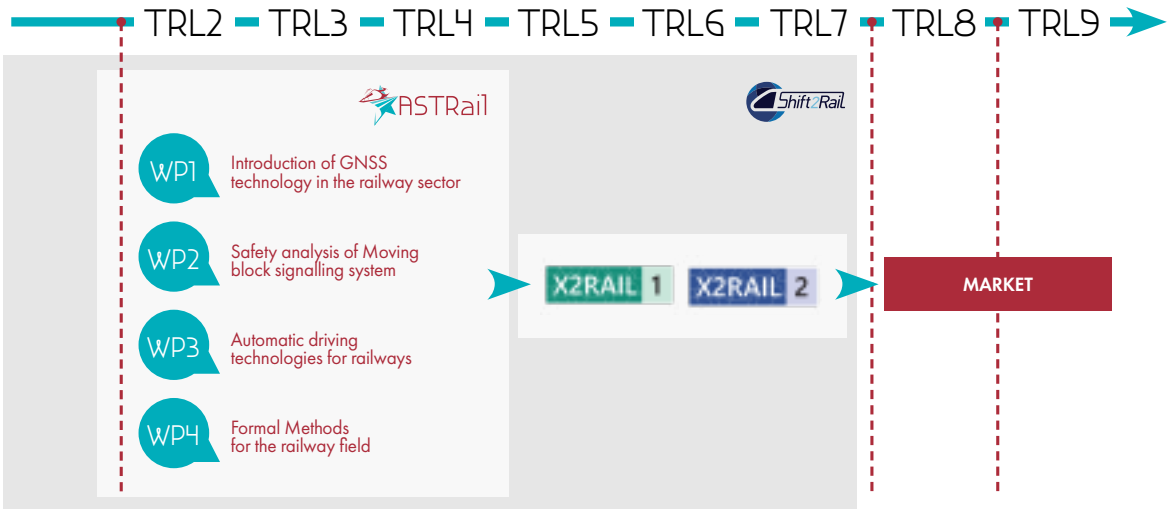


Figure 2. ASTRail project structure within S2R frame

WP1 - INTRODUCING GNSS TECHNOLOGY IN THE RAILWAY SECTOR

WP1 of ASTRail has addressed the introduction of GNSS technology into the railway sector. In the first year of the project, the state-of-play regarding the requirements, standards and assumptions in the rail sector and in current safety-critical applications of GNSS were analysed along with an analysis of localised error sources. In the second year, the possible architectures have been assessed and the development of a Minimum Operation Performance Standards (MOPS) concept has been developed and proposed.

