Contribution to safety and operational performance evaluation of GNSS-based railway localization systems using a formal model-based approach

Ouail Himrane

Université de Lille - Sciences et Technologies
Université Gustave Eiffel

THÈSE

présentée en vue d'obtenir le grade de

DOCTEUR

en

Automatique, Génie Informatique, Traitement du Signal et des Images

par

Ouail HIMRANE

Doctorat délivré par l'université de Lille

Titre de la thèse :

Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach.

Contribution à l'évaluation de la sécurité et des performances opérationnelles des systèmes de localisation ferroviaire utilisant le GNSS par une approche fondée sur les modèles formels.

Soutenue le 16/12/2022 devant le jury d'examen :

Présidente	Juliette Marais	Directrice de recherche	Université Gustave Eiffel - COSYS/LÉOST
Rapporteur	Mohamed Sallak	Maître de conférences-HDR	Université de Technologie de Compiègne
Rapporteur	Ouajdi Korbaa	Professeur	ISITCOM - Université de Sousse
Examinatrice	Rim Saddem	Maître de conférences	Université Marseille-Aix
Invitée	Imen Ben Hafaiedh	Maître de conférences	ISI - Université Tunis El Manar
Invité	Bob Janssen	Docteur-ingénieur	Eulynx, Pays bas
Directeur de thèse	Mohamed Ghazel	Directeur de recherche	Université Gustave Eiffel - COSYS/ESTAS
Encadrante	Julie Beugin	Chargée de recherche	Université Gustave Eiffel - COSYS/ESTAS

Thèse préparée au Laboratoire d'Évaluation des Systèmes de Transports Automatisés et de leur Sécurité
Université Gustave Eiffel, COSYS/ESTAS, Villeneuve d'Ascq
École Doctorale MADIS-631 - Université Lille Nord de France

Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach.

Abstract

Transportation systems are safety-critical systems whose failures may result in considerable losses. In railway transportation, this may involve damage to equipment and environment, serious injury to people or even the loss of human lives. In order to avoid train collision or derailment, safety-related functions (e.g., management of routes allocation, safe distance separation between trains, and over-speed prevention) are implemented. These functions are at the core of railway control-command and signaling systems (CCS) which provide the driver with the relevant information and warnings to adapt the speed of the train or brake when necessary.

Historically, European rail CCS systems were developed on a national basis. Hence, the absence of common technical and operational standards has considerably limited the railway interoperability between countries. That is why the European Rail Traffic Management System (ERTMS) standard was defined with the aim of harmonizing the railway systems throughout Europe. More specifically, European Train Control System (ETCS) is the CCS component of the ERTMS. This system is essential to guarantee the safe and interoperable operation of trains. To enhance the competitiveness of rail transport services, the introduction of innovative solutions is under study in view of the evolution of ETCS. In this context, the adoption of Global Navigation Satellite System (GNSS) for train localization is investigated as a technology which can ensure an undeniable added value for railways. In particular, the adoption of such satellite-based solution should permit the train to autonomously and continuously determine its location. Hence, implementing more flexible operating principles (i.e., Moving Block) that pave the way for increasing line capacity while reducing maintenance and operating costs shall be possible.

However, the introduction of such technological innovations leads to the emergence of new risks that need to be investigated meticulously. Accordingly, a main challenge is to provide safety evidence permitting the certification of these new systems. In particular, classical safety analysis approaches (e.g., FMECA, HAZOP, FTA) show limitations in dealing with the complexity of such systems. Therefore, more adapted safety and performance analysis techniques need to be elaborated.

The contribution of this thesis falls within this context by proposing a model-based approach to evaluate performance and safety properties related to the use of GNSS-based localization systems in railway. Specifically, the investigated method consists in translating the relevant behavior of the train localization system through a modular and configurable representation.

Considering the safety-critical aspect of the localization function in railways, formal methods which are based on rigorous mathematical foundations are adopted in the present work. Namely, probabilistic timed automata formalisms are employed. Concretely, such notations allow for considering stochastic and dynamic aspects, so as to reflect the GNSS-related uncertainties in a trustworthy way.

The elaborated models being parameterizable, various operational scenarios, considering a wide range of configurations, can be investigated. Such a feature is particularly relevant considering the impact of the environmental conditions on the GNSS performances.

Then, the safety and performance properties to be checked can be formulated by means of temporal logics. Accordingly, the analysis of such features can be achieved by means of model-checking and simulation techniques. This evaluation phase yields both qualitative and quantitative results and allows for assessing the impact of various parameters and functional choices on both safety and performance. In this thesis, UPPAAL-SMC is used to set the tooling chain of our approach, and to provide illustrative numerical analysis results considering various operational cases study.

Finally, as the present contribution implements a model-driven technique to perform safety analysis in railways, it is fully in line with the increasing willingness to reduce recourse to on-site tests in the sector (as such costly and time-consuming tests jeopardize the introduction of technical innovations in railways).

Keywords: railway system safety; model-based approach; gnss-based train positioning; formal methods; ERTMS/ETCS; intelligent transportation systems

Résumé

Les systèmes de transport collectifs sont des systèmes critiques dont les défaillances peuvent entraîner des pertes considérables. Dans le cas du transport ferroviaire, ces défaillances peuvent mener à des dommages matériels ou environnementaux, des blessures graves ou des décès de personnes. Afin d'éviter les collisions et les déraillements de trains, des fonctions liées à la sécurité telles que la gestion des itinéraires, la séparation entre les trains et la prévention de survitesses, sont mises en œuvre. Ces fonctions sont au cœur des systèmes de Contrôle-Commande et de Signalisation ferroviaire (CCS) et fournissent au conducteur les informations et les avertissements nécessaires leur permettant d'ajuster la vitesse du train ou de freiner si nécessaire.

Historiquement, les systèmes CCS ferroviaires européens ont été développés sur la base de principes nationaux. De ce fait, l'absence de normes communes a considérablement limité l'interopérabilité ferroviaire entre les pays. C'est pourquoi, le système européen ERTMS (European Rail Traffic Management System) a été défini dans le but d'harmoniser les systèmes ferroviaires à travers l'Europe. Plus précisément, le système européen de contrôle des trains ETCS (European Train Control System) est la composante CCS de l'ERTMS. L'utilisation de ce système est requise pour garantir l'exploitation sûre et interopérable des trains. Afin de répondre à la demande croissante et renforcer la compétitivité des services de transport ferroviaire, l'introduction de solutions innovantes est actuellement à l'étude en vue de l'évolution de l'ETCS. Dans ce contexte, les technologies de rupture comme celles s'appuyant sur les GNSS (systèmes globaux de navigation par satellite) sont explorées pour améliorer la localisation des trains. En effet, l'adoption de solutions satellitaires permettra à un train de déterminer sa position de manière autonome et continue. Ainsi, il sera possible d'implémenter des principes d'exploitation plus flexibles (tels ceux liés aux cantons mobiles) permettant d'augmenter la capacité des lignes tout en réduisant les coûts de maintenance et d'exploitation.

Toutefois, l'introduction de ces innovations technologiques entraîne l'apparition de nouveaux risques qui doivent être analysés méticuleusement. En conséquence, l'un des principaux défis consiste à fournir des preuves de sécurité permettant la certification de ces nouveaux systèmes. En outre, les approches classiques d'analyse de la sécurité (par exemple, AMDEC, HAZOP, FTA) montrent des limites face à la complexité de ces systèmes. Ainsi, des techniques d'analyse de sécurité et de performance plus adaptées doivent être élaborées.

Ces travaux de thèse s'inscrivent dans ce contexte en proposant une approche orientée modèles afin d'évaluer des propriétés de sécurité et de performance liées à l'utilisation de systèmes de localisation intégrant les GNSS pour l'exploitation ferroviaire. Compte tenu de l'aspect critique de la sécurité liée à la fonction de localisation, les méthodes formelles qui reposent sur des fondements mathématiques et logiques rigoureux sont mises à profit. En particulier, les formalismes d'automates temporisés probabilistes sont employés. Concrètement, ces notations permettent de prendre en compte les aspects temporels et aléatoires dans le comportement de la fonction de localisation, de manière à refléter les incertitudes liées au GNSS d'une manière fiable. Les modèles élaborés étant paramétrables, divers scénarios opérationnels, considérant une large variété de configurations, peuvent ainsi être étudiés. Cette possibilité est particulièrement pertinente compte tenu de l'impact des conditions environnementales sur les performances du GNSS. Sur la base des modèles développés, des propriétés de sécurité et de performance à vérifier peuvent être formulées au moyen de logiques temporelles. En conséquence, l'analyse de ces caractéristiques peut être réalisée à l'aide de techniques de vérification analytique et de simulation. Cette phase d'évaluation permet d'obtenir des résultats qualitatifs et quantitatifs et offre la capacité d'anticiper l'impact de différents paramètres et choix fonctionnels sur la sécurité et les performances. Dans cette thèse, l'outil UPPAAL-SMC est utilisé comme support à notre approche et nous permet d'obtenir des résultats d'analyse numérique illustratifs, en considérant divers cas d'étude opérationnels. La contribution proposée adoptant des techniques fondées sur des modèles répond avantageusement à la volonté croissante de réduire le recours aux essais sur site ferroviaire pour vérifier des conditions ou propriétés de sécurité. Ces essais étant coûteux et chronophages, ils compromettent l'introduction d'innovations techniques dans le secteur ferroviaire.

Mots clés : sécurité des systèmes ferroviaires ; approche fondée sur les modèles ; positionnement des trains par gnss ; méthodes formelles ; ERTMS/ETCS ; systèmes de transport intelligents

Acknowledgment

This thesis manuscript cannot be considered complete without expressing my heartfelt thanks to all the persons who supported and encouraged me throughout my PhD journey.

First, my acknowledgments are due to my advisors, *Mr. Mohamed Ghazel, and Ms. Julie Beugin* for giving me the opportunity to follow this thesis. Without their confidence, patience, and constant encouragement, this work would not have been possible.

I would also like to express my gratitude to *Ms. Juliette Marais* for accepting to be the chair of my jury. I would like to extend my respectful thanks to the members of my jury, *Mr. Ouajdi Korbaa, Mr. Mohamed Sallak, Ms. Imen Ben Hafaiedh, Ms. Rim Saddem, and Mr. Bob Janssen* for their time and valuable feedback. Their insights and suggestions will undoubtedly contribute to the improvement of my research.

Thanks should also go to all the members of the Université Gustave Eiffel (COSYS/ESTAS and LEOST laboratories) and IRT Railenium. It has been a pleasure to have you around me during the last few years. *Sonia, Nathalie, Joaquin, Philip, Simon, Marielle, Miloudi, Insaf, and Sébastien*, your kindness, caring and good mood have made the work place a very pleasant and joyful environment.

Special recognition goes to *Nourdine and Abderraouf* who believed in me and provided me with guidance and support. Their dedication has been invaluable to me. For that, I am grateful and delighted that our paths have crossed.

My heartfelt thanks are extended to my family and friends. This endeavor would not have been possible without their unwavering support and understanding. *Redha, Samira, Fateh, Mohammed, Abhi, Ali, Sana, Dalay, Sabrine, Chakib, Reza*, many thanks for all the moments of happiness and joy shared on a daily basis both in and outside the work environment.

Last but not least, words cannot express my gratitude to *my parents, my wife, and my brother.* Their love and encouragement have been my source of strength throughout this challenging yet rewarding journey. Without them, I would not be the person I am today.

Finally, I thank all those who have contributed in any way to the completion of this thesis.

To the memory of my grand parents.
To my mother & my father.
To my wife & my brother.
To my uncle Redha.

Contents

List of Tables

List of Figures

Acronyms

AL	Alert Limit
APIS	Authorization for Placing Into Service
ATP	Automatic Train Protection
ATPL	Along Track Protection Level
BDD	Binary Decision Diagrams
BDS	BeiDou navigation satellite system
BG	Balise Groups
BTM	Balise Transmission Module
CBTC	Communication-Based Train Control
CCS	Control-Command and Signalling
CNSS	Compass Navigation Satellite System
CoP	Code of Practice
CPF	Central Processing Facility
CPN	Colored Petri Nets
CSM-RA	Common Safety Method for Risk Evaluation and Assessment
CSMs	Common Safety Methods
CTCS	Chinese Train Control System
EGNOS	European Geostationary Navigation Overlay Service
EMI	Electromagnetic Interferences
EoA	End of Authority
ERE	Explicit Risk Estimation
ERTMS	European Rail Traffic Management System
ETA	Event Tree Analysis
ETCS	European Train Control System
EU	European Union
EVC	European Vital Computer
FMB	Full Moving Block
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FTA	Fault Tree Analysis
FVB	Fixed Virtual Block
GBAS	Ground Based Augmentation System
GLONASS	Global'naya Navigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HAZOP	Hazard and Operability studies
HMI	Hazardously Misleading Information

HPL	Horizontal Protection Level
ICAO	International Civil Aviation Organization
IGSO	Inclined Geosynchronous
IMU	Inertial Measurement Units
INCOSE	International Council on Systems Engineering
IR	Integrity Risk
LML	Lifecycle Modeling Language
LOS	Line-of-Sight
LRBG	Last Relevant Balise Group
LTS	Labeled Transition Systems
MA	Movement Authorities
MA	Markov Automata
MBSA	Model-Based Safety Analysis
MBSE	Model-Based Systems Engineering
MC	Model-Checking
MC	Model-Checking
MEO	Medium Earth Orbit
MI	Misleading Information
MITL	Metric Interval Temporal Logic
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NLOS	Non-Line-of-Sight
NSTA	Network of Stochastic Timed Automata
NTA	Timed Automata
PB	Physical Balises
PE	Position Error
PHA	Preliminary Hazard Analysis
PL	Protection Level
PN	Petri Net
PTA	Priced Timed Automata
RAMS	Reliability, Availability, Maintainability and Safety
RAP	Risk Acceptance Principle
RBC	Radio Block Center
SBAS	Satellite Based Augmentation System
SIL	Safety Integrity levels
SMC	Statistical Model Checking
STA	Stochastic Timed Automata
SysML	Systems Modeling Language
TA	Timed Automaton
THR	Tolerable Hazard Rate
TOA	Time of Arrival
TSIs	Technical Specifications for Interoperability
TTA	Time To Alert
UML	Unified Modeling Language
VB	Virtual Balises
VBR	Virtual Balise Reader
VPL	Vertical Protection Level
WMTL	Weighted Metric Temporal Logic

Chapter 1

Introduction

Outline of the current chapter

1.1 General Context

Identified by the Conference of the Parties (COP) as one of the major threats of the 21st century, evidence of global warming and the challenges caused by its impact continues to grow (Conference of the Parties 2022).

More specifically, the Intergovernmental Panel on Climate Change (IPCC) established that warming of the climate system is *"unequivocal"* and it is "*extremely likely*" that human influence has been the dominant cause of warming since the mid-20th century (Intergovernmental Panel on Climate Change 2022).Moreover, the IPCC stated that *'Continued emissions of greenhouse gases (GHG) will cause further warming'* and *'limiting climate change will require substantial and sustained reductions of greenhouse gas emissions'*.

Focusing more particularly on the European context, the European Environment Agency (EEA) claims that transport accounts for 27% of the Europe's total CO2 emissions (in 2018) (European Environment Agency 2021).

In this same context, the International Union of Railways (UIC) announced in a report published in 2015 that emissions from the transport sector primarily originate from road transport (72%), while maritime and air transport account for 14% and 13% of emissions, respectively (International union of railways 2015; European Environment Agency 2022), (see Figure 1.1).

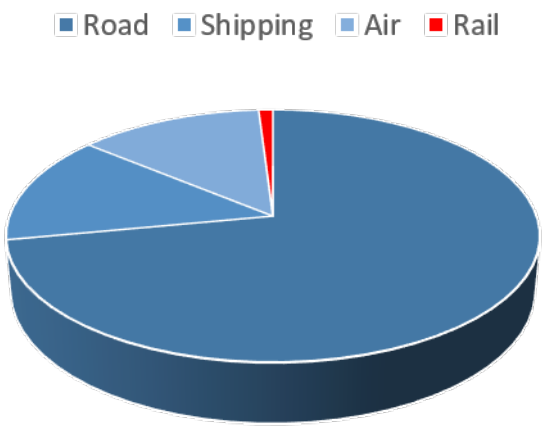


Figure 1.1: Share of the European Union CO2 emissions from transport

In this same report, one can find that the railway sector accounts for just 0,6% of transport GHG emissions through direct usage (diesel), and by around 1,5% if emissions from electricity generation are taken into account, even though railways represent 8,5% of transport activity.

Thus, it is plain that rail is the most emissions-efficient major transportation mode. This observation is even more accentuated given that modern trains can be powered by renewable energy, hence offering practically neutral carbon footprint. Accordingly, having a higher share of passenger and freight journeys performed by train is fundamental for decarbonizing the transport sector. Besides, today the global railway stakeholders are working hard to maintain

the environmental advantage of the sector, especially as the demand for passenger and freight transportation services has significantly increased in recent years (Cowie 2009).One of the main challenges in this context is to find viable solutions to substantially increase the railway capacities. Yet, the definition of railway capacity is a classical problem, and the assessment of this feature has long been a significant issue in the railway industry (Abril et al. 2008; Stok 2008; Pouryousef, Lautala, and White 2015; Damy 2016; Landex 2008). It should be noted that the term '*railway capacity*' can refer to two distinct significations. On one hand, the first meaning is related to the '*Passenger capacity*', which represents the number of passengers that can be accommodated in a passenger train. On the other hand, the *'Line capacity*' is pertaining to the maximum number of trains that can be operated simultaneously on a line without conflict. Thus, based on these definitions, the increase in railway capacity can be achieved through different approaches:

- The first approach consists in building new railway lines. However, such a solution obviously requires a lot of resources and, thus, can be economically unviable. Moreover, this approach may not even be feasible in certain conditions due to the constraints related to the already saturated urban environment.