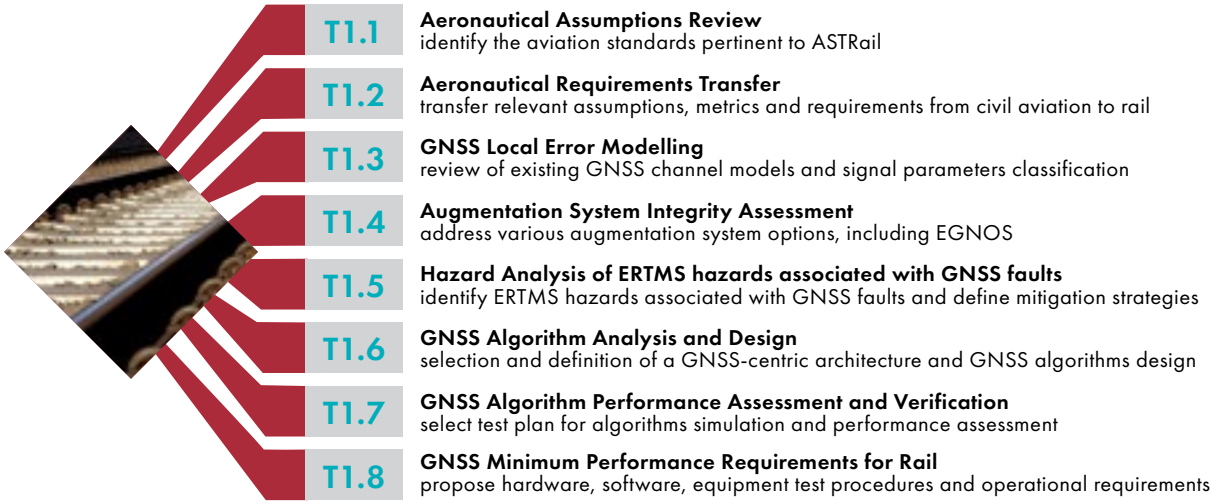


Figure 3. WP1 tasks

Two strands of work have been assessed within the wider question of architecture analysis and testing. The first relates to a hybridised solution, which may be of benefit to an enhanced odometry solution under environmental conditions which are challenging. It is important to account for the different signal environments and within ASTRail, as is described in the proposed MOPS, multiple solutions, or modes of the GNSS-Based Localisation System (GBLS) are proposed to account for these environments. The second of the above mentioned threads has looked at how the integrity of the virtual balise based concept might be assured. A threat diagnosis technique using a bank of monitors based on the position displacement variations between GNSS and existing odometry sensors as well as the track geometry has been developed. Ramp type faults, which present the most dangerous threat are shown to be detected under reasonable conditions down to rates of 1-2 cm/s. The architecture of the assessment modules for this method are shown below.

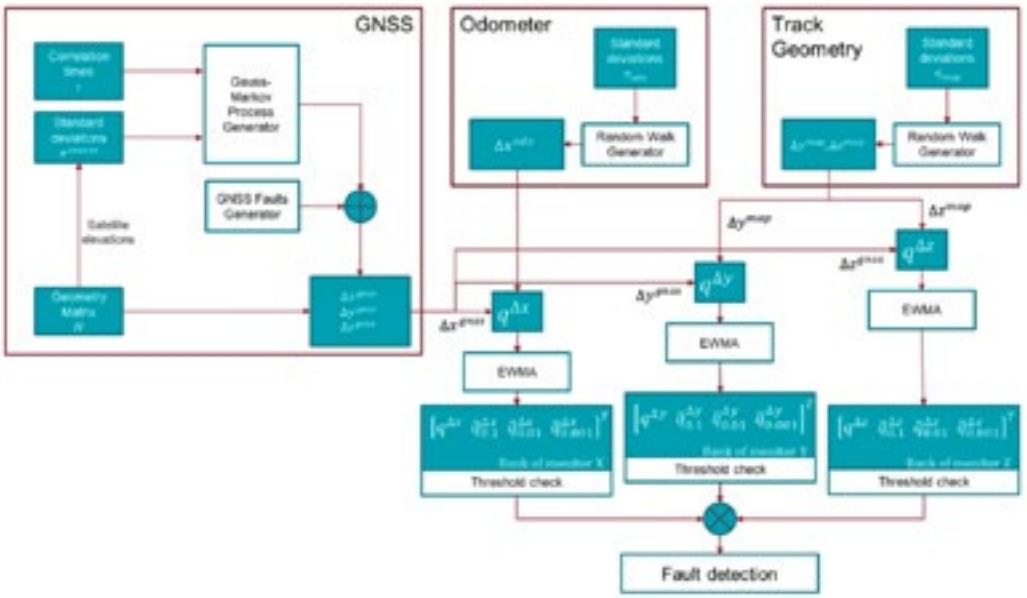


Figure 4. GNSS Threat Diagnosis Assessment Architecture

The figure below plots the probability of missed detection i.e. the likelihood a threat is not detected given that is has occurred against the time to detection relative to the occurrence of a dangerous condition. It is clear that for ramps of at least 3cm/s such faults may be detected with high confidence prior to the dangerous condition.

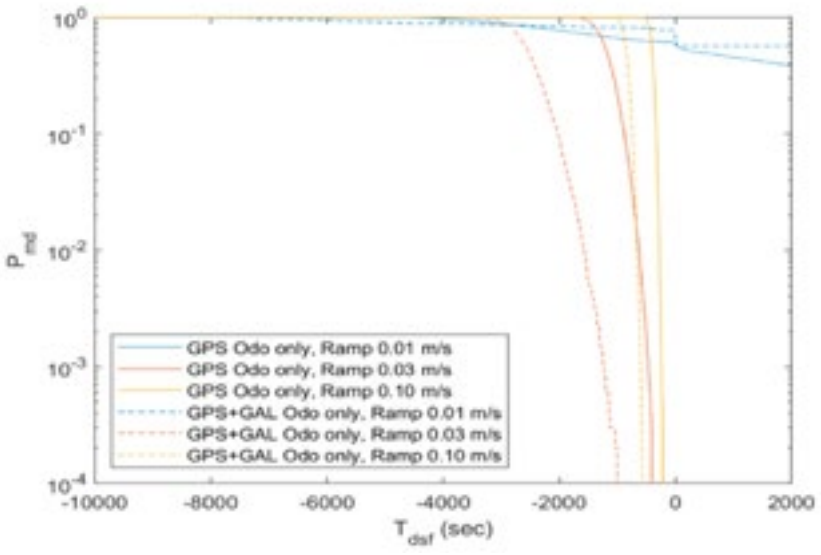


Figure 5. GNSS Threat Diagnosis Results

The development of a proposed MOPS in the final phase of ASTRail has addressed a key issue with the use of GNSS within railway standards. Any standard must have sufficient scope to cover all intended uses of the treated technology. Since trains move from favourable GNSS conditions, known as open-sky conditions, through urban canyons which are areas in which signals are susceptible to disturbances leading

to significant errors and into tunnels for which signals are entirely blocked. This differs from aeronautical standards in which only classifications with respect to equipment types relating to the level of integration of displays and controls are needed.

The proposed solution to the MOPS is to define within the standards environment classes. This allows different modes to be assigned to operations within the different environments. An alternative, would be for the railway infrastructure manager to separate the network into areas in which the legacy solution (based on physical balises and odometry) applies and areas in which GNSS may be used. However, whilst this could account for tunnels, it would not take into consideration the strong variation in performance between open-sky and urban environments.

An attempt has been made therefore to classify the local environment. This classification could be invariant with respect to time or a function of it. The latter; however, presents in the view of ASTRail an unnecessarily complex solution that would require significant data collection, analysis offline prior to rail operations as well as heavy communication during operations. Whilst this approach was studied and is not ruled out as a potential future aspect of a GNSS Based Localisation System (GBLS), a fixed classification was preferred in this work and is used in the proposed MOPS. Environments are split into seven categories as a function of the minimum, average and maximum number of visible and blocked satellites over the combined constellation (GPS and Galileo) cycle with respect to the local terrain and infrastructure topographic databases. Each location along the track (at distances of 10m in this work) is assigned an environment class through this offline work, that would be provided in the form of a database or through communication to the train. An example of such a classification is shown below.