- The second approach for increasing the railway capacity is to operate longer trains. Nevertheless, the train length remains constrained by the dimensions of the station platforms along the rail line.

- Finally, the third approach consists in operating more trains while using the same infrastructure. Concretely, this could be achieved through optimizing the timetables and allowing the trains to run closer to each other.

Considering the constraints pertaining to each of the aforementioned alternatives, the third option is particularly investigated in order to more optimally exploiting the existing resources. As a result, several academic and industrial research projects (e.g., Shift2Rail) are conducted at the European level with the common objective of contributing to the development of new generation of railway control/command and signaling systems that allow for higher railway train density at the cost of a minimal investment.

Now that the high level context of our work has been outlined, we should expose the main subsystems composing the railway system. It should be noted that decomposing the railway system can be made according to either a structural or a functional point of view, as detailed in Annex 2 of the DIRECTIVE (EU) 2016/797 2016 and illustrated in the Figure 1.2 below.

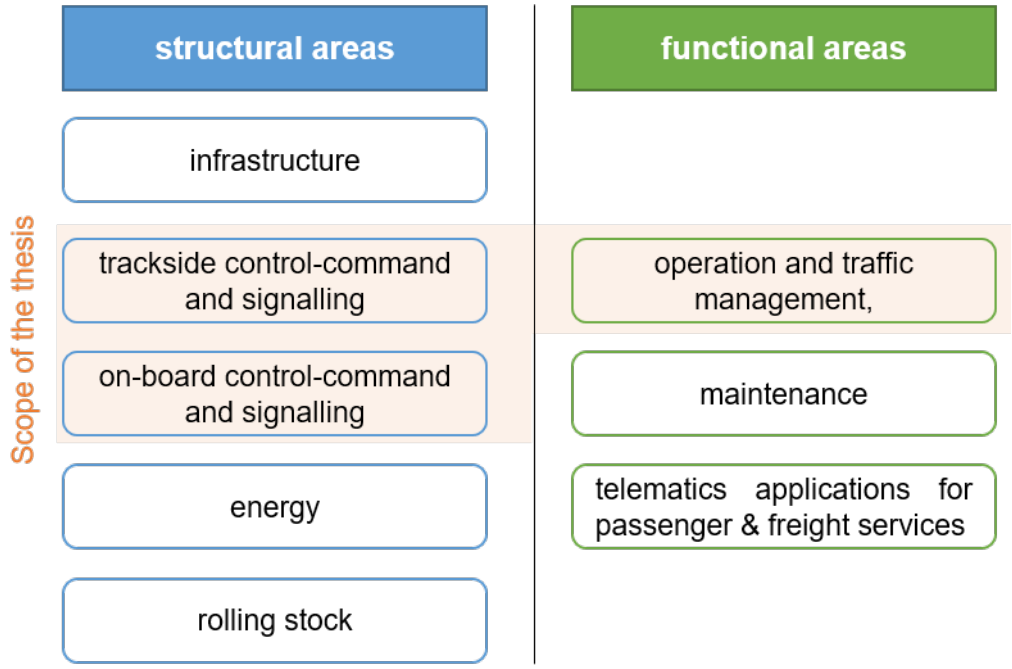


Figure 1.2: Overall decomposition of the rail system into subsystems according to DIRECTIVE (EU) 2016/797 2016.

One of the main challenges to be tackled towards increasing railway train density is to achieve an efficient localization of the trains. In fact, the localization function plays a critical role in the safe control of train movement and in traffic management. The research conducted in the framework of this thesis falls in this particular context. Namely, we are particularly interested in the study of satellite-based train localization solutions. Indeed, bringing into play satellite-based localization in railway operation shall allow a quasi-continuous tracking of trains' positions, hence opening the way to various optimization possibilities in terms of railway operation. We should recall here that, in general, the railway localization function is fulfilled by relying on both the *Trackside* and *the On-board control-command and signaling subsystems*. For this reason, these subsystems will be referred to frequently in the rest of this manuscript.

1.2 Problems Statement

New technologies, such as GNSS-based systems (Global Navigation Satellite Systems), offer promising means to implement the train localization function while allowing for better operational performances (i.e., increase of railway capacity). Furthermore, beyond performance improvement, such solutions allow for new operational concepts and principles to be implemented, such as the concept of "virtual balise" that will be addressed later in this thesis. This concept can be seen alongside the notion of "virtual block section," which is one of the main concepts at the center of the third operational level L3 of ERTMS (European Rail Traffic Management System), which is presented in Section 2.3. Operation under ERTMS L3 allows for reducing the train separation distance and, hence, increasing line capacity.

In this context, the Shift2Rail (S2R) [1] Joint Undertaking that coordinates the research and innovation investments of the H2020 European program in the railway domain has launched several projects, some of which consider the evolution of ERTMS, such as, X2Rail-1–5, MOVINGRAIL[2], and PERFORMINGRAIL[3]. Among different innovative topics pertaining to the ERTMS railway standard, these research projects explore the concepts of virtual blocks, moving blocks, and virtual balises (Shif2Rail 2022), particularly with respect to safety and performance evaluation. In the H2020 research program as well as in previous European research initiatives (not always under the aegis of S2R), some projects have explicitly focused on proving the feasibility of using GNSS-based on-board systems to implement the railway localization function (Marais, Beugin, and Berbineau 2017). Projects such as STARS[4], RHINOS[5], ERSAT-GGC[6], ASTRAIL[7] and GATE4RAIL[8] have resulted in multiple innovative solutions, and conducted wide measurement and testing campaigns that support the integration of GNSS-based solutions in ETCS (European Train Control System), which is the automatic train control and protection subsystem in ERTMS. Several challenging issues were tackled in these projects, such as the local propagation effects in harsh railway environments (with vegetation, buildings, hills, railway cuttings, etc.) and those due to interference. These aspects directly impact the signal quality and, therefore, the localization performances, which can raise safety hazards.

Considering the safety-critical nature of the localization function in railway Control-Command and signaling systems (CCS) like ERTMS, an essential prerequisite for the adoption of GNSS-based systems is related to the definition of the relevant safety requirements and providing a set of safety evidence that allows their certification in accordance with the in force regulations (today the CCS Technical Specification of Interoperability Regulation TSI CCS (EU) 2016/919 2016) .

When conducting safety analysis regarding the use of satellite-based localization systems in railways, three crucial issues can be identified:

1. Firstly, GNSS have their own performance criteria that are issued, mainly, from aeronautics and which are defined in terms of MOPS (*Minimum Operational Performances Standards*). Therefore, railway safety properties have to be formulated w.r.t the existing GNSS criteria and the railway operation rules and standards.

2. Secondly, it is not appropriate to only consider the inherent risk of the localization system, since the safety analysis has to be conducted at system level while considering the global risk of the system in operation within a given environment. Nevertheless, the constraints induced by the railway environment on GNSS signals are not easy to analyze and quantify. Besides, performing ad-hoc on-site tests proves to be awkward, costly, and very time-consuming.

3. Thirdly, the different possible choices regarding the architecture of GNSS-based localization systems involve various specific fault detection techniques, which makes defining a generic and systematic safety assessment process particularly challenging. In general terms, the classical safety analysis approaches show limitations in dealing with the complexity of such systems in their operational environment. Besides, the lack of adequate safety

[1] projects.shift2rail.org
[2] www.movingrail.eu
[3] www.performingrail.com
[4] www.stars-rail.eu/
[5] cordis.europa.eu/project/id/687399, and rhinos-h2020.org/
[6] www.ersat-ggc.eu/
[7] www.astrail.eu/
[8] www.gate4rail.eu/

demonstration tools to assess and qualify GNSS-based railway localization solutions is noticeable. Obviously, this constitutes a considerable obstacle for the deployment and acceptance of GNSS-based systems in railway CCS. The various questions we address within this thesis are directly linked to these issues.

1.3 Main Contributions

In order to foster the introduction of GNSS-based solutions in railways and set the stage for innovative and performing railway operational modes, advanced safety and performance analysis techniques need to be elaborated. The research work conducted during this thesis falls within this context and is intended to comply with the following criteria:

1. As the GNSS systems typically adopt performance criteria originating from aeronautics, those criteria cannot be employed without some adaptation effort to the railway operation context. Thus, the first step of our contribution focuses on considering the GNSS-based railway localization block as a black box, and attempting to identify the relevant performance criteria that are adequate to the railway context. For this purpose, research works dealing with the relation between GNSS and railway performance, such as in (Filip, Beugin, et al. 2008; Beugin, Filip, et al. 2010; Beugin and Marais 2012; Lu and Schnieder 2014), will be particularly addressed.

2. Satellite-based localization systems are, by nature, particularly sensitive to the environment in which they are deployed. It is then apparent that the analysis of a train localization solution cannot be properly carried out without taking into account the railway environment in which the GNSS receiver operates. Therefore, the method described in this contribution seeks to consider the surrounding environment's characteristics as inputs and to reflect their potential effects on the outputs generated by the localization solution. Namely, the outcomes of our analysis need to be consistent with the environment in which the considered system evolves (Himrane, Beugin, and Ghazel 2020b; Himrane, Beugin, and Ghazel 2020a).

3. It is important to recall that no architecture of the GNSS-based train localization solution has yet been agreed upon. Therefore, it is essential that the proposed safety and performance verification method relies on a modular and parametrizable logic. This should not only enable to take into account the complexity of the treated system gradually, but also open the way to reuse some modules and adapt them to analyze different localization solutions through certain input adjustments (Himrane, Beugin, and Ghazel 2021).

In the last two decades, formal verification has matured considerably thanks to more sophisticated algorithms for formal verification and more powerful computers (Ferrari, M. H. t. Beek, et al. 2019). Formal methods are techniques that are based on mathematical and logical foundations, and allow for rigorously describing the system behavior and setting the basis for automatic verification of a wide range of settings. Besides, the Shift2Rail Joint Undertaking (S2R JU) has identified the use of formal methods as one of the key concepts to enable reducing the time it takes to develop, test, certify and deliver railway control-command and signaling systems, and to reduce high costs for procurement, development and maintenance. In fact,

formal methods are deemed as promising means to ensure correct behavior, interoperability and safety on these systems, while, at the same time, reducing long-term life cycle costs. Besides, formal methods have already been brought into play in a number of railway CCS projects with noticeable success stories (Ferrari and M. H. t. Beek 2021), see Section 3.3.3. In this S2R JU initiative, two complementary projects, one proposed by the JU Members themselves, the other one as a result of an open call, respectively X2Rail-2[9] X2Rail-4[10] and ASTRail[11], have been funded having as one of the common objectives to perform a state of the art on formal methods' application in railways, so as to identify the best-used practices.

The contributions developed in this thesis are in line with the aforementioned trends. They adopt Model-Based Engineering (MBE) to develop parametrizable and modular models that allow for rigorously capturing the various artefacts that intervene in the railway localization function while adopting, inter alia, GNSS-based solutions. The underlying idea is to establish a set of models that can cope with various operational configurations, and which can serve as a basis to derive various safety and performance analyses. Therefore, the analysis of different settings can be performed at the cost of a minimal adaptation effort. Namely, in our work, we use model-checking techniques to perform verification of various features. Model-checking is an automatic technique that allows for checking properties, specified by means of temporal logic formulas. Overall, the undertaken work is fully in line with the increasing willingness to reduce on-site testing which is costly and time-consuming.

In a related context, the main contributions stemming from this thesis have been communicated through a number of scientific publications, including:

- **Ouail Himrane**, Julie Beugin, Mohamed Ghazel. "Proposal for a model-oriented approach to evaluate the safety of railway signaling systems using GNSS". *Lambda Mu 22, 22e Congrès de maîtrise des risques et de sûreté de fonctionnement. Les risques au coeur des transitions (e-congrès)*, Oct 2020, Le Havre (e-congrès), France. pp687-696.
- **Ouail Himrane**, Julie Beugin, Mohamed Ghazel. "Towards a Model-Based Safety Assessment of Railway Operation Using GNSS Localization". *ESREL 2020 PSAM 15, 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, Nov 2020, Venise, Italy. 8p.
- Dalay Israel de Almeida Pereira, **Ouail Himrane**, Philippe Bon and Julie Beugin (2020). "From French National signaling Systems to ERTMS: Considering the Evolution of Trackside Systems". *The 13th International Conference on Computer Science and Information Technology (ICCSIT 2020)*, October 14-16, 2020. Amsterdam, The Netherlands
- Dalay Israel de Almeida Pereira, **Ouail Himrane**, Philippe Bon and Julie Beugin (2021). "From French National signaling Systems to ERTMS: Considering the Evolution of Trackside Systems". *International Journal of Signal Processing Systems (IJSPS).* , 9(2), pp11-16.
- **Ouail HIMRANE**, Julie Beugin, Mohamed Ghazel (2021). "Toward Formal Safety and Performance Evaluation of GNSS-Based Railway Localisation Function". *16th IFAC Symposium on Control in Transportation Systems*, Jun 2021. Lille, France

[9] projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2
[10] projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-4
[11] www.astrail.eu/

- **Ouail HIMRANE**, Julie Beugin, Mohamed Ghazel. "Model-Oriented Approach for Supporting the Safe Integration of GNSS-Based Virtual Balises in the Context of ERTMS/ETCS Level 3 Operation", *IEEE Open Journal of Intelligent Transportation Systems* (submitted - under review).

1.4 Organization and Structure of the Dissertation

The remainder of this dissertation is organized as follows:

A first part (including chapter 2 and chapter 3) serves to present an extended overview of the thesis context, problematics, and challenges. Then, a second part (i.e., chapter 4 and chapter 5) that focuses on introducing our contribution in proposing a new methodology that intends to help tackling the research issues identified in the first part of the manuscript.

More specifically:

- Chapter 2 presents the importance of the localization function in railway control-command and signaling systems (CCS). The European CCS (i.e., ERTMS/ETCS) being considered in the context of this thesis, the existing and investigated solutions to provide safe train localization within ETCS are covered. Accordingly, the challenges facing the possible adoption of satellite positioning systems in the rail context are identified, especially, from a technical perspective. Overall, particular attention is paid to the potential risky behaviors resulting from the uncertainties of GNSS systems in the dynamic railway environment.

- Chapter 3 focuses on investigating the potentially applicable methods to address the GNSS-based train localization. For that, we start by introducing the European regulatory and normative framework for ensuring the safety of railway systems. Then, we intend to highlight the limitations of the existing classical safety methods when dealing with complex, dynamic, and uncertain systems such as the GNSS-based train localization. Finally, we explore the state-of-the-art initiatives that address the adoption of more advanced approaches in order to deal with such complex systems. Along this chapter, numerous research issues related to the safety methods are discussed from a methodological perspective.

- Chapter 4 presents the core of our contribution on proposing a methodology that can help tackling the challenges inherent to the specificities of the GNSS-based train localization. Accordingly, we begin by discussing the features that should be covered in the introduced formal model-based approach. Concretely, we underline that the adopted formal modeling techniques are employed with the aim of providing a modular representation that allows considering the uncertainties related to the use of GNSS systems in the railway environment. In a related context, a set of relevant input parameters are listed and explained in order to allow addressing various scenarios with a reasonable model adaptation effort.

- Finally, chapter 5 focuses on how variant safety and performance properties can be investigated as a part of the introduced formal model-based approach. In this context, the principle of the statistical model-checking (SMC) technique is detailed as this technique will be adopted to investigate a set of illustrative railway scenarios in this contribution. Then a set of case studies are addressed to provide numerical results on some safety and performance properties.

Part I

Preliminary

Chapter 2

Safe train management with satellite positioning: rail context and challenges

Outline of the current chapter

2.1 Chapter Introduction

This chapter presents the railway operational context considered in the research work performed during this thesis. More precisely, this work concentrates on the evolution of the European control-command and signaling system (ERTMS), which is a safety-critical system for managing train movements. ERTMS has been developed for over twenty years and its evolution is today necessary mainly to face the increasing transport demand. Satellite-based navigation solutions are especially envisaged, but are also confronted with **technological and operational issues** on which this work will concentrate.

The current railway context, challenges, and research issues are thus detailed in this chapter as follows. First, Section 2.2 will explain why ERTMS has been introduced in Europe, what are its safety-related functionalities and its main architecture. Next, Section 2.3 will focus on ERTMS operational principles. Section 2.4 will then present the different challenges by highlighting those investigated during this thesis, namely the challenges linked to the train localization enhancement with GNSS. Subsequently, Section 2.5 will detail the existing and envisaged train localization solutions. In this context, the functioning principle of satellite-based navigation is introduced in Section 2.6, and Section 2.7 will address the related safety issues introduced when using GNSS for safety-critical applications.

2.2 Rail control-command and signaling systems: the European context

First and foremost, this section is dedicated to the introduction of the European railway context. A particular focus is put on the safety-related functions of the railway signaling systems. Moreover, the principal motivations leading to the development of a common European signaling system are presented. In particular, the limitations resulting from the use of different national systems are discussed. Finally, the various subsystems forming the European Rail Traffic Management System are briefly presented.