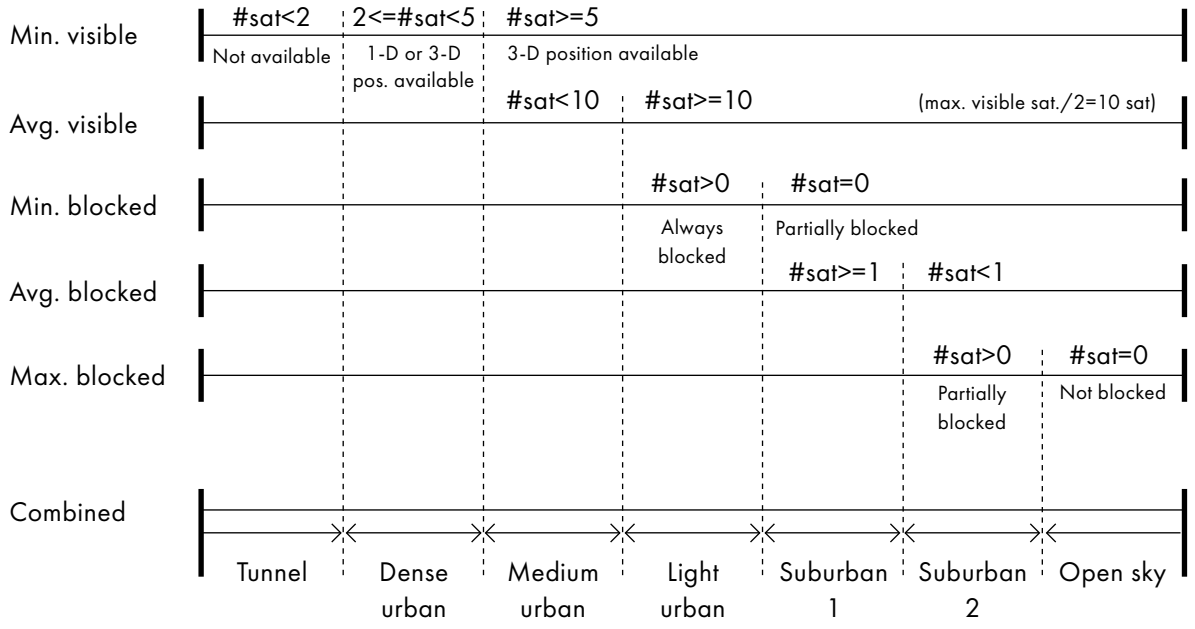


Figure 6. Environment Classes

The three GBLS modes eluded to above, legacy, enhanced odometry and virtual balise would then be employed in the tunnel, urban and suburban/ open sky environments respectively. Clearly in a tunnel, no GNSS is available and the legacy (or updated with alternative sensors not susceptible to signal loss) approach must be used. In dense urban areas, some physical balises may be removed leading to cost reduction and GNSS may then be integrated with other sensors, existing odometry sensors and/or modern additions such as vision. In the less impacting environments, suburban and open sky, full GNSS based positioning, under the virtual balise concept, may be used, supported by integrity solutions such as the threat monitoring described above.

WP2 - SAFETY ANALYSIS OF MOVING BLOCK SIGNALLING SYSTEM

The ASTRail WP2 focuses on safety and security analysis of the Moving Block system in view of complete removal of trackside detection. This work stream contributes to the X2Rail-1 WP5 "Moving Block" that aims to define a high capacity, low cost, high reliability signalling system, based on Moving Block principles, which is applicable across all railway market segments.

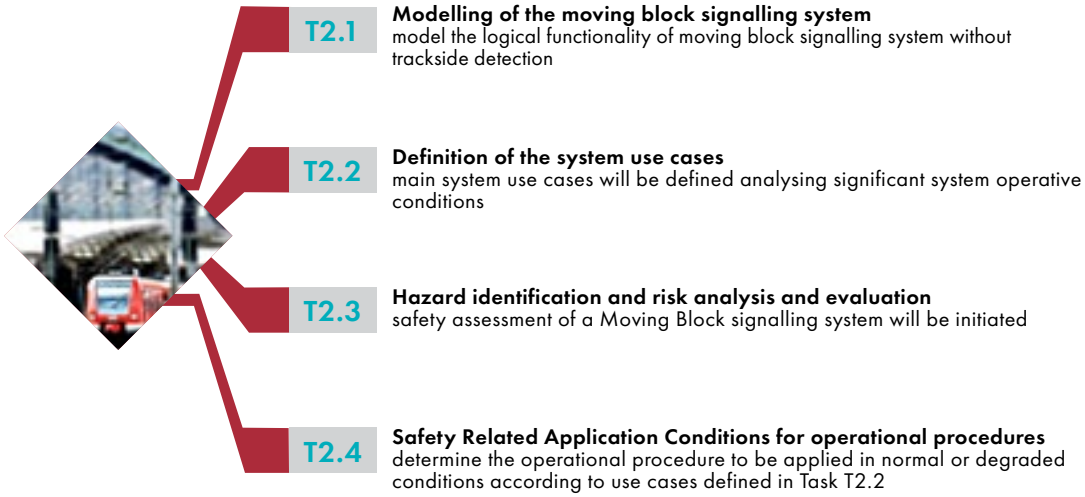
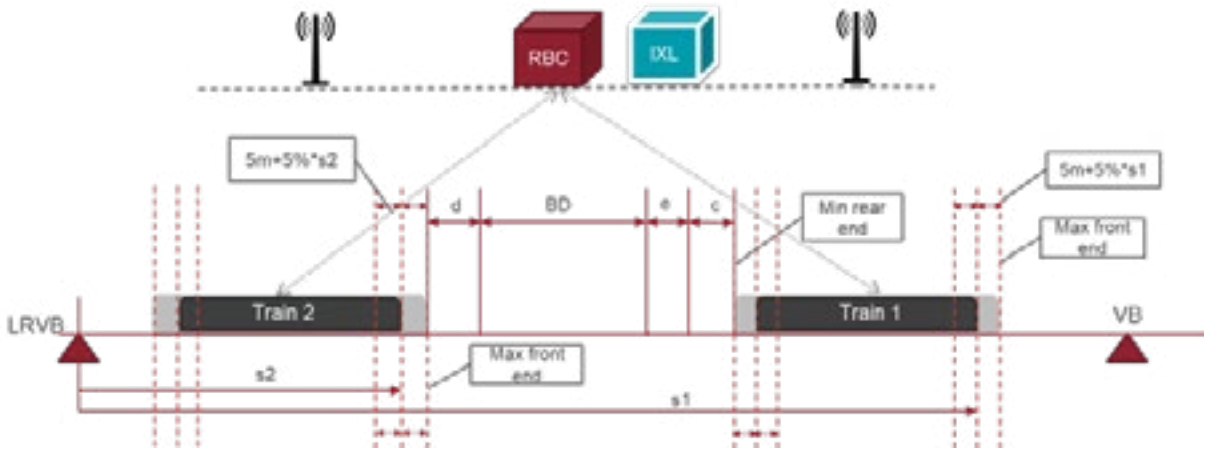


Figure 7. WP2 tasks

The safety assessment of a Moving Block signalling system (MBS) consisted in identification of hazards assigned to each safety function of the system, derived from GNSS relative errors, communication failures in main system interfaces and random and systematic failures of principal components of the system. The identified hazards were then analysed, and the risks associated with these hazards were evaluated.
To perform the Hazard Analysis, the MBS system safety functions have been defined applying the top-down analysis which has been derived from the most common types of railway accidents and the scenarios which can lead to these accidents and involve signalling system. The analysis is based on MBS system model considering the interchange of the data between its main components.
After the determination of the MBS system safety functions, the hazards which can prevent system from performing its safety function have been defined, their plausible causes and consequences have been analysed. The results of the analysis are recorded in the Hazard Log which contains the hazards identified during the

analysis and the evaluated risk, proposed mitigations measures, derived requirements and related operational conditions.
Moreover, the most significative system Use Cases have been identified and analysed from the safety point of view, concluding about achievable safety level in each case and the hurdles encountered to assure SIL4 level with the explanation of the related hazards. The hazards with residual risk different from negligible are highlighted along with the discussion on the possibilities to reduce it to at least "tolerable" level. In the analyses it is assumed that only technical measures can assure risk reduction to "negligible" level, while operational measures will in the best case achieve "tolerable" level due to human factor presence.



Picture legend:

LRVB- Last Reference Virtual Balise
VB- Virtual Balise
s1- train 1 distance from LRVB
s2- train 2 distance from LRVB
RBC- Radio Block Centre
IXL- Interlocking system
BD-Breaking Distance
d- deadline to emergency break
e- positioning error
c- message delay

Figure 8. Moving Block signaling system based on Virtual Balise

WP3 - AUTOMATIC DRIVING TECHNOLOGIES FOR RAILWAYS

The aim of ASTRail WP3 is to provide recommendations about the technological solutions, coming from non-railway sectors (e.g. automotive, agriculture, avionics and maritime sectors), which may be exploited in the next future for enhancing autonomous driving in the railway sector.