2.2.1 Railway CCS systems and safety

Transportation systems are safety-critical systems whose failures may result in considerable losses. In railway transportation, an accident may involve damage to equipment and environment, severe injury to people, or even the loss of human lives. In railway operation, it is plain that a train driver does not have a global view of the train routes due to the complexity of the rail network, and the need for considering the movement of the other trains in the network. In addition, the high kinematic energy, generated by the imposing weight of the trains together with the high speed at which they can travel, imply long braking distances before a train can safely stop (up to 3km for high-speed trains). As a result, the driver can not detect or react to dangerous situations in a reliable way without relevant indications from external modules. In fact, CCS systems are used to assist the driver and guarantee the safe movement of trains. In this context, multiple safety-related functions are at the core of railway signaling systems (see Fig. 2.1), such as:

- Manage train routes in order to avoid itinerary conflicts and collisions.

- Maintain safe distance separation between trains in order to allow for braking without collisions.
- Ensure that trains do not exceed their permitted speed, dynamically computed according to the infrastructure constraints, in order to avoid train derailment.
- Protect trains from potential driver faults resulting from inattention or misjudgment.

Through these functions, the railway control-command and signaling system provides the driver with the relevant information and warnings to adapt the speed of the train or brake when necessary (Yin et al. 2017).

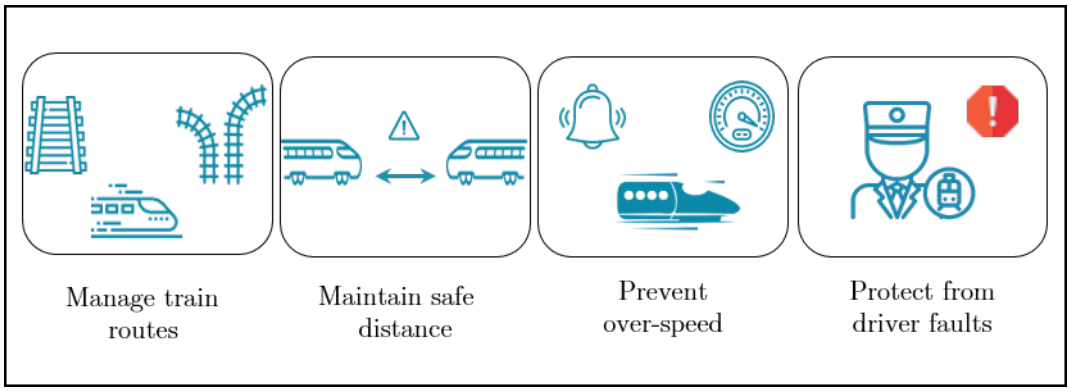


Figure 2.1: Railway signaling systems main safety functions

Besides these main safety-related functions, the signaling systems are also used to ensure some non-safety functions, namely:

- To maximize the line capacity
- To provide information to the on-board passengers and the public at the railway stations.
- To collect diagnostic data for managing defects and providing predictive maintenance.

2.2.2 ERTMS: the European standard CCS system

Historically, multiple European rail CCS systems have been developed on a national basis (European Commission 2016). Unfortunately, these systems are usually not compatible with each other (see Figure 2.2). Thus, a train must be equipped with both leaving and entering area-compatible devices in order to cross a signaling area border. Moreover, the train driver licenses are specific to each European country/CCS and, often, the train driver has to be changed at signaling area borders. As a result, the absence of common technical and operational standards has considerably limited railway interoperability between countries.

With the need to increase international railway services, the European Union backed the initiative of replacing the existing national systems in order to tackle the previous limitations (Almeida Pereira et al. 2021). In this context, the ERTMS (European Rail Traffic Management System) standard was defined. The fundamental objective of ERTMS is to develop and deploy a single harmonized control-command, signaling, and communication system that is fully interoperable across borders. As a result, the main expected advantage is to ensure railway interoperability

in Europe and enhance the competitiveness of the railway sector (Ranjbar and Olsson 2020). Another benefit behind the adoption of ERTMS is the possibility of an incremental and modular introduction of new technologies in the different ERTMS functions.

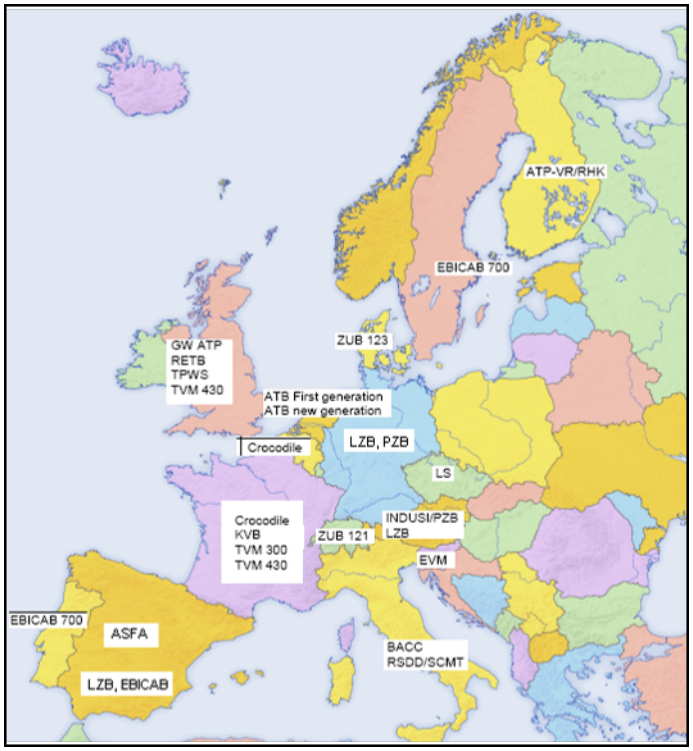


Figure 2.2: Automatic Train Protection System (ATP) throughout Europe

2.2.3 Main ERTMS components

According to the technical specifications, the European Rail Traffic Management System consists of two main components:

1. *GSM-R*: a radio system based on GSM for providing voice and data communications between the track and the train (in level 2 & level 3).

2. *European Train Control System (ETCS)*: an Automatic Train Protection system (ATP) representing the train control-command and protection part of ERTMS.

As shown in Figure 2.3 and based on the different equipment emplacement, the European Train Control System (ETCS) can further be decomposed into two subsystems, namely:

1. ETCS Trackside

2. ETCS On-board

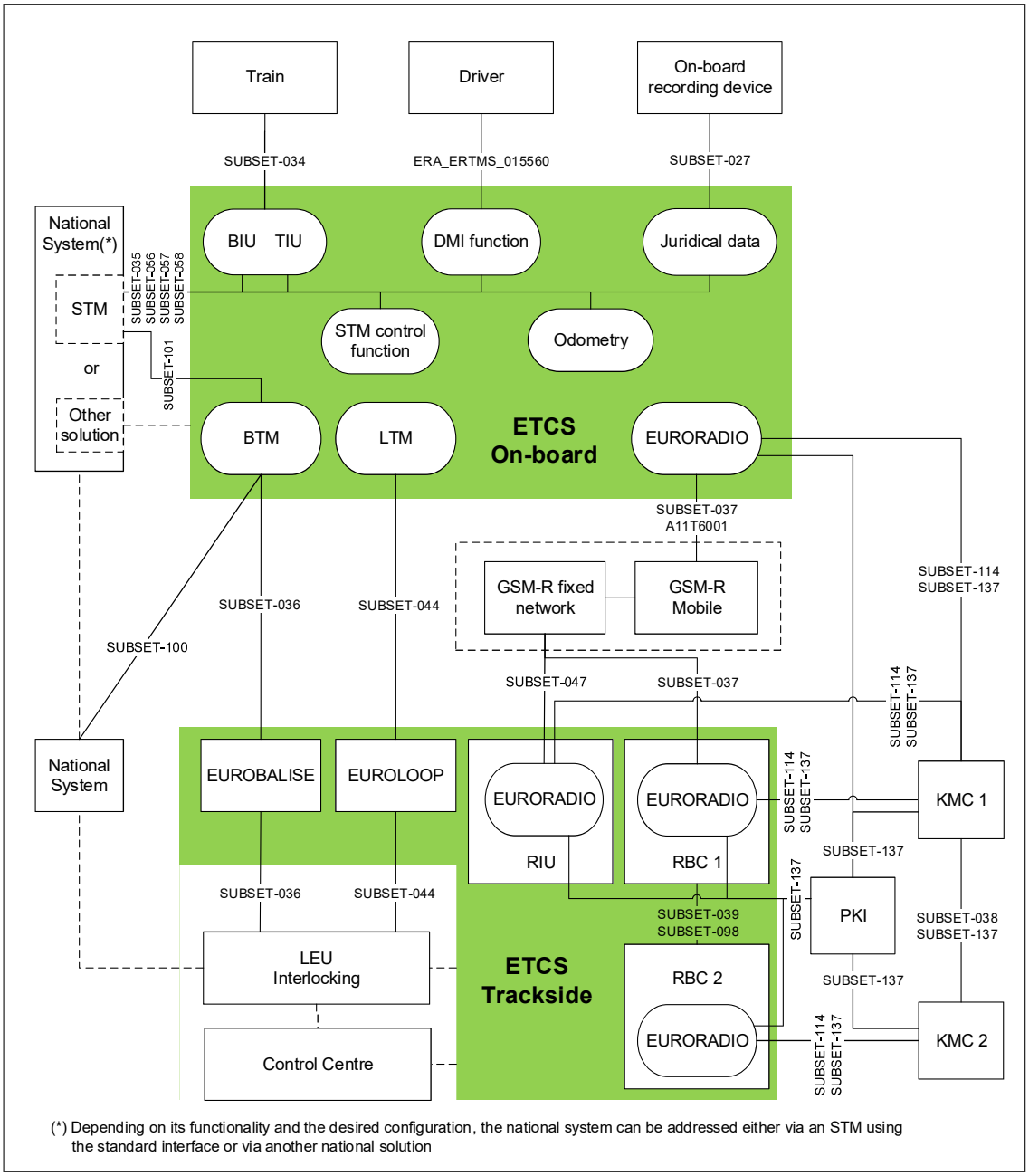


Figure 2.3: ETCS system reference architecture, its interfaces, and their associated specification (subsets)

The principal trackside equipment is the *Radio Block Center (RBC)*. The RBC is a computer-based system installed along the track (usually in a building of a railway station). It uses information received from external trackside systems and exchanged with several on-board subsystems to elaborate the messages sent to the train. These messages provide information required by the train for its movement. In particular, movement authorities (MA) allows the safe movement of trains on the railway infrastructure area under the responsibility of the RBC. A MA is defined as the permission for a train to run to a specific location within the physical constraints of the infrastructure (e.g., speed limitation related to rail line gradient or curve). A RBC can control a railway area of some hundreds of kilometers, while the control of larger areas requires the cooperation between different RBCs.

In parallel, the core module of the ETCS On-board is the *European Vital Computer (EVC)*. This equipment supervises the movement of the train based on the information exchanged with the trackside subsystem. Concretely, on-board EVC of each train uses the MA received from the RBC, in addition to data stored on-board (e.g., the braking capability of the train) to compute the maximum allowed speed (i.e., the braking curve or the dynamic speed profile). If this calculated speed limit is exceeded, the EVC automatically triggers a service or an emergency brake according to the operational circumstances.

Finally, it is important to indicate that different types of equipment (e.g., eurobalises) are included or not in the ETCS subsystems depending on the ERTMS/ETCS application levels (part 2 in Subset 026: 2016).

2.3 Operational principles in ERTMS/ETCS application Levels

According to Subset- 023: 2014, "the different ERTMS/ETCS application levels are a way to express the possible operation relationships between track and train. Level definitions are related to the trackside equipment used, the way the trackside information reaches the on-board units and to which functions are processed in the trackside, and in the on-board equipment, respectively". In particular, the operational principles related to the ERTMS/ETCS application levels (in short: levels) are distinguished and presented in this section.

2.3.1 Fixed block operation

In ETCS Level NTC, 0, 1 and 2, the train separation function (collision avoidance) is based on the division of the line into sections. Normally, no more than one train can occupy each section. To this aim, the generated MA allows a train to move from one block to the next only when the block ahead is clear (except in some specific situations). Since the extremities of the block sections are at fixed locations, this train separation concept is called *(physical) Fixed block*, (see Figure 2.4).

It should be noted that the length of these blocks is determined according to three main parameters, namely:

1. The speed limit of the line.
2. The braking characteristics of the operated trains.
3. The targeted traffic density.

However, to ensure safe railway operations, the the block length is constrained by the most restrictive configuration. As a result, the faster the trains are allowed to run, the longer is the braking distance and, consequently, the longer the blocks must be. Obviously, this directly impacts the line capacity.

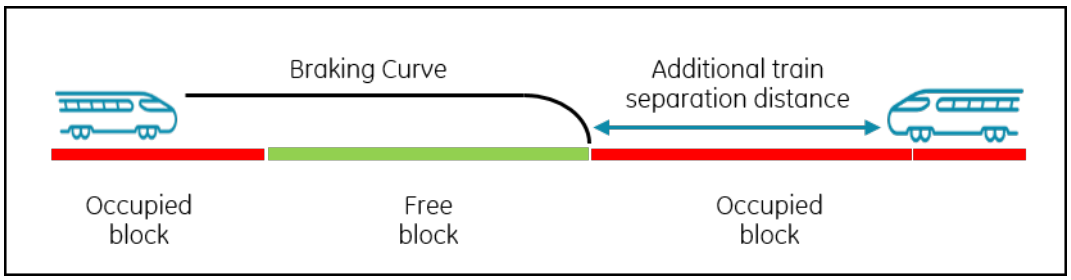


Figure 2.4: Physical fixed Block train separation principle

Moreover, the fixed blocks are delimited by physical trackside equipment such as track circuits or axle counters. Based on the status of these track detectors (free/occupied), the trackside system infers the train location based on the occupancy of the block sections (as will be seen later in Subsection 2.5.2). Yet, the precise position in which the train lies in the block section remains unknown.

In order to tackle these limitations and increase line capacity, the adoption of more flexible operating principles for train separation such as Moving Block are envisaged in the ERTMS/ETCS Level 3. We underline that contrary to the ERTMS Levels 1 and 2, which are currently implemented in several railway lines, Level 3 is only defined today as a concept.

2.3.2 Moving block operation

Full moving blocks:

The ETCS Level 3 application-level relies on the moving block concept. The basic idea underlying this concept is to determine, in real-time, a virtual protection zone around the train position. Therefore, the MA calculated by the trackside system is based on the knowledge of the rear-end position of the preceding train (train ahead). Hence, the MA is issued until the rear of the train ahead (while considering some safety margin) and is then passed to the on-board train computer using the GSM-R radio-communication link (Subset- 023: 2014). As trains move, they regularly communicate their current position to the RBC which, in turn, updates and transmits MAs to the trains in its control area. In such a way, trains can be continuously controlled and kept at a minimum safe distance from each other. As a result, the time interval separating trains can be considerably reduced, hence improving the line capacity.

Following this operational paradigm, unlike in the fixed block operation, the End of Authority (EoA) can be in any place of the railway line. In fact, this above described operational concept is referred to as the *"Full Moving Block" (FMB)* principle.

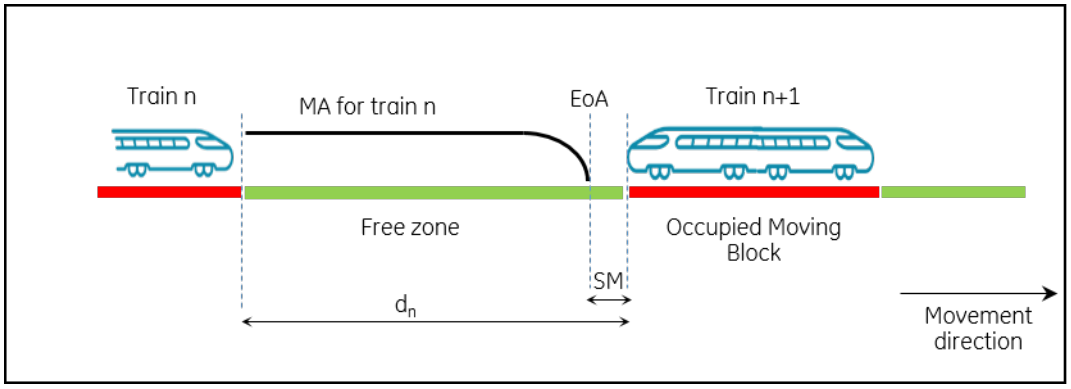


Figure 2.5: Full Moving Block train separation principle

For the implementation of the FMB system, three distinct mechanisms are considered, as summarized below (Y. Zhou and Mi 2012). Namely, *Moving Space Block*, *Moving Time Block*, and *Pure Moving Block*.

In each case, d_n is the minimum instantaneous distance between the head of train n and the rear of train $n+1$. This distance corresponds to the braking distance needed by train n to decelerate from the speed v_n to 0, with a deceleration coefficient b_n. We also denote by v_{max} the maximum velocity of train n (with respect to the maximum line speed) and SM the safety margin between trains n and $n+1$. In reality, the train position information is associated with nominal errors linked to the estimation process. That is why a safety margin is considered and is calculated according to the confidence interval provided with the estimation process. Finally, the time interval needed by train n for running distance d_n is called *headway*, (see Figure 2.5).