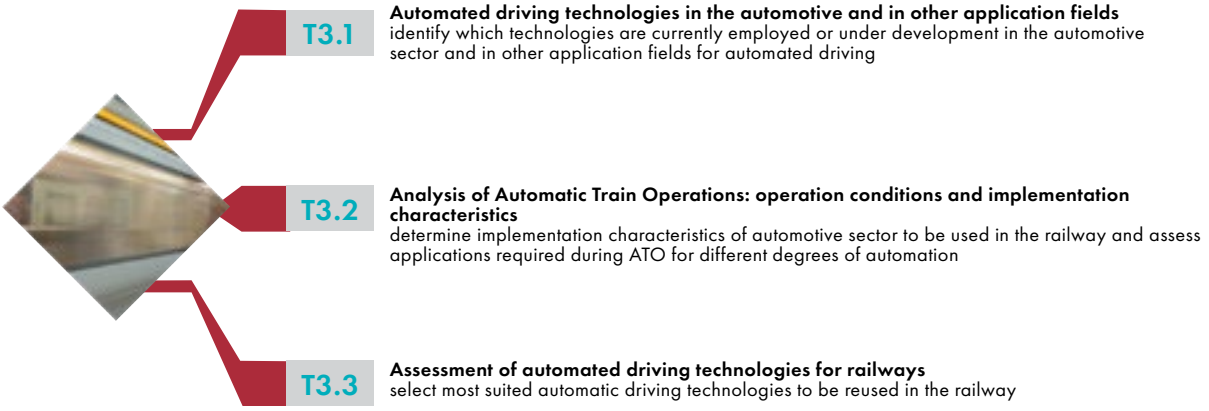


Figure 9. WP3 tasks

To achieve its goal, ASTRail first performed an analysis of the state-of-the-art technologies for autonomous driving, based on mature and cutting-edge solutions. After having defined the implementation characteristics and types of applications, which can be transferred in the railway's field from the automotive and other sectors, ASTRail identified the best autonomous driving solutions, considering specific use cases and different grade of automation in Automatic Train Operation (e.g. driverless or unattended operations).

Summarizing, the main high-level outcomes of the WP3 activities are:

- 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, railway environment;
- It is difficult that a single technology can guarantee to satisfy a requirement in all conditions and cases, a multi-sensors data fusion system, which exploits more than one technology, is expected to provide a more accurate, reliable and effective solution.

WP4 - FORMAL METHODS FOR THE RAILWAY FIELD

ASTRail WP4 aims at identifying the most mature formal languages and methods to be used in the railway industry for safety-critical system and software development. This goal is achieved by means of a systematic literature review of formal methods applications in railways, and through trial applications of formal methods and tools for the ERTMS Level 3 moving-block system concept and automatic train operation (ATO) principles. Surveys with practitioners are also performed to investigate the current uptake of formal methods and features desired by the railway industry.

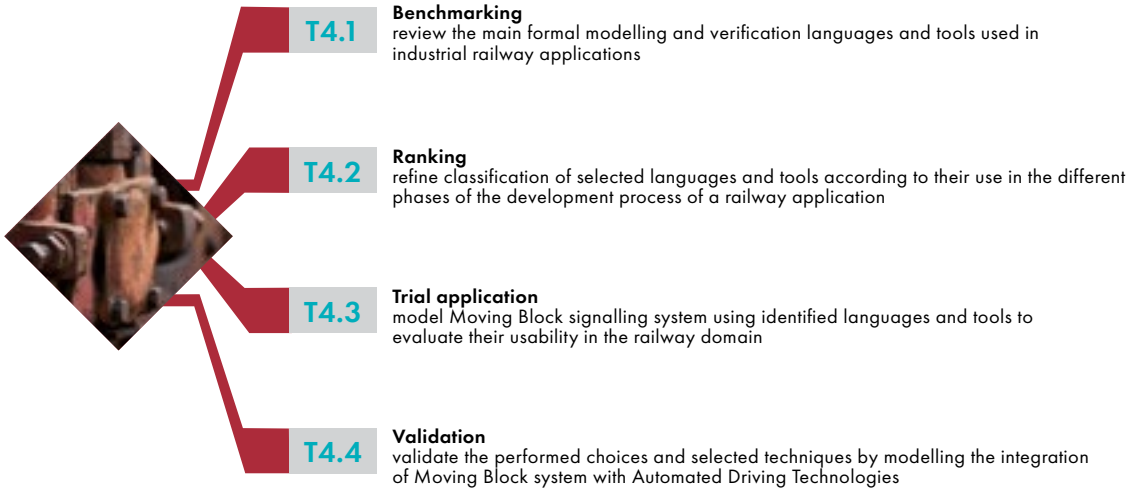


Figure 10. WP4 tasks

ASTRail WP4 has completed Task 4.3 and is completing Task 4.4. To address the goal of identifying the most adequate formal methods for modelling railways systems, T4.3 aimed at experimenting the usage of a set of selected formal methods through the modelling of the moving-block system defined in T2.1. Selected on the basis of Tasks 4.1 and 4.2, a total of 8 formal tools (Simulink, SCADE, UPPAAL, NuSMV, SPIN, UMC, ProB, Atelier B) have been used to model the moving-block system following the requirements provided by WP2 and according to the approach sketched in Figure 11.

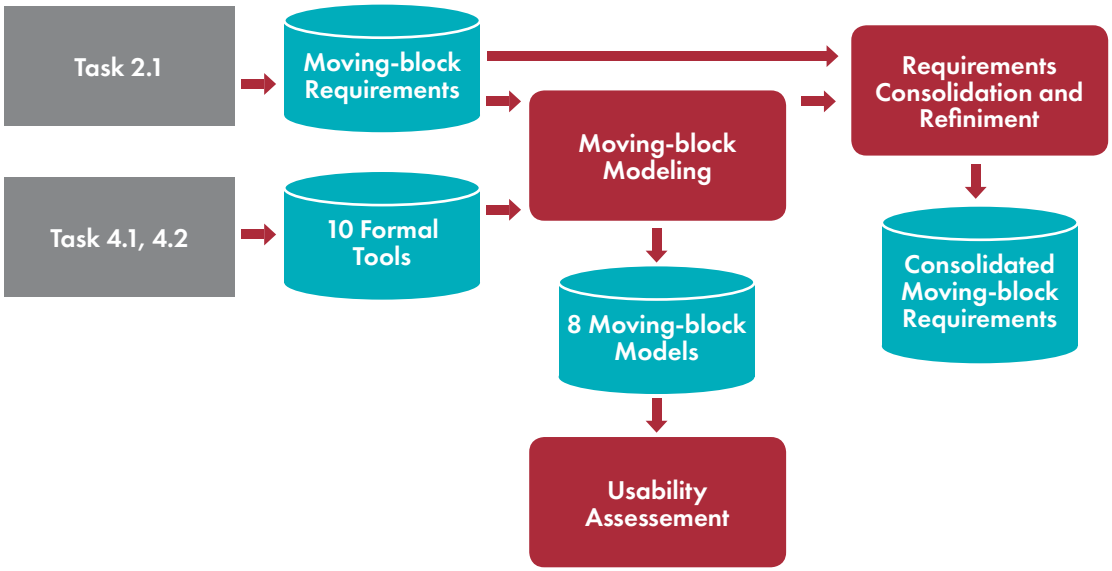


Figure 11. Overview of the followed approach

This multiple modelling activity has provided interesting hints concerning the capabilities of the different tools: some tools, such as Simulink and SCADE, are more appropriate if one aims at creating prototypes that can be simulated and wishes to generate code from the models. Others, such as UML and associated tools, are more appropriate if one wishes to provide a high-level view of the system architecture, and aims to communicate with stakeholders with different backgrounds. Tools such as SPIN or NuSMV are more oriented to brute-force formal verification of large systems. Model checkers such as UPPAAL are appropriate when one wishes to verify real-time and probabilistic aspects of a system, possibly by means of statistical model checking. Finally, tools based on the refinement paradigm, such as ProB and Atelier B, are more oriented towards top-down development of single systems rather than composition of systems.
A usability assessment of the 8 tools was performed by means of a showcase involving industrial railway stakeholders, who preferred at this regard the provision of graphical modelling languages such as those given by Simulink and SCADE.
As a side effect of the modelling activity, a requirements consolidation and refinement phase was performed, also employing analysis by means of NLP techniques, providing as results a final set of requirements for the moving-block system.

Task 4.4 aims at a further validation of the usage of the selected formal methods by integrating in the moving-block model the ATO from T3.3. The first step concerned the requirements elicitation for the ATO features, additional moving block requirements, and integration-related aspects, from stakeholders and documentation.
To support requirements elicitation, Simulink (and its package for state machines modelling, named Stateflow) was chosen, on the basis of the experience and the tool usability evaluation of T4.3, to model the requirements and to check their coherence by means of a simulation prototype.

The results of the previous tasks have indicated ProB as the preferred tool for the formal verification of the elicited requirements, i.e., verification of qualitative properties related to conditions and expected actions. To facilitate the transition from Simulink and corresponding natural language requirements to ProB, UML was chosen as intermediate representation language.

The steps supported by the mentioned tools are part of the process depicted in Figure 2. The starting point of the process is the set of input documents about the systems to be developed, specifically the moving-block system requirements developed in T4.3, and the requirements for the ATO system available from the Shift2Rail X2Rail-1 project.