Using the aforementioned notations, the FMB implementation mechanisms can be defined as follows:

1. *Moving Space Block*: is the implementation scheme in which the minimum instantaneous distance is adjusted according to the maximal line speed v_{max} (cf. Equation 2.1). Thus, d_n keeps constant (as v_{max} is unchanged) and follows the displacement of train n at $v_n \leq v_{max}$.

$$d_n = \frac{v_{max}^2}{2b_n} + SM \tag{2.1}$$

2. *Moving Time Block*: implies that the headway time between two trains passing any point along the line is constant (cf. Equation 2.2) where $\frac{d_{max}}{v_{max}}$ is the headway time and v_f is the current speed of train n.

$$d_n = v_f . \frac{d_{max}}{v_{max}} + SM \tag{2.2}$$

   where d_{max} is the braking distance when train decelerates from v_{max} to 0 at the deceleration rate of b_n

3. *Pure Moving Block*: allows the adjustment of the minimum instantaneous distance according to the current speed v_f of train n (cf. Equation 2.3).

$$d_n = \frac{v_f^2}{2b_n} + SM \tag{2.3}$$

In the light of the above discussed mechanisms, one can conclude that the *Pure Moving Block* implementation mechanism gives the best performances, as the train separation distance is optimal (minimal) in this case, allowing for the most promising operational approach in terms of line capacity. However, since the FMB concept constitutes a breakthrough in terms of operation, it raises many issues to railway stakeholders in terms of specification and development, which slows down the penetration of MB systems in railway operation. As an alternative to FMB, *Fixed Virtual Block (FVB)* that will be discussed in what follows, brings an interesting trade-off solution between the use of classic fixed blocks and FMB.

Fixed Virtual Block:

Contrary to the FMB, where a dynamic area around trains is established, FVB operation is based on the establishment of fixed virtual blocks (similarly to classical fixed blocks). However, these FVB limits are not associated with trackside equipment but are defined through information stored in digital databases. Such an approach leads to a logical (rather than a physical) division of the line into sections of known lengths. Accordingly, depending on traffic demands, the operational performance may be flexibly changed by reconfiguring the VB length (Pachl 2020), i.e., their size could be reduced in order to separate trains with a smaller distance. Hence, FVB enables to easily and finely discretize the railway line into smaller block sections compared to the fixed physical blocks without requiring to install additional trackside equipment. Besides, the number of FVB can be increased without the need for additional equipment. As a result, FVB allows for reducing the train separation distance while keeping the same logic as in the fixed block operation. Namely, the train EoA can only be placed at discrete locations on the line predefined by the FVB limits (similarly to the classical fixed blocks).

A common feature for FMB and FVB is that track occupancy determination is based on the knowledge of the actual train location, and that such information are sent by train-to-ground communication link. However, track occupancy is determined differently under the two operational contexts (Furness et al. 2017). Concretely, on the one hand, occupied track sections are only determined by the train rear and train head positions in the FMB. On the other hand, FVB defines the occupied track sections according to occupied block sections (as shown in Figure 2.6 and Figure 2.7).

Figure 2.6: Track occupancy determination following the FMB principle.

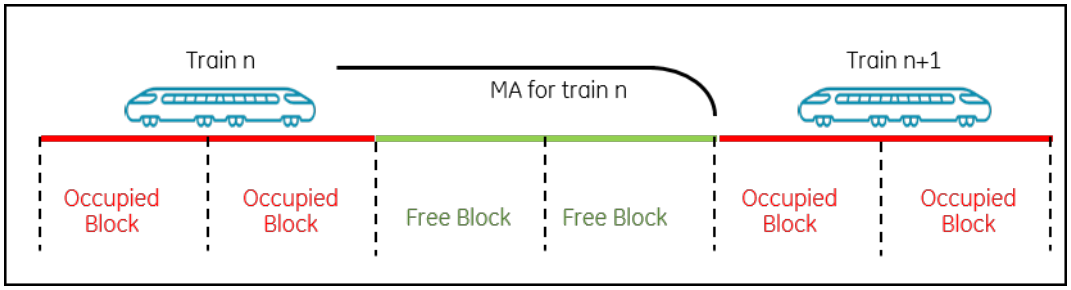


Figure 2.7: Track occupancy determination following the FVB principle.

Furthermore, it should be noted that, nowadays, MB operation is investigated with the intent to allow the use of a mixture of different systems at the same time. In other words, the ETCS-L3 system can act as an overlay over existing conventional system. This approach enables for a smooth transition for lines on which a migration towards ETCS-L3 is foreseen. During this transition phase, mixed traffic is possible with trains operating under the MB system while other trains can be operated under the classical fixed block sections on the same line. Consequently, non-equipped trains can be gradually equipped or replaced with equipped ones.

Besides, we should also mention that, under MB operation, on-board devices are adopted to monitor the train integrity. Likewise, the on-board sub-system is responsible for correctly supervising the speed and the braking curve. Yet, the remaining crucial information required to ensure a safe headway is regarding the precise positioning information of trains. In the remainder of this chapter, the most relevant train localization solutions will be presented.

In conclusion, in this section, we presented the different operational principles of ERTMS used according to the different ETCS levels. An underlying idea behind defining various ETCS levels is to progressively transfer the functionalities performed by trackside equipment to on-board train equipment. In fact, the possibilities offered by the new technologies allow the integration of autonomous functionalities on board (see Section 2.5). These technologies make it possible not only to implement the operational principles related to ETCS level 3, but also to improve the operational performances. However, the development of ETCS-L3 and, in general, the evolution of ERTMS to optimize the capacity of the railway infrastructure is still facing several challenges, as discussed hereafter.

2.4 Challenges for ERTMS evolution

Technological innovations allow for on-board implementation of different features linked to moving blocks while offering, at the same time, enhanced performances for railway operation. The main embedded features are:

- Train integrity monitoring (continuous monitoring of the completeness of the train),
- Train localization,
- Train communication with radio control centers and with traffic management actors.

These technological innovations allow for envisaging an even more advantageous operational possibility: the train virtual-coupling, i.e., trains which move synchronously in platoons thanks to a vehicle-to-vehicle radio link. Nevertheless, the ERTMS evolution toward moving block and virtual coupling operations encounter the following challenges (Ranjbar and Olsson 2020) addressed in national research programs (e.g., "Digital Schiene" in Germany, "SmartRail4.0" in Switzerland, "Tech4Rail" in France) and European research programs (cf. the "Multi-annual action plan" of Shift2Rail [1]):

1) Which intelligent equipment needs to be designed for railway operations?
To realize cost savings and improve operational performances, a number of technological means can be employed:

- adaptable communication systems for train/trackside message exchanges (GSM-R is obsolete) or for train integrity monitoring,
- GNSS-based positioning for train localization,
- digital maps for track description.

However, a main challenge that faces the deployment of such new technologies is pertaining to the specification of safety requirements regarding the functionalities fulfilled by such new technologies.

2) How to analyze the cybersecurity of intelligent equipment used in railway operations?
Cyber-physical systems rely on interactions between distributed, connected, computational and physical components. Thus, such systems are vulnerable to cyber-attacks, and their cybersecurity needs to be analyzed. Such issues are particularly relevant in the case of ETCS-L3 operation which highly relies on distributed architectures, digital means and wireless communication.

3) How to analyze the safety of railway operations?
New safety approaches need to be proposed in order to tackle the difficulties in identifying and analyzing all the possible hazards and causal scenarios resulting from the increasing connectivity and complexity of such innovative systems (Rangra et al. 2018).
In particular, the complexity of the system can be even higher due to the potential mixed train operations, the increasing number of components employed, and the multiple interactions especially encountered when the trains are operated in complex track configurations.

One can find several formal tools and languages in the literature. While some of those tools deal with the formal modeling task envisaged for analyzing and validating complex behaviors, no emerging formal methods are today dedicated explicitly to the needs of the railway. As a result, there is still a need to certify compliance with safety requirements.

4) How to validate railway operations with mobile and intelligent systems?
Especially as the increasing connectivity and complexity of the system hinder the modeling and testing tasks that aim to validate the functionality, the performance and the safety of railway operations.

[1] www.rail-research.europa.eu/publications/multi-annual-action-plan/

These challenges are intensively addressed in the European projects managed by the Shift2Rail Joint Undertaking, which coordinates and manages the rail research and innovation investments of the H2020 program. The evolution of ERTMS is particularly addressed in X2Rail-1 to 5, as well as in MOVINGRAIL, ASTRAIL and PERFORMINGRAIL projects.

In the context of this thesis, our contribution is mainly focused on points 1 and 3. With regard to the first point, our work does not address the related technological developments, but rather focuses on what the use (from the user's point of view) of satellite positioning (with GNSS) implies for train operations, especially in terms of safety. On the other hand, the thesis work contributes more specifically to topic 3, for which the current and emerging approaches and techniques in terms of safety will be detailed in a dedicated chapter (see Chapter 3).

In order to highlight how the localization function is specifically involved under ERTMS operation, Section 2.5 describes the operational aspects related to train localization and track occupancy determination.

In particular, this section will address the **existing** trackside/on-board operational points of view regarding block occupancy and train position, the possible (relative and absolute) positioning methods, in addition to the employed equipment (beacons, odometer, axle counters, track circuits)

2.5 Existing Train Localization solutions

This section is dedicated to the description of the main positioning methods used in railway operation. brief definitions of the necessary terminology and basic positioning-related concepts are firstly provided. Then, the train detection and positioning systems that are currently used are reviewed. Finally, the discussion on the limitations of the current solutions paves the way to introducing alternative GNSS-based systems that are envisaged to overcome the current system limitations.

2.5.1 Introduction to Positioning Terminology

In this subsection, we briefly introduce the main position determination related concepts, namely: Localization, Positioning, and Navigation. In addition, the associated accuracy, precision, uncertainty, and error parameters are shortly presented.

The Localization, Positioning and Navigation concepts

Train Localization consists in the determination of the geographical movement state of a train (i.e., location, speed and direction according to a reference point) in a spatial reference system (Hofmann-Wellenhof, Legat, and Wieser 2003).

In this dissertation, *'Train localization'* is employed for train position calculated in a track-based coordinate system and is considered equivalent to the *'train positioning'* notion.

On the other hand, *'Train location'* refers to the track occupancy as seen by the trackside system (i.e., free/occupied block).

Navigation can be defined as a means for estimating the location, course, and distance traveled by a mobile (Merriam-Webster 2022). The*Navigation* encompasses the localization of the mobile and its guidance from a starting point location to a destination.

According to the previous definitions, it can be concluded that localization is only part of the navigation purposes. However, in the applications addressed in this thesis, the train control systems already define the operating train routes. Therefore, we are particularly interested in the localization and not in the navigation.

Metrology-related terminology (Accuracy, precision, uncertainty, positioning error)

regarding railway positioning, the actual value of train position cannot be determined in real-time, and the measured values are subject to errors. Therefore, metrology-related notions such as uncertainty and confidence interval are associated with the estimated train position. In the context of this thesis, we should make it explicit the difference between the following parameters (Bell 2001).

1. The term *'positioning error'* indicates the difference (i.e., deviation) between the measured position and the *'actual position'* of the train, where, actual position (or 'true value') is the value that a perfect measurement would obtain.

    - The component of the total measurement error, which varies in an unpredictable way, is called random error.

- The component that tends to shift all measurements in a systematic predictable way is referred to as systematic error.

2. The term *'uncertainty'* is used as a quantification of the doubt about the train position measurement. Therefore, known systematic errors result in offsets that can be corrected. On the other hand, any error whose value is unknown is a source of uncertainty.

3. The *'precision'* is a measure of how close independent results are to one another when the same measurement is made repeatedly, and does not require knowing the actual position.

4. The term *'accuracy'* is used to indicate the closeness between the measurement of the train position and its actual position.

In particular, the difference between the *precision* and the *accuracy* notions is illustrated in Figure 2.8 (inspired from PR NF ISO 5725-1: 2022).

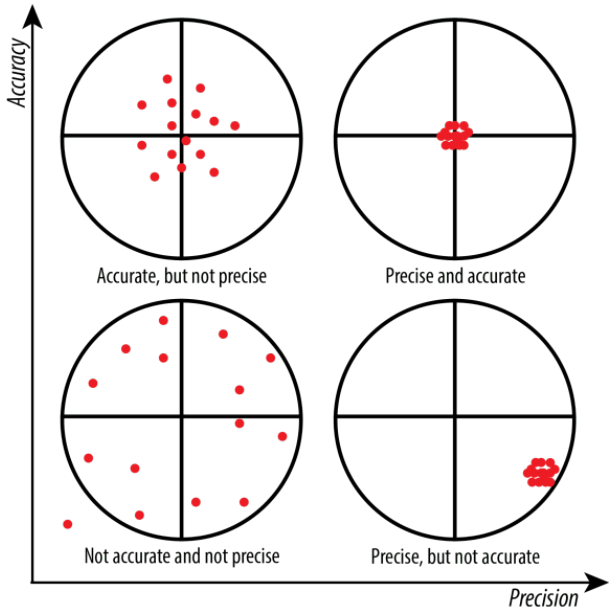


Figure 2.8: Accuracy vs Precision (inspired from PR NF ISO 5725-1:2022)

Relative vs Absolute position

In fact, the positioning (position determination) is a process the result of which is a position. This position can be determined with respect to a coordinate system (usually geocentric), relatively to another point, or within the context of several points (Wells et al. 1986). Hence, two modes of positioning systems can be distinguished; namely: absolute point positioning and relative positioning (Hofmann-Wellenhof, Legat, and Wieser 2003).

1. Relative positioning is the determination of the position of one point with respect to a fixed reference point in the environment (e.g., a railway balise).

2. Absolute positioning is the determination of the coordinates of a point with respect to a coordinate system.

The type of collected observations and the kind of the desired coordinates dictate whether the mathematical model of position should be formulated in a one-dimensional, two-dimensional, or three-dimensional space. Thus, the dimension defines whether a system provides one-, two-, or three-dimensional positioning (Vanicek and Krakiwsky 2015).

Proprioceptive vs Exteroceptive sensors

Depending on the required type of positioning, two types of sensors are used to provide a relative or absolute position:

1. Proprioceptive sensors determine information from their local perception of the vehicle's movement. These sensors have satisfying short-term accuracy but suffer from a cumulative bias over time. Such a bias increases if no readjustment is performed.

2. Exteroceptive sensors measure the absolute position of a vehicle according to a fixed point in the environment whose coordinates in a given coordinate system are known. These sensors are commonly used to correct the bias of the relative measurements.

In general, both types of sensors are combined for their complementarity. In particular, the most common sensors and localization solutions used in the railway domain are presented in the remainder of this section.

2.5.2 Track occupancy detection

Train detection is a trackside function that aims to determine, whether a track section (block) is occupied by a train. This function is fundamental to the safe operation and usage of trains. To this aim, train detection systems are used to detect either the presence or absence of trains within a block section. Most of the train detection units automatically perform such detection by means of track circuits or axle counters.

Track Circuits

The mechanism of Track Circuits systems is based on the use of insulated sections of the rails as an electrical circuit. In its simplest form, the transmitter is a voltage generator and the detector is an electromechanical relay.

The transmitter is responsible for injecting a low-voltage current into the system. This current is passed through the tracks in order to energize the receiver at the other end of the circuit.

When the block section is not occupied by any train, the relay is energized and keeps the signal at proceed aspect (green), as shown in Figure 2.9.

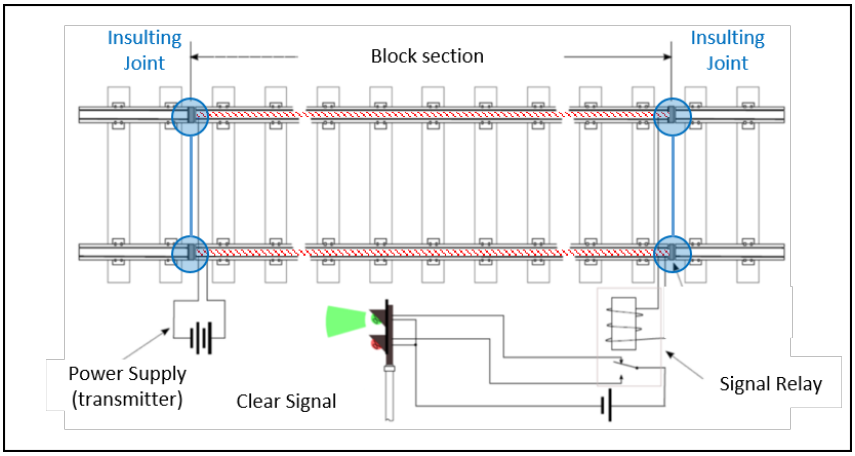


Figure 2.9: Free track circuit

As soon as a train enters the section, the leading axle of this train enters the circuit and establishes a low-resistance connection (short-circuit) between the rails. Consequently, no more current reaches the receiver and the relay is de-energized. As a result, the signal is switched to show the stop aspect (red), as shown in Figure 2.10.

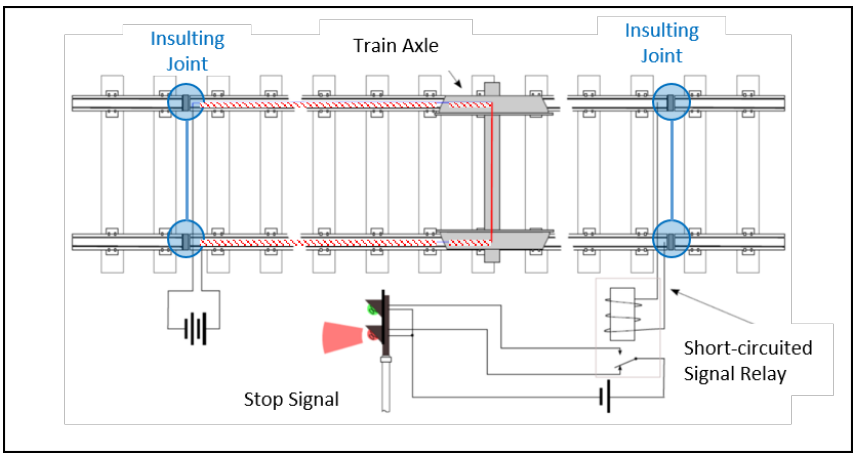


Figure 2.10: Occupied track circuit

The status of each track circuit is periodically acquired via a wired communication and processed by safe equipment (e.g., interlocking) installed in specific locations along the railway line.