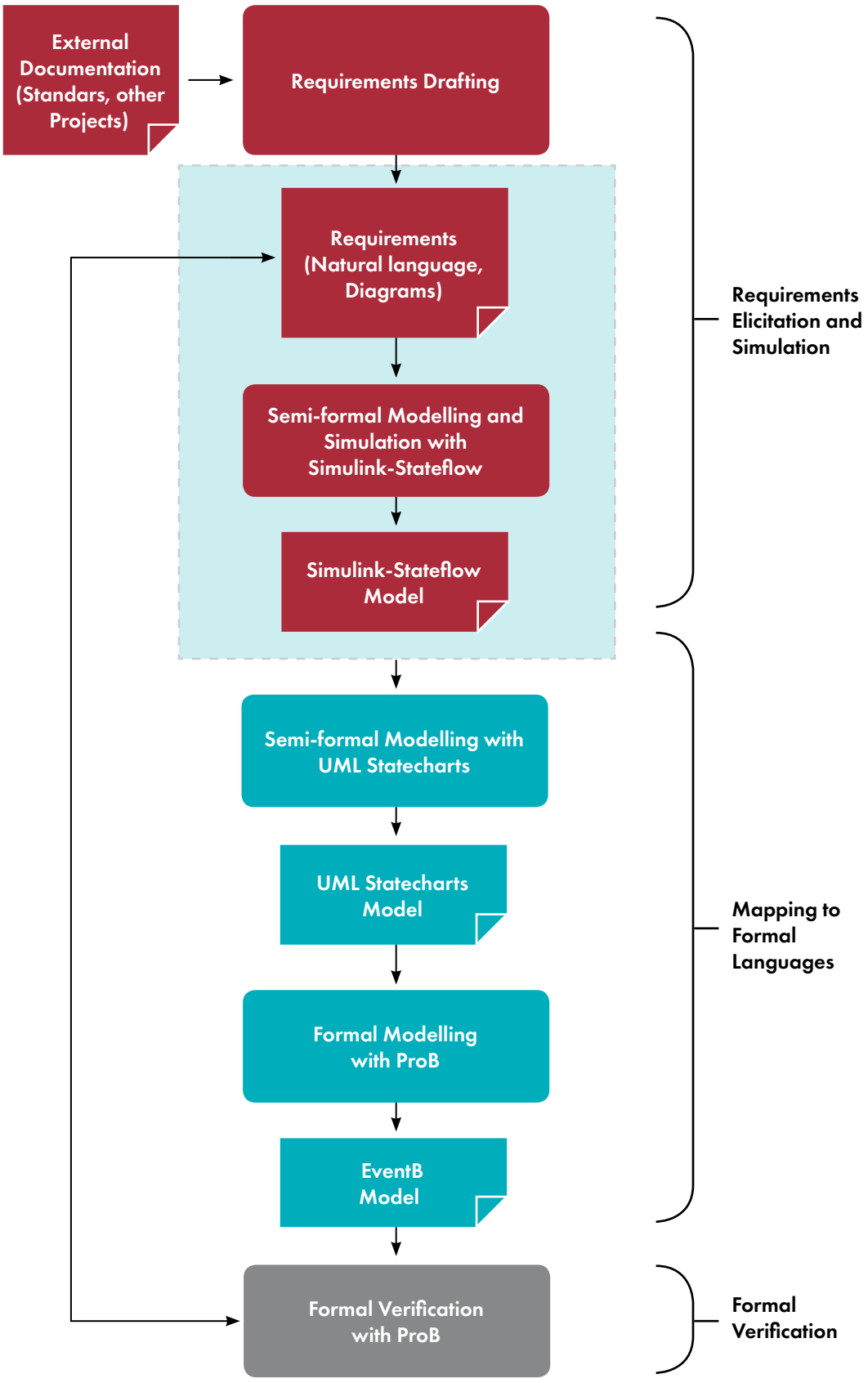


Figure 12. Overview of the adopted formal process

FACTS AND FIGURES

1.8€
Million

6
Partners

26
Months

Project Start Date:
1st September 2017

Project End Date:
31st October 2019

Grant Agreement n:
777561

PARTNERS

Project coordinator

Technical leader

Project partners

CONTACT US

Riccardo Scopigno
Project Coordinator, Linksfoundation
riccardo.scopigno@linksfoundation.com

PROJECT WEBSITE

www.astrail.eu

PROJECT TWITTER ACCOUNT

www.twitter.com/S2R_ASTRail