It is worth noting here that the track circuit functioning perfectly illustrates the key "Fail-Safe" principle applied in railway signaling systems. Concretely, the presence of closed track circuits, the occurrence of a power breakdown, or any break in the circuit between the transmitter and the receiver have the same functional effect as the presence of a train in the section. Hence, the signals indicate the corresponding block section as occupied, and the system *fails-to-a-safe* state.

However, the track circuit can fail to detect a train due to the lack of good electrical contact

between the rails and the train wheels. Such failure can be caused typically by falling leaves during the autumn season. Hence, an occupied section may not be reported timely. Moreover, the high initial investment required to install track circuits, and their related maintenance costs represent a main disadvantage of these systems. Therefore, some railways replace track circuits with axle counter systems (Kozol and Thurston 2010).

Axle Counters

Axle counter systems represent an alternative to track circuits. Similar information to the track circuit about the occupation status of a specific track section can be provided. Their operating principle is simply based on counting the number of train axles entering and leaving a section of track. Therefore, the counting points detect trains in and out by counting the number of train axles at both ends of a block (Durazo-Cardenas et al. 2014). The track section is considered as occupied as soon as the first axle of a train enters that track. If the number of axles counted at the entrance of that block section is equal to the one counted at the exit, the block section is considered cleared by the train. Otherwise, the track section remains occupied (H. Hamid, Nicholson, and Roberts 2018).

Concretely, the axle counter unit is composed of two elements. Namely, a detector and an evaluator. Detectors are counting points installed on both ends of the track section. Each detector uses a pair of sensors to detect the passing axles and determine whether an axle is entering or exiting the track section. On the other hand, the evaluator is responsible for storing the number of axles in the section. Concretely, the count increases upon the detection of an entering axle, while each detection of a leaving axle decreases the count (Jiang 2011). Consequently, a zero count value indicates that the track section is clear, while any higher value of the count implies that the track section is occupied.

The overall functioning of axle counters is shown in Figure 2.11.

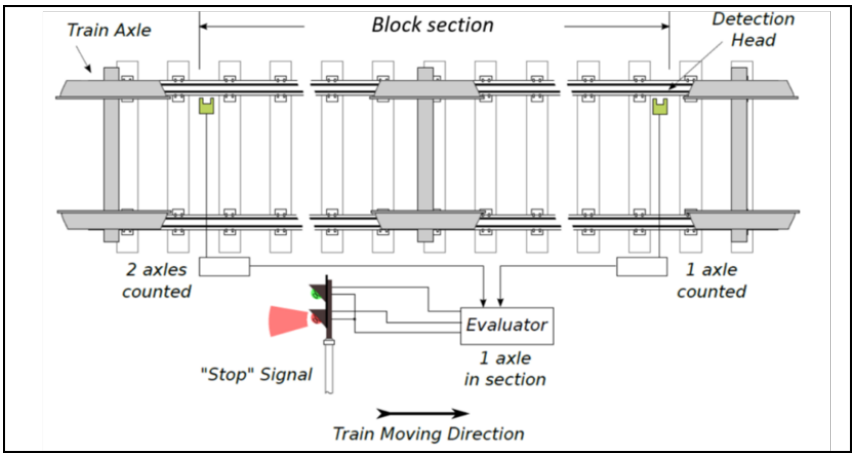


Figure 2.11: Axle Counters System principle (Hassan Abdulsalam Hamid 2020)

Compared with track circuits, the main advantages of axle counters are related to the simpler maintenance and no need to install equipment along the line. Concretely, no bonding and less cabling are required to operate axle counter units.

However, axle counters encounter some problems in maintaining a correct count of the

number of axles in a section for various reasons, such as power failure. In that case, a manual override is required to reset the system. An additional limitation of axle counters is related to the difficulty of detection when the wheels stop precisely on the counter mechanism. This limitation is particularly problematic at stations and areas where train coaches/wagons are shunted, joined, and divided. Finally, axle counter systems do not provide broken rail protection and present a lack of fail-safe modes.

From an operation point of view, both the track circuits and axle counters allow for determining if a particular section (block) of the track is occupied. Yet, the precise position of the train in the section cannot be determined. Being given that the track blocks are typically long (2-3 km), this limitation significantly decreases the line capacity.

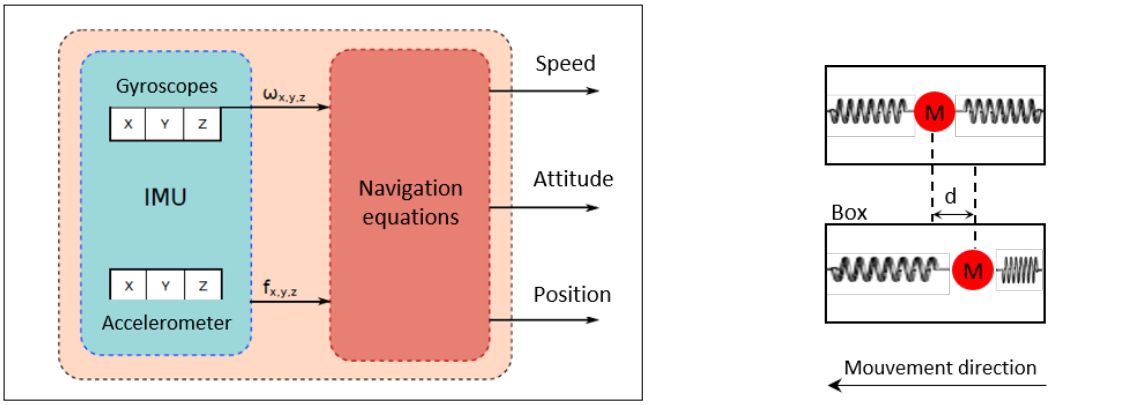
In order to tackle the aforementioned issue, complementary (relative and absolute) train positioning solutions, such as inertial sensors and odometers, are adopted. These solutions are discussed in the following subsection.

2.5.3 Methods for train positioning: Relative vs Absolute solutions

The position of a moving train can be obtained through a wide range of positioning methods. For instance, relative positioning solutions, such as Inertial Sensors and Odometers, are on-board sensors used to estimate the train position relatively to a reference position, which is geo-located on the track, and used as a local referential origin. On the other hand, *balises* constitute widely used trackside equipment in railway infrastructures, and particularly in the context of ERTMS/ETCS as absolute train positioning solutions. The working principles of these positioning solutions are presented hereafter.

Inertial Sensors relative positioning solutions

Inertial systems are devices that combine the use of gyroscopes and accelerometers to measure an angular position and an acceleration (see Figure 2.12a). Concretely, a gyroscope provides the angular velocity and the variation in the attitude angles, while accelerometers (which are mass-spring systems) directly deduce the acceleration from the force applied to the mass and measured by the spring deformation. Besides, a calculator is responsible for determining both the velocity and the attitude angles (Hirwa 2013).



(a) Inertial Navigation System

(b) Basic Accelerometer principle

Figure 2.12: Inertial Measurement Units (IMU)

Focusing on the acceleration deduction, Figure 2.12b shows the structure of a simple accelerometer. Namely, whenever an acceleration occurs, the mass (M) held by the spring moves. The resulting displacement (d) is then measured and transformed into an electrical signal to calculate the acceleration. In fact, the box is fixed to the vehicle so that the measured acceleration corresponds to the vehicle acceleration.

Finally, it should be noted that for a three-dimensional navigation solution in (x,y,z) reference system, a pair of gyroscope/accelerometer per axis is used (i.e., three gyroscopes/accelerometers). In practice, the usage of such inertial sensors in the railway field remains relatively limited compared to the more commonly deployed odometer-based systems.

Odometers

Odometry is the process of measuring the train's movement along the track (Subset- 023: 2014). In the ERTMS Level 2, on-board odometry sensors are conventionally used for speed and distance measurement. This technique enables the estimation of the traveled distance by a train from a reference point. In practice, the distance is extrapolated by integrating the speed measured over time by the odometer. Concretely, the operating principle relies on velocity data that often come from angular speed sensors located on locomotive wheels. The traveling speed can thus be deduced easily, knowing the circumference of the wheel.

$$Traveled\ Distance = Wheel\ Rotations\ Number \times Wheel\ Circumference$$

with:

$$Wheel\ Circumference = Wheel\ Diameter \times \pi$$

Therefore, the performance of odometers depends on the accuracy of the measured speed and the clock that controls their operation. Moreover, the accuracy of such a device depends on the intrinsic characteristics of the sensor. In practice, the resulting inaccuracies can be estimated by the on-board localization system, which provides a confidence interval associated with the measured parameters.

As defined in (Subset 035: 2015), the provided odometer information includes the current values of:

1. Train Direction
2. Estimated train running speed
3. Estimated traveled distance since the last reference position
4. Confidence interval associated with the speed measurement
5. Confidence interval associated with the distance measurement
6. Information on timestamps when the odometer data are valid

Furthermore, the distances measured by odometers can be affected by several external error sources, such as shape irregularities in the wheel geometry (e.g., out-of-roundness, wear, and diameter) and unevenness in the rail track.

Moreover, odometer systems are also susceptible to unpredictable environmental conditions (i.e., bad adhesion conditions between the wheel and the rail). In particular, such conditions can generate wheel slipping (especially during acceleration phases) or wheel blocking (especially during braking phases). In general, the resulting measurement errors increase progressively with the travelled distance, as they accumulate in time (as long as they are not reset). Consequently, the uncertainty on the estimated position increases (cf. Figure 2.13). It should be noted that in the ERTMS control-command and signaling system specifications (Subset 041: 2015), the tolerated position error of the odometry is bounded by the confidence interval $\pm(5 + 5\%.d)$, with d being the measured distance since the last reference point.

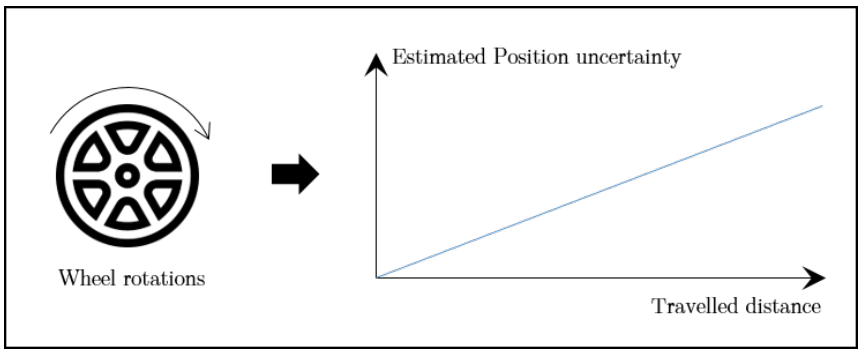


Figure 2.13: Error accumulation of the odometer

In order to tackle the aforementioned weaknesses and comply with the ERTMS requirements, the error accumulated by the odometer is regularly reset utilizing geo-referenced track equipment, namely *Eurobalises* (see the following subsection). Thus, the on-board odometer and the eurobalises set along the track are combined to localize the train: relative positioning by the odometry device and absolute positioning by balises (addressed in the following subsection)

Train absolute positioning using balises

With the aim of providing absolute train positions and correcting the error accumulated by the odometer on the estimated position, Physical Balises (PB) are positioned on the track, at suitable intervals and around critical positions such as junctions and entrance of stations. These

geo-referenced balises are passive components as they can only be energized/activated using the energy supplied by some antenna devices installed at the bottom of the trains. In fact, the train continuously emits an electromagnetic signal while running in order to activate any encountered balise.

The function of a balise is mainly to send information to the on-board module. The information to be sent can be either:

- Fixed pre-stored information. The balises that hold only fixed information are called *fixed balises*,
- Dynamically changing information based on the inputs received by the balise (i.e., such balise is named switchable balise).

In practice, various types of balises can be encountered depending on the signaling system they belong to (e.g., KVB balise, ERTMS balise).

Figure 2.14: Physical Balises (PB) and Balise Groupe (BG)

Under ETCS operation, the fixed balises are commonly used as a reference point for relative positioning solutions. Concretely, each fixed balise contains information regarding its exact position. Once activated, the balise sends a telegram containing information on its position along the track to the train on-board module. This telegram is received and interpreted by a computer on-board the train. Therefore, the train is able to determine its exact position every time a PB is encountered. Such a position is then used as a new reference for the train localization, hence, resetting the odometer accumulated errors.

In reality, balises are often used in groups called Balise Groups (BG), as shown in Figure 2.14. Each BG comprises two to eight balises placed one behind the other on a few meters track zone and characterized with an internal sequence number. When grouped, the position of the first balise (i.e., balise number 1) is the origin of the balise group coordinate system and defines the location reference of the BG (Pachl 2020; Presti and Sabina 2018). Such configuration has several purposes, namely:

1. to ensure a safe redundancy of the transmitted information
2. to detect the direction of a train (nominal or reverse)
3. to send large messages in several concatenated balise telegrams when needed

With the perspective of implementing the ETCS Level 3 Moving Block concept (introduced in Subsection 2.3.2), the trains should be able to estimate their positions with more autonomy. This aims to reduce the number of physical equipment installed along railway tracks as they generate substantial installation and maintenance costs (Pachl 2020). In this context, the replacement of the physical balises by virtual entities called Virtual Balises (VB) is investigated (Ciaffi et al. 2019; Wullems et al. 2018; Filip, Sabina, and Rispoli 2018; Filip, Rispoli, and Capua 2020). The underlying idea behind using VB is to emulate the behavior produced by physical balises without resorting to physical devices. Concretely, Virtual balises are geo-referenced points recorded in a database embedded in the train computer. In such implementation, on-board embedded positioning systems (e.g., GNSS receivers) will be used to estimate the train position and activate the virtual balises when needed. In such a way, the GNSS receiver allows the implementation of the VB concept, which is functionally equivalent to the physical one (or to a balise group) (Presti and Sabina 2018). More details on the VB activation mechanism can be found in chapter 4 while the following section is dedicated to the introduction of the GNSS systems.

2.6 Global Navigation Satellite System (GNSS)

In this section, the Global Navigation Satellite System (GNSS) is addressed. First, the different existing satellite constellations are introduced in Subsection 2.6.1. Then, Subsection 2.6.2 is dedicated to the presentation of the different GNSS segments. In particular, insight on the GNSS position calculation is provided in Subsection 2.6.3. Accordingly, the augmentation systems associated with the use of GNSS systems are finally discussed in Subsection 2.6.4.

2.6.1 Introduction of GNSS and the existing constellations

GNSS is a comprehensive term that refers to Global Navigation Satellite System. If the GPS system is certainly the most famous satellite-based localization systems, it is nevertheless not the only existing GNSS system. In fact, the GNSS concept encompasses four distinct systems (see Figure 2.15). Namely, the American GPS, the Russian GLONASS, the European GALILEO, and finally the Chinese BeiDou.

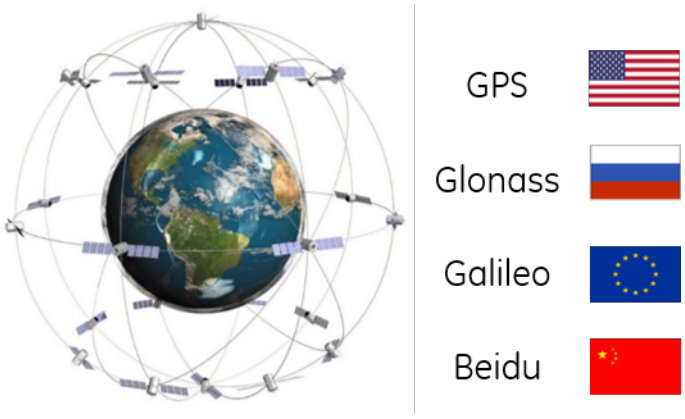


Figure 2.15: The currently existing GNSS constellations.

Each of the aforementioned systems employs a number of orbital satellites, called constella-

- **Global Positioning System (GPS):** The baseline GPS constellation holds 24 Medium Earth Orbit (MEO) satellites disposed in six Earth-centered orbital planes. Each plane hosts four satellites and has a radius of 26,560 km (i.e., about 20,163 km above the Earth).

- **GLONASS (Global'naya Navigatsionnaya Sputnikovaya Sistema):** The GLONASS in its nominal constellation comprises 24 active MEO satellites (21 active satellites + 3 active spares) in three orbital planes separated by 120 degrees. The satellites operate in circular 19,100-km-orbits at an inclination of 64.8 degrees to the Earth's surface.

- **GALILEO:** The Galileo constellation consists of 30 MEO satellites (27 operational satellites + 3 active spares) divided within three operational orbital planes and at an altitude of 23,616 km above the Earth's surface.

- **BeiDou navigation satellite system (BDS):** The design for the BeiDou-2 system consists of a constellation of 27 MEO satellites. The MEO satellites are equally split into six orbital planes at an altitude of about 21,500 km above the Earth's surface.

From a historical perspective, each of the previous constellations has been developed independently, as presented in Annex B. However, these systems summarized as GNSS share the same system structure, which is presented in the following subsection.

In the context of ETCS Level 3, the use of the European GALILEO system is particularly investigated.

2.6.2 Presentation of GNSS segments

The four GNSS systems (i.e., GPS, GLONASS, GALILEO, and BeiDou) are composed of three distinct segments. Namely, space, control, and user segment, as shown in Figure 2.16 (Jeffrey 2010).

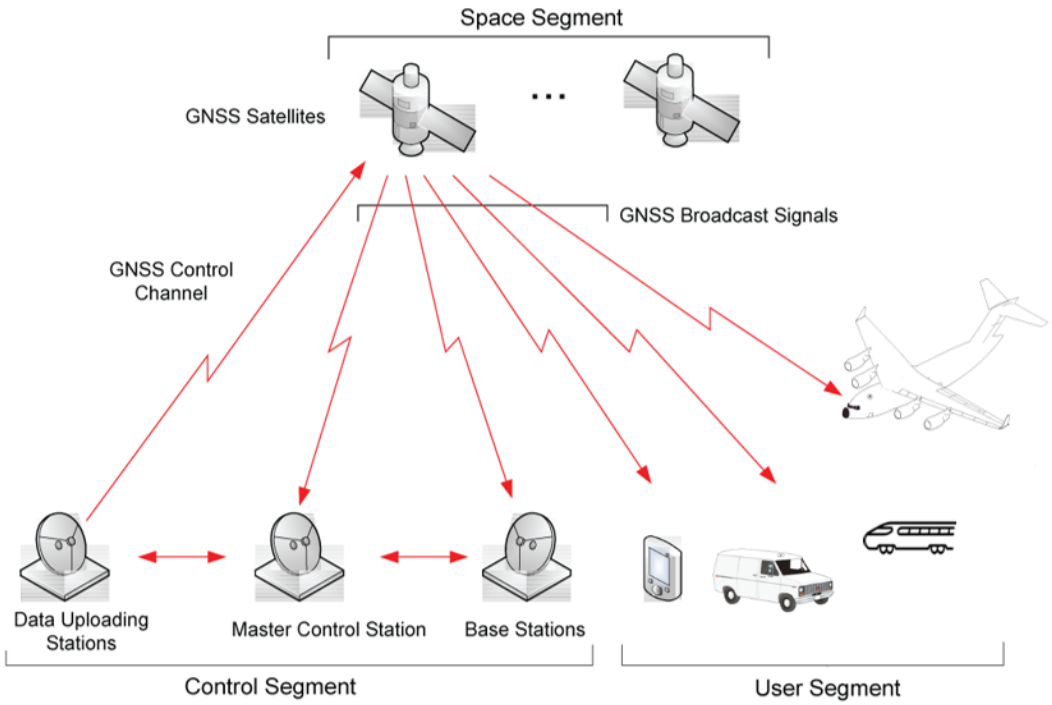


Figure 2.16: The GNSS Segments

1. The space segment (satellite constellation) is the set of satellites in orbit that provide the ranging signals and data messages to the receiver equipment. In each satellite constellation, the GNSS receiver is expected to have a sufficient number of satellites in view from any point of the earth (e.g., at least 6 in the case of GPS).

2. The user segment includes all the user reception equipment. These receiver equipment are capable of simultaneously processing the signals from a minimum of four satellites in order to obtain location, velocity, and timing measurements. As a result, the user positioning function can be performed.

It should be noted that the user segment receives signals from the satellites only, while the space segment and control segment communicates with each other bidirectionally. Finally, these three segments operate in conjunction to permit a relatively accurate three-dimensional position calculation, as explained in the following subsection.

2.6.3 GNSS position calculation principle

Basically, the GNSS-based localization approach relies on signals propagation time measurement to determine the receiver position. This method consists in measuring the time it takes for a signal transmitted by an emitter (i.e., satellite) at a known location to reach the user receiver. Concretely, each of the constellations satellite broadcasts a continuous coded signal. These codes are different for every satellite. Hence, the receiver is able to distinguish the received messages and identify the identity of the transmitter. The GNSS receiver simultaneously processes all

the signals reaching its antenna and estimates the time of arrival (TOA) of each of these signals. These signal propagation times are then multiplied by the speed of the signal (i.e., the speed of light for GNSS) to obtain the emitter-to-receiver distances, called pseudo-ranges (Kaplan and Hegarty 2017).

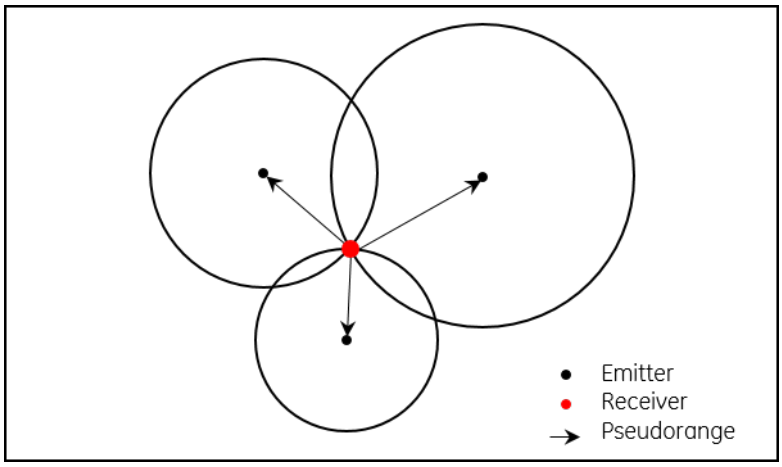


Figure 2.17: Trilatiration principle (2D) used in GNSS position calculation.

Based on these pseudo-ranges, the receiver position is calculated based on the trilateration concept. Figure 2.17 illustrates the use of trilateration to determine of a 2D position based on three pseudo-ranges values. Using the same principle, one can conclude that four satellites are needed in order to compute a 3D position. However, assuming that the user position is restricted to the earth's surface, the radius of the earth can be used as complementary information. Consequently, three satellites are theoretically sufficient to calculate a 3D position. Yet, the satellites have atomic clocks which can be synchronized to the level of nanoseconds. However, as the atomic clocks are very expensive (i.e., more than $100,000 each), the clocks used in GNSS receivers are less accurate. Thus, a fourth satellite is necessary to mitigate the time synchronization errors.

Overall, the reception of n (at least four) satellites will allow the receiver to benefit of n observations to solve the system of n equations, where the unknowns are $(x, y, z, \delta t)$; with (x, y, z) representing the receiver position and (δt) is the offset between the user and the satellite clocks. This offset is the result of the non-synchronization between the satellite and receiver clocks (Presti and Sabina 2018).

Finally, it is worth noticing that GNSS positioning accuracy is strongly related to the satellite distribution around the reception antenna. Indeed, the straighter the path of the signal between the sender and the receiver is, the more accurate will be the satellite-receiver distance estimation. Furthermore, atmospheric effects (i.e., ionospheric and tropospheric) do perturb the signal propagation time and result in additional measurement errors. Therefore, complementary means, such as augmentation systems addressed in the following subsection, are needed to provide corrections and improve the positioning performances.

2.6.4 Augmentation systems (GBAS/SBAS)

As discussed previously, satellite transmitted signals are the core of the GNSS-based positioning process. However, these signals are subject to errors related to clocks synchronization and atmospheric effects. Thus, augmentation systems serve as a solution to enhance the GNSS performances, by tackling the clock synchronization errors (Van Diggelen 2009). Depending on their functioning principle, two augmentation systems types can be distinguished:

1. Satellite Based Augmentation System (SBAS)
2. Ground Based Augmentation System (GBAS)

Satellite Based Augmentation System (SBAS)

SBAS is a wide coverage augmentation system in which the user receives augmentation information from a satellite-based transmitter. Similarly to the GNSS, the SBAS systems have a three segments architecture (i.e., space, control, and user). The principle of SBAS is to provide the user with information enabling to improve his/her GNSS estimated localization. These information corresponding to the errors due to signal propagation in the atmosphere, are calculated by a network of ground stations and then transmitted to the user via geostationary satellites.

European Geostationary Navigation Overlay Service (EGNOS), the European SBAS (working with GALILEO), is composed of a network of monitoring stations used to collect measurements that are processed by a Central Processing Facility (CPF). Then, the CPF computes clock and ephemeris corrections and a model for ionospheric errors. It worth noting that these corrections are valid for a defined coverage area and permit to improve the positioning accuracy for users within this area.

Ground Based Augmentation System (GBAS)

GBAS is an augmentation system in which the user receives augmentation information directly from a ground-based transmitter. The GBAS architecture comprises a number of ground stations located at accurately surveyed points and organized in order to serve a geographical area representing tens of kilometers. Each station receives GNSS satellite signals and compares the GNSS-estimated position with the real position of the station. Since the satellites being considered are the same for the user and the reference station, the errors' effects are assumed to be similar. Hence, relevant correction information are sent to the users in order to enhance their position's estimation.

Finally, it should be mentioned that the use of GBAS and SBAS augmentation systems is an important contributor to the development of safety-related positioning applications, such as Virtual Balise detection. However, the adoption of GNSS-based localization solutions to detect virtual balises in ERTMS Level 3 is not the only possible application of GNSS in railway. The adoption of GNSS-based localization for Railway applications is the subject of the following subsection.

2.7 GNSS-based systems in railway CCS: safety centered issues

In this section, a short review of current and potential applications of GNSS in railway functions is presented. Then, the main issues delaying GNSS adoption in railway operation, particularly for safety-related applications, are addressed.

2.7.1 Current and Intended GNSS applications in railway operation

The GNSS-based localization systems are relatively cheap solutions. Hence, their adoption is considered in a wide range of applications. In this subsection, a number of railway applications currently including GNSS are briefly presented, in addition to future investigated GNSS adoption for safety-related functions.

Current non-safety related applications

GNSS utilization in railway transportation is currently helpful in tracking or tracing trains, i.e., determining current locations (in real-time) or past locations (in delayed time) of trains/wagons, respectively.

The existing applications mainly concern passenger information or cargo management. In fact, several European countries have equipped their freight locomotives with GNSS receivers to better track freight trains and inform clients.

Moreover, GNSS-based localization solutions have been adopted in passengers trains for passenger information functions. For instance, the trains positions and scheduled times can be displayed on smartphones. Furthermore, the GNSS position can be used in mathematical models in order to optimize train energy consumption. In particular, this can be achieved through the adoption of the train speed profile in accordance with the position of the train on the line.

It is plain to say that the aforementioned applications are non-safety-related applications, as the safety of individuals and goods is not impacted.

Safety-related applications

On the other side, railway signaling systems can benefit of GNSS to realize some safety tasks such as:

1. Train detection and/or positioning,
2. Train spacing along the lines,
3. Selective doors opening at stations,
4. Train integrity monitoring,
5. Train driver assistance via the interface in train cabin.
6. Automatic train protection (ATP system),
7. Automatic train control (ATC system)

The advantages of these applications are no longer to be demonstrated (i.e., increased line capacity, reduced infrastructure costs, etc.). However, it is harder to accept the use of GNSS for such safety-critical functions than for non-safety-related functions, as the associated risks are important. Consequently, applications such as the virtual balises detection using GNSS-based positioning systems remain at concept and test lines stage and are not yet implemented. In fact, the safety demonstration related to the use of GNSS for railway safety-critical applications are still under investigation. The particular issues that have to be addressed before adopting GNSS for railway safety-related functions are the subject of the following subsection.

2.7.2 Safety Issues related to the use of GNSS in the Railway environment

As shown earlier in this chapter, the use of GNSS augmentation systems is a considered option to provide protection against errors originating from satellites, the GNSS ground segment, and from the ionosphere. Yet, the remaining hazards consist of the unbounded errors related to the railway local environment and receiver failures.

In this context, receiver failures can be addressed as a classical component failure problem. On the other hand, the errors resulting from the local environment are more tricky to consider and are the principle issue delaying the adoption of GNSS in railway safety applications.

In particular, the positioning accuracy of a GNSS-estimated position is highly dependent on the environmental conditions around the receiver. Indeed, GNSS are able to provide acceptable accuracy in clear open-sky conditions. For instance, in avionic applications, as the surrounding environment is particularly unchallenging, the local environment perturbations can be considered negligible. However, the typical environment around railway tracks may include, buildings, tunnels, bridges, forests, and urban canyons. In such conditions, signal perturbations due to environmental elements can lead to signal blockages, attenuation, reflection, or diffraction. A number of typical rail environments are illustrated in Figure 2.18.

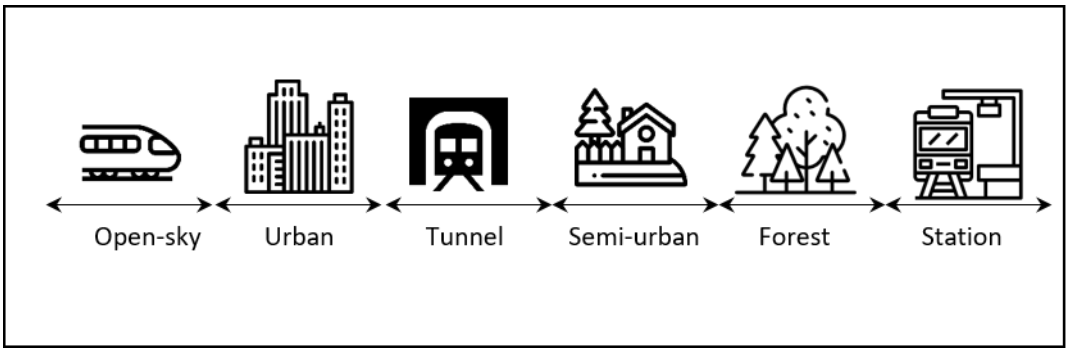


Figure 2.18: Example of typical rail environments.

In some cases (e.g., tunnels), the GNSS may not even be able to provide position due to signal blockage. In the other cases, the GNSS performance deterioration is mainly due to *multipath* phenomenon.

In fact, multipath results from the cumulative reception of reflected and diffracted echoes in the presence of a direct line-of-sight signal (LOS). As a result, signal propagation times between satellites and receivers can be delayed due to the reflection of the signals on the obstacles in the vicinity of the receiver (Pachl 2020; Presti and Sabina 2018). Furthermore, as these propagation times are the most important parameters for position estimation, the calculated positioning information can be biased without the system notices it. Hence, it is particularly challenging to detect and correctly estimate the multipath delays. In particular, the non-line-of-sight (NLOS) phenomenon is a specific form of multipath that occurs when only the reflected signals reach the receiver while the obstacles block the LOS signal. In such conditions, the GNSS performances are further degraded, leading to an increased risk. The multipath and the NLOS phenomena are illustrated in Figure 2.19.

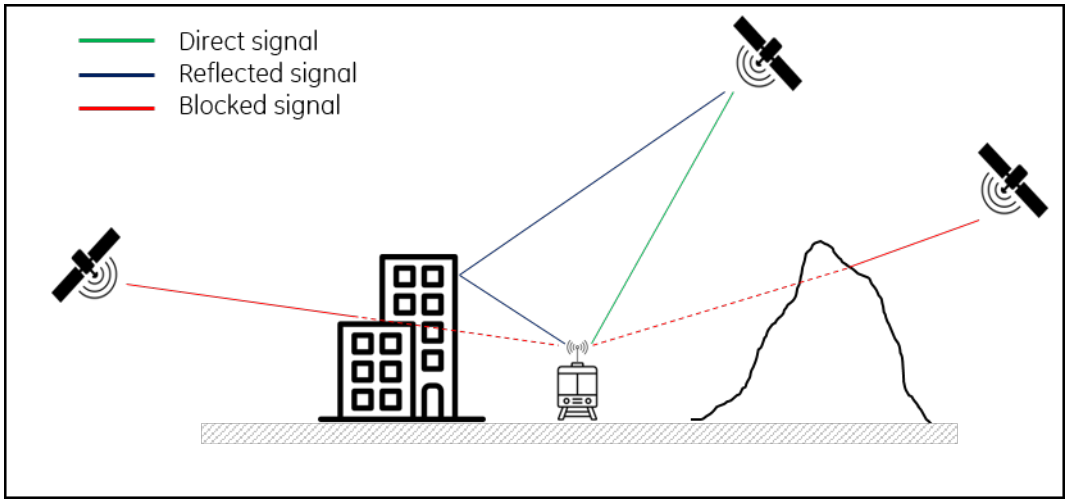


Figure 2.19: Multipath phenomena illustration.

Besides, additional perturbations may result from electromagnetic interferences (EMI) with the electrical equipment present in the local railway environment. However, we should highlight that the EMI and the intentional perturbation (e.g., spoofing and jamming) are out of the scope of this contribution. In fact, w.r.t. GNSS localization, the contribution presented in this thesis intends to tackle the following issues:

- How to consider the hazards associated with the railway *'**dynamic**' and '**environment-related**' aspects?*
- What is the correlation between the train ***'operational conditions'*** and the *'**uncertainties**'* associated with the GNSS-estimated position?
- Which ***testing process*** can be adopted in order to address the aforementioned challenges?

2.8 Chapter Conclusion

In this chapter, the main context elements related to our research topic have been synthetically addressed. In particular, the limitations that are inherent to the current railway positioning solutions, in addition to the knowledge gaps regarding the safety of satellite-based train positioning, are pointed out. For this purpose, railway signaling systems and their central safety-related functions were firstly addressed, as the investigated ERTMS Level 3 concept is at the center of our interest.

As our research theme is essentially centered on the railway localization function, an overview of the various railway positioning techniques was presented. In so doing, the limitations of the localization solutions currently used, both in terms of accuracy and in terms of installation and maintenance costs, were addressed. It was also discussed how promizing is the introduction of on-board embedded localization techniques, such as GNSS, to overcome the limitations of current railway localization systems. We should mention, here, that the detailed mechanisms related to the GNSS-based train positioning (e.g., Virtual Balise detection) were not discussed in this chapter. More details can be found in Chapter 4 of this manuscript.

The following part of this chapter focused on the presentation of the GNSS systems. Indeed, satellite positioning is present in the daily life of everyone, with a wide range of applications. Nevertheless, its functioning principle often remains unknown to most of the public. Yet, the exposition of such principle basics is of paramount importance for a good understanding of the rest of this thesis. In this context, one must keep in mind that the fundamental principle of GNSS position estimation is based on calculating the signal propagation time. These signals are emitted by different satellites in constellations. However, such signals may encounter several obstacles before reaching the user GNSS receiver, especially in the railway operation environment.

Moreover, it has been explained that the GNSS systems were initially developed for avionic applications in a clear environment. Hence, the safety evaluations of the GNSS systems usually neglect the hazards related to the exploitation environment. Nevertheless, such a hypothesis cannot be accepted in the railway context.

In conclusion, although GNSS would offer substantial benefits for railway operations, the lack of safety evidence remains the main issue that hinders the adoption of GNSS-based positioning solutions for railway safety-related functions. Therefore, *it is crucial to define an efficient validation framework for GNSS-based train localization in order to ensure safety*. In fact, this is *not only a matter of safety but also a matter of acceptability*. Accordingly, the following chapter is dedicated to the relevant safety aspects to be investigated in order to tackle these issues.

Chapter 3

Which safety approach for complex railway systems?

Outline of the current chapter

3.1 Chapter introduction

Providing sufficient safety proofs is a necessary condition to be fulfilled before a safety-critical system can be authorized to operate. As shown in the previous chapter, train localization is a safety-related function in Control-Command and Signaling Systems and, therefore, its operating conditions have to be safely proved. Namely, the demonstration of the safety of GNSS utilization in the railway operational environment is a challenge that has inevitably to be tackled before the adoption of GNSS for train positioning.

To conduct such a safety demonstration, various approaches can be found in the literature and adopted depending on the addressed system. In this context, in the present chapter, we firstly introduce the European regulatory framework that must be respected to ensure the safety of railway systems (3.2). With respect to this framework, a wide range of safety methods can be used to perform the various safety activities that derive from the safety demonstration process. Accordingly, Section 3.3 is dedicated to the presentation of both *classic* and *advanced* safety methods. Moreover, the advantages and limitations of those methods are discussed throughout this chapter to conclude on the most suited methods to adopt when dealing with complex railway systems. The relevant contributions that fall within this context are also presented in this section. In Section 3.4, a particular focus is made on the specificities pertaining to GNSS-based train positioning systems in order to identify the relevant obstacles that need to be tackled when proposing a new safety approach.

3.2 European regulatory framework for ensuring safety of railway systems

This section is dedicated to the presentation of the European-specific regulatory framework related to ensuring the safety of railway systems. First, the main applicable regulations and standards are introduced. Then, the various safety activities to be conducted along the life cycle of the system are presented. Finally, the manner in which the results of the safety activities can be compiled in order to provide an assessable *Safety Case* is covered.

3.2.1 Applicable regulations and standards

In the European context, railway systems are developed while ensuring various interoperability requirements. In particular, Technical Specifications for Interoperability (TSIs) provide guidance allowing to ensure the interoperability of the railway system of the European Union. Thus, harmonization at European level requires interoperability, yet interoperability cannot be achieved at the expense of safety. Hence, parallel to the interoperability principle, an immutable ground rule in the railway domain stipulates that *it is forbidden to degrade the safety level of a critical railway system*. Accordingly, European safety standards and one regulation, respectively EN 50126/28/29 and Common Safety Method for Risk Evaluation and Assessment (CSM-RA), have established a system's safety management process to ensure safe railway operations. An insight into these aforementioned standards and regulations is provided in the remainder of this subsection.

Technical Specifications for Interoperability (TSIs)

The European directive EU-2016/797 defines the subsystems, either structural or functional, forming part of the railway system of the European Union. For each of those subsystems, the essential requirements need to be specified and the technical specifications determined in order to meet those essential requirements, which can be categorized into six distinct classes:

- **Safety**
- Reliability and availability
- Health
- Environmental protection
- Technical compatibility
- Accessibility

In order to meet the essential requirements and ensure the interoperability of the railway system, the Technical Specifications for Interoperability (TSIs) define the technical and operational standards which must be met by each subsystem or part of subsystem. Accordingly, the various TSIs can be listed as follows:

1. Control Command and Signalling TSI
2. Rolling Stock - Locomotives and Passengers TSI
3. Rolling Stock - Freight Wagons TSI
4. Safety in Railway Tunnels TSI
5. Energy TSI
6. Infrastructure TSI
7. Noise TSI
8. Operation and Traffic Management TSI
9. Telematics Applications for Passenger service TSI
10. Telematics Applications for Freight service TSI
11. Persons with Disabilities and with Reduced Mobility TSI

Among these TSIs, it should be noted that the CCS TSI (Control-Command and Signalling) develops the most safety-related requirements as CCS is a pillar of railway safety.

EN 50126, EN 50128 and EN 50129 standards

In addition to the rules described in legal texts (i.e., directives, decisions, regulations), the design and operating conditions of railway systems in Europe are today subject to a normative framework that requires the demonstration of the system's safety. This framework is composed of specific European standards derived from the generic functional safety standard IEC 61508 : 2011 (cf. Figure 3.1).

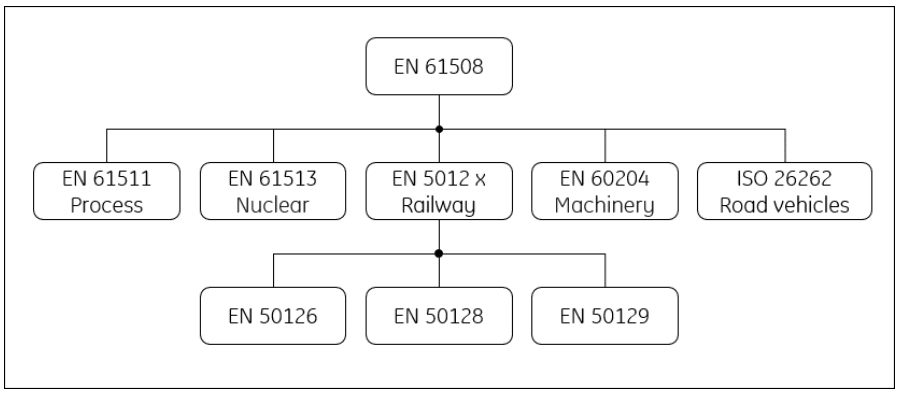


Figure 3.1: Main Safety related standards

Compared to other industrial sectors, the railway sector is distinguished by the existence of three safety standards (EN 50126 : 2017, EN 50128 : 2011, and EN 50129: 2018]). Each of them addresses a particular safety aspect and can be applied depending on the considered subsystem.

- The EN 50126 standard describes a systematic RAMS management process (starting from the design phase until the system decommissioning) in order to specify and demonstrate reliability, availability, maintainability, and safety. Part 1 of this standard focuses on the generic RAMS process, while part 2 addresses the systems approach to safety.
- The EN 50128 standard specifies the process requirements and techniques applicable to the development of software for programmable electronic systems used in railway Control-Command and protection applications.
- The EN 50129 standard addresses safety-related electronic systems (including subsystems and equipment) for railway signaling applications.

Overall, the rail standards recommend applying a risk management process prior to the design of a rail transportation system. Yet, at the European level, different national regulations and safety cultures can be found across the various Member States. Such a diversity can lead to some misunderstandings between the various national railway safety authorities when applying the risk management process. To overcome this limitation, the various steps of the risk management process are harmonized in the CSM-RA European regulation (EU) No 402/2013 (amended by the implementing regulation (EU) No 2015/1136) part of a set of Common Safety Methods defined by ERA (EU Agency for Railways 2021).

Common Safety Methods (CSMs)

The CSMs describe how the safety levels, the achievement of safety targets and compliance with other safety requirements should be fulfilled .

In fact, the CSM regulation is declined into six distinct elements. Namely:

- Common Safety Methods for risk evaluation and assessment (CSM-RA)
- Common Safety Method for monitoring
- Common Safety Methods for safety management system requirements
- Common Safety Methods for supervision
- Common Safety Method for common safety targets
- Common Safety Methods for conformity assessment

In the rest of this thesis, a particular attention is drawn to CSM-RA regulation that sets out the risk assessment process, in addition to the criteria to be fulfilled by the assessment body responsible for checking the correct application of the risk assessment process and the results of this application.

Furthermore, it should be noted that the CSMs are directly applicable and enforceable in the European Member States. Their application in fact mandatory for any new railway system, as well as for any existing system undergoing significant technical, operational, and/or organizational changes. Yet, such a condition raises the question of *'when is a change considered significant?'*

To address this question, the fourth Article of the CSM stipulates that in the absence of notified national rule defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system. Namely, if the proposed change has an impact on safety, the proposer shall decide, by expert judgment, on the significance of the change based on the following criteria:

1. Failure consequence: considering the credible worst-case scenario in the event of a system failure, taking into account the existing safety barriers that are external to the system;
2. Novelty used in implementing the change: this concerns both what is innovative in the railway sector and what is new for the organization implementing the change;
3. Complexity of the change;
4. Monitoring: the ability to monitor the implemented change throughout the system life-cycle and the possibility to intervene appropriately;
5. Reversibility: the inability to revert to the system before the change;
6. Additionality: assessment of the significance of the change (taking into account all recent safety-related changes to the system under assessment and which were not judged to be significant).

In the case of GNSS-based railway positioning systems, the consequences of failures can be dramatic; moreover, the novelty and complexity criteria are clearly matched. Therefore, the introduction of such systems is subject to the comprehensive application of the CSM regulation.

3.2.2 Safety activities in the system life cycle

With the aim to ensure safe and performant railway systems that fulfill their intended objectives, various performance and safety-related activities are conducted all along the system life cycle. Accordingly, the EN50126 standard recommends adopting the life cycle approach that provides a structure for planning, managing, controlling, and monitoring all the aspects of a system, including reliability, availability, maintainability and safety (RAMS).

In this subsection, we will firstly outline the general life cycle process. Then, the most relevant activities with respect to safety (i.e., Risk assessment; compliance with RAMS; verification and validation; and operation safety management) are further detailed.

The V-shaped life cycle process

The life cycle approach proposed in the EN50126 standard can be represented according to the 'V' diagram depicted in Figure 3.2.

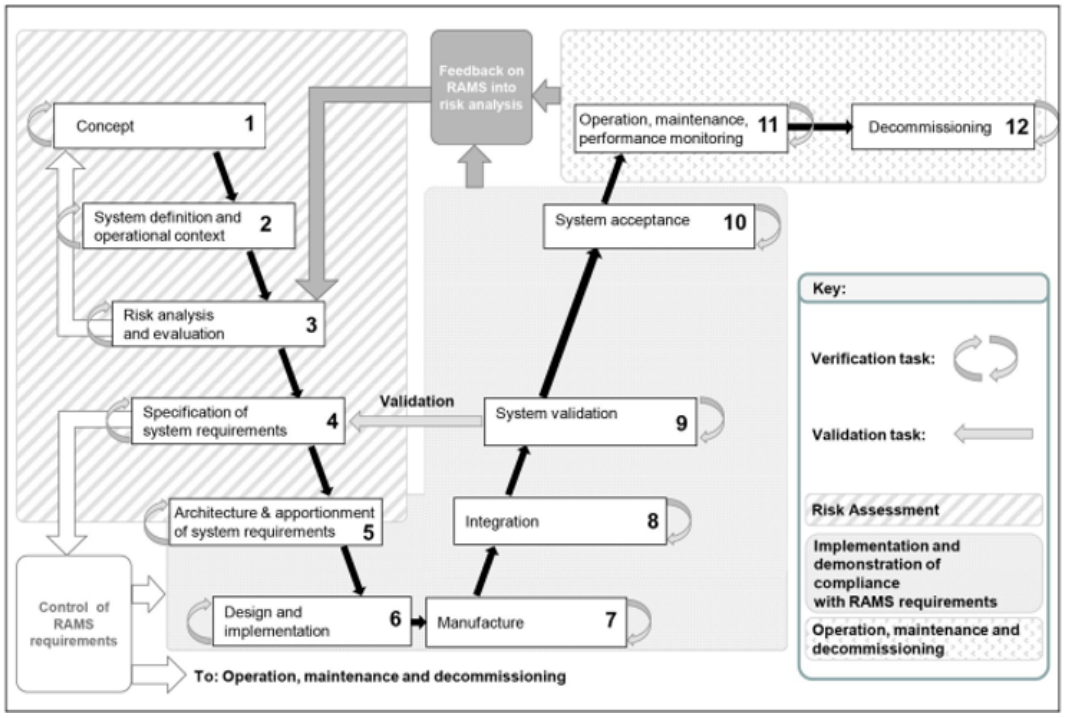


Figure 3.2: The V-cycle representation according to EN50126

Generally speaking, the left side of the V-cycle represents a top-down branch commonly referred to as the "development" phase, which consists in a refining process ending with the

manufacture of the system components. The right-hand side is a bottom-up branch related to the assembly, installation, hand-over and 'operation and maintenance' of the entire system.

Concerning safety, three major blocks of phases can be distinguished in the general V-cycle process, namely:

- *Risk assessment* (cf. phases from 1 to 5 in Figure 3.2.)
- *Implementation and demonstration of compliance with RAMS requirements* (phases from 5 to 10)
- *Operation, maintenance and decommissioning* (phases 11 and 12)

Alongside this nominal process flow following the life cycle phases, the general process includes loops, such as the *'feedback on RAMS into risk analysis'* that should be applied if new or additional knowledge about risk (requiring the risk to be reassessed) comes up during any phase of the project. Furthermore, it can be noted that Verification and Validation activities (represented by arrows in Figure 3.2) are performed all along the V cycle. Validation has a specific dedicated phase based on verification steps.

Risk assessment activities

Risk assessment activities are related to the first phases of the life cycle (from phase 1 to phase 5).

Phase 1: Concept
The first step of the life cycle is the *'Concept'* phase. Its objective is to develop a sufficient understanding of the system to ensure the proper performance of all subsequent RAMS life cycle activities.

Phase 2 : System definition and operational context
Before any analysis relating to RAMS is undertaken, boundaries and functions of the system under consideration shall be established. Therefore, the objective of phase 2 (i.e., *System definition and operational context*) is to provide a description of the essential characteristics and functions of the system, in addition to a clarification of the interfaces with other systems and the operational context.

Phase 3 : Risk analysis and evaluation
This phase constitutes the main activity of the *risk assessment* task. Such a phase comprises both the *Risk Analysis* and *Risk Evaluation*, which are performed based on the system definition resulting from phase 2 of the life cycle (e.g., the defined scope of system risk analysis).

In particular, the *Risk analysis* consists in the systematic use of all available information to identify hazards (or its RAM equivalent for the quality of service), related potential losses and to evaluate the associated risk. Accordingly, the first steps of the risk analysis consist of the *identification and classification of hazards*.

Concretely, the classification of hazards means that it shall be decided, for each identified hazard, if the related risk can be considered as "*broadly acceptable*".

- If the risk analysis identifies cases with a level of risk that is "broadly acceptable", there is no need to specify further requirements for those cases.

- However, if the risk analysis concludes that a risk is not "broadly acceptable", the risk analysis activity shall be continued by choosing and applying a 'risk acceptance principle' (RAP), before applying risk evaluation. Namely, the three risk acceptance principles correspond to:
  - the use of Code of Practice (CoP);
  - a comparison with a similar system as a reference;
  - Explicit risk estimation (ERE), which can be either qualitative or quantitative.

Finally, the risk assessment process continues with risk evaluation in order to determine the safety measures allowing the achievement of the criteria associated with the selected RAP.

It can be noted here that the CSM-RA regulation provides more detailed explanations of the risk assessment process (in accordance with the EN 50126)((EU) No 402/2013). The risk assessment process in the overall risk management process is depicted in Figure 3.3 (taken from ERA 2009).

Phase 4: specification of system requirements
The following step of the life cycle is the '*specification of system requirements*', including safety requirements (i.e., the Safety Measures to be implemented). This phase aims to provide a comprehensive and identified set of requirements for the subsequent life cycle phases. To this aim, the initial system requirements are further detailed in addition to the ones derived from risk assessment in phase 3. Moreover, the overall demonstration of the compliance process is specified alongside the definition of the RAMS acceptance criteria.

Phase 5: Architecture and apportionment of system requirements
The main objective of this phase is to allocate system requirements to the various subsystems and/or components.

Demonstration of compliance with RAMS requirements

Based on the system architecture established in Phase 5 of the life cycle, the set of process phases from 6 to 8 respectively address:

- the *design and implementation* (i.e., creation of the subsystems and components),
- the *manufacture*, and
- the *Integration* (i.e., assembly and installation of all subsystems and components to form the complete system).

All of the aforementioned phases should be performed with respect and compliance with the system safety requirements defined as part of the *Risk Assessment*.

Such compliance is at the center of *phase 9: System Validation*, which will particularly be addressed, conjointly with the verification activities, in the sequel. If the results of the *system validation* phase are satisfactory and conclusive, the *system acceptance* phase can be initiated.

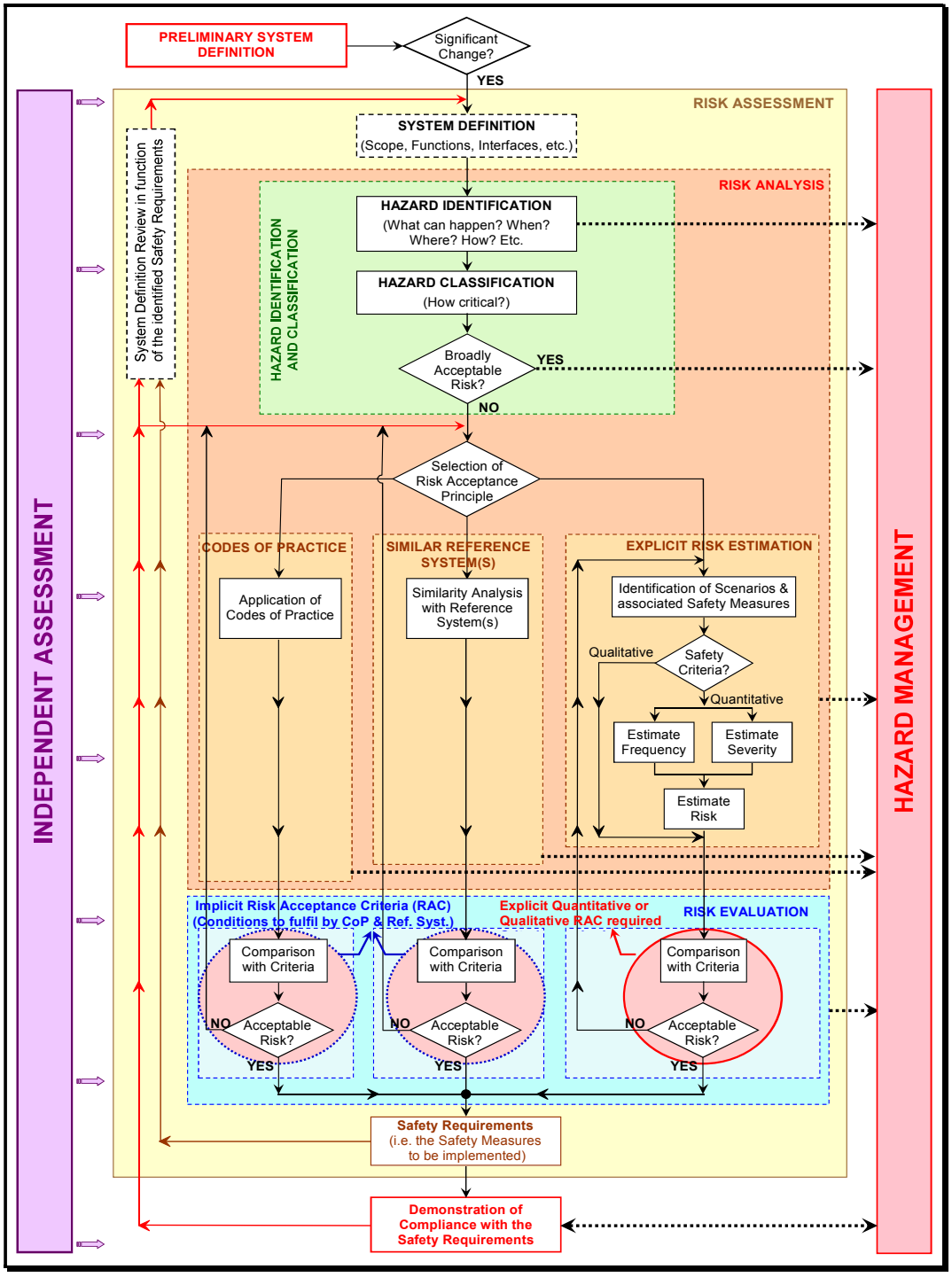


Figure 3.3: Risk management process according to the CSM-RA

It is here underlined that the *Reliability*, *Availability*, *Maintainability*, and *Safety* attributes, usually referred to as RAMS, are the determining parameters that constrains the acceptance of the system. Their definitions are inherited from the IEC 60050-192: 2015, IEC 61508-4: 2010, and EN 50126 : 2017, and can be summarized as:

Reliability
Reliability is the ability that an item can perform a required function, without failure, for a given time interval, and under given conditions.

Availability
Availability is the ability of an item 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
Maintainability is the ability to be retained in (or restored to) a state to perform as required under given conditions of use and maintenance.

Safety
Safety is the freedom from an unacceptable risk of harm. This later (i.e., harm) is further defined as the physical injury or damage to the health of people or damage to property or the environment.

Accordingly, the *safety function* concept represents any function whose purpose is to achieve or maintain a safe state for the system in respect of a specific hazardous event.

Moreover, the *safety integrity* is further defined as the ability of a safety-related system to satisfactorily perform its required safety-related functions under all the stated conditions within a stated operational environment and a stated period of time.

Note 1: it is worth noticing that the assessment of the aforementioned parameters can be challenging when dealing with systems under uncertainties. Accordingly, some literature contributions specifically focused on proposing adapted means to evaluate the reliability and availability of systems in the presence of such uncertainties (Sallak 2007; Sallak, Schön, and Aguirre 2013; Martinez, Sallak, and Schön 2015; Qiu et al. 2014a; Akrouche et al. 2022).

Note 2: we finally note that the concept of *safety* should not be confused with the *Security* which represents the robustness against intentional hostile action.

Finally, more insight about the RAMS characteristics and the mean of quantification are available in the appendix of this manuscript.

Operation safety management

Following the acceptance of the system, its commissioning can be carried out.

During such an operational phase, and until the decommissioning of the system, the system

under consideration should be operated, maintained, and supported in such a fashion that compliance with RAMS requirements is maintained. This compliance is precisely the objective of phase 11 of the life cycle, which includes continuously monitoring and evaluating the RAMS performance of the system and deriving corrective measures if required. It is worth noticing that such operational safety management framework is crucial, since this is the point at which pre-operational safety studies and analyses encounter the reality of the system in its actual operating environment. Furthermore, practical evidence from real-world operations provides a considerably higher degree of confidence than the evidence obtained from pre-operational studies and tests.

The operational evaluation methods are essentially based on the collection of data from practical experience feedback. Accordingly, the adoption of this process requires relavant data issued from the monitoring of the equipment in operation, or the measurements obtained during the testing phase, for new systems. Then, the clustering of all the extracted data in structured databases, and their their analysis, permit the extraction of useful information (cf. Figure 3.4).

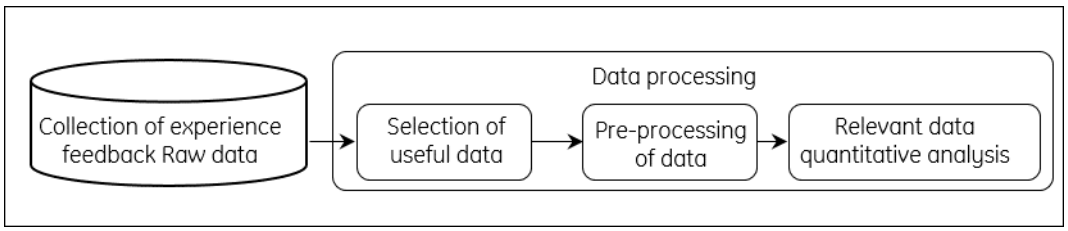


Figure 3.4: Evaluation procedure based on the analysis of Operational Experience and Feedback data.

Finally, the processing of this information by statistical analysis allows for estimating some indicators such as the operational performance of the system or deducing probabilistic distributions.

Verification and Validation

All along the system life cycle, some verification and validation tasks should be conducted as an integral part of the overall process.

Verification

On the one hand, *Verification tasks*, which are included within each life cycle phase, support and provide input to the validation activities (cf. below). The objective of these verification tasks is to demonstrate that the requirements of each life cycle phase have been fulfilled. Accordingly, these tasks shall be conducted in each life cycle phase to deal with:

- the correctness and adequacy of the RAMS analysis, where specified;
- the compliance of the deliverables of the phase with the deliverables of former phases;
- the adequacy of the methods, tools and techniques used within the life cycle phase, where specified;

- the correctness, consistency and adequacy of test specifications and executed tests, as appropriate.

Finally, it can be noted that in case some errors or deficiencies are elucidated by the verification tasks, the reapplication of some or all of the activities of one or more previous phases along the life cycle may be necessary.

Validation

On the other hand, *Validation* activities are undertaken as follows:

- In Phase 4 "Specification of System Requirements", the validation aims to ensure that the system requirements (including RAMS requirements) have been properly specified.
- In Phase 9 "System Validation", the validation aims to assure that the system under consideration meets the specified requirements for the intended use or application.

In particular, Validation shall demonstrate that the process for the system under consideration, including related lifecycle outputs of related life cycle phases, is such that:

- the RAMS requirements for the system under consideration, including safety-related application conditions, have been properly specified for the intended use or application;
- the system under consideration, including safety-related application conditions, fulfills the related RAMS requirements for the intended use or application.

Note that the validation can further depend on specific requirements defined by applicable legal regulations.

3.2.3 Safety Case

A safety case is a structured and documented safety justification that provides evidence of the compliance of the system under consideration with the specified safety requirements.

The safety case is relevant within a defined scope of the proposed use of the system under consideration and enables the users and operators of the system to have confidence that the system meets the specified safety requirements. For that, the safety case should expose a compelling demonstration of how the system complies with the requirements determined following the EN 50126/28/29 normative framework.

In practice, the safety case refers to a set of complementary documents that cover an extensive array of subjects, including:

- the definition of the system under consideration (i.e., key subsystems, architecture, expected behavior, etc.)
- a report on quality management activities and evidence.
- a report on safety management activities and evidence.
- a technical report on safety assurance activities and evidence in various contexts (i.e., in nominal fault-free conditions, in the event of failures and errors)

- References to the safety cases of all subsystems/equipment on which the main safety case depends.
- A conclusion report that summarizes the presented safety claims and evidence.

Furthermore, it should be underlined that the safety case sets the basis for the certification process. To obtain certificates of conformity to safety and interoperability requirements, an independent safety assessment is before required. The entity realizing the assessment performs an essential step to provide additional confidence to the safety authority regarding the avoidance of systematic failures. In fact, independent safety assessment is based on the evaluation of the verification and validation activities already undertaken, with a particular focus on the adequate application of the risk management process to achieve safety-related activities. In Europe, such an independent safety assessment process is mandatory in the system authorization process. This last process is managed by the National railway Safety Authorities (e.g., EPSF in France, EBA in Germany) and results in an APIS (Authorization for Placing Into Service).

3.3 Toward the use of advanced safety methods for complex railway systems

From a safety perspective, the objective of safety engineering can be summarized as the proper identification and classification of all the hazards that the system can present, the evaluation of the associated risks with respect to some defined risk acceptance criteria, and the implementation of safety measures in order to prevent potential harm and accidents.

To perform the safety engineering tasks, a set of methods, referred to as traditional, are commonly employed. Nevertheless, with the advent of increasingly complex and distributed systems, those classical methods show limitations when dealing with certain particular aspects related to such growing system complexity. Consequently, more advanced methods, which are better adapted to the investigation of complex systems, have emerged in the last decades. In the railway field, where more and more communication and computerized systems are adopted, we currently experience a progressive trend of adopting advanced methods to address safety issues.

In this section, we present a short overview of traditional and advanced safety methods that can be found in the literature. We devote special attention to the research works that use advanced methods in the railway domain.

3.3.1 Traditional safety methods

This first category of safety methods can be referred to as the traditional approaches since the associated techniques are well known, widely adopted in various domains, and benefit from good experience. Without claiming to be exhaustive, among the most commonly employed methods, we can refer to the following techniques:

1. Preliminary Hazard Analysis (PHA) is a method that allows for identifying and evaluating risks at the early stages of system design. Based on the set of hazards to which the system may be exposed to throughout its mission, the objective of the PHA is the identification, evaluation, prioritization, and control of the resulting risks.

2. Hazard and Operability studies (HAZOP) make use of a set of guide-words to identify possible hazards. This process is continuously applied throughout the project life-cycle to ensure all risks are identified and properly managed (EN 61882: 2016).

3. Fault tree analysis (FTA) is a deductive technique based on identifying a system-level fault at the top of the tree. The combinations of events that can cause the addressed feared event are then investigated (IEC 61025: 2006).

4. Event tree analysis (ETA) is an inductive technique, and consists of the adoption of logical reasoning to identify the possible consequences (in contrast with FTA) resulting from an initiating event that the system can experience (IEC 62502: 2010).

5. Failure Mode and Effect Analysis (FMEA) is based on human expertise to review the whole system at either the system, the functions, or the components level, and identify the potential failures and their consequences. By identifying these faults early in the system life-cycle, design changes at a later stage can be avoided (IEC 60812: 2018).

6. Failure Mode, Effects, and Criticality Analysis (FMECA) is the extension of FMEA by adding the criticality measurement to the consequences of the failures. Concretely, the criticality analysis is a procedure where each potential failure is ranked according to the combined influence of severity and probability of occurrence (IEC 60812: 2018).

Generally speaking, the methods mentioned above adopt a predictive analysis approach that seeks for conditions and events (e.g., a component failure) to predict the set of potential consequences resulting from some identified failures, or to determine the possible causes of some feared events. Concretely, such predictive analysis process can be summarized in four main steps (see Figure 3.5):

1. A technical and functional analysis gathering information about the system and its environment in order to define the scope of the study. This information may include:

   (a) system structure (nature and number of components).

   (b) nature of the system (electronic, mechanical, etc.).

   (c) identification of the main and secondary functions.

   (d) list of the operating and failure modes.

2. A qualitative analysis by applying one or more methods (e.g., HAZOP, FMEA), leading to a classification of the hazards.

3. A quantitative analysis leading to a probabilistic estimation of the studied parameters.

4. A conclusion synthesizing the qualitative and quantitative analysis results and a potential set of improvement or modification proposals.

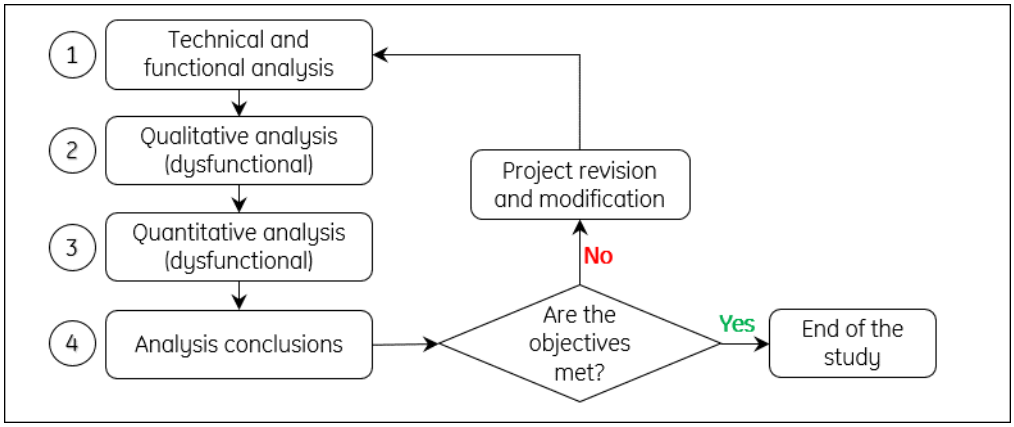


Figure 3.5: Predictive analysis steps.

From an application perspective, those methods can be used either for risk analysis, failure analysis, or even both. This adaptability in terms of objective depends on the way the methods are applied in terms of :

- the level at which the system is analyzed :
  - high level: hazardous context/function
  - low level: failure of equipment or components
- the type of the adopted approach :
  - bottom/up: mostly for RAMS performance verification,
  - top/down: often for quantitative requirement allocation.

Nevertheless, these methods and approaches are mostly dysfunctional and are, in general, hard to implement, or even inappropriate, when dealing with a complex system. For instance, those classical methods are static. Hence, the analysis of temporal and dynamic aspects (e.g., varying environmental conditions as the train moves on the rail line.) inherent to complex systems is limited when using such approaches. Besides, the traditional methods show a lack of modularity. Yet, the modularity feature is of particular importance when dealing with large-scale systems. finally, the dependence on human expertise (i.e., the system analysis relies on human knowledge and feedback) can be seen as a drawback of these methods. Indeed, such a feedback approach does not permit to guarantee neither the objectivity nor the exhaustiveness of the conducted analysis.

3.3.2 Existing advanced methods for safety analysis of complex systems

When dealing with complex systems, a number of issues arise. In particular, requirements engineering, maintainability, testing and evaluation, become more challenging. Yet, such activities

are necessary for successful system design, development, operation and ultimate decommissioning. To overcome the limitations of the classical approaches presented in the previous subsection, the recent decades have experienced the adoption of some *advanced* methods, which bring a substantial added value in designing and verifying safety critical systems. Such advanced methods, which are the subject of this subsection, support more features permitting to address complex systems.

In this context, *systems engineering* recently emerged as an interdisciplinary scientific approach that aims to formalize and apprehend the design and validation of complex systems that cannot be easily managed. In particular, this interdisciplinary field of engineering focuses on how to design, integrate, and manage complex systems all over their life cycles. Concretely, systems engineering overlaps technical and human-centered disciplines (such as mechanical, manufacturing, control, software engineering, and project management) to ensure that all likely aspects of a project or system are correctly considered and integrated.

Model-based approaches (MBSE/MBSA)

Model-based systems engineering (MBSE) is identified as a technical approach to systems engineering that focuses on creating and exploiting models as the primary means of information exchange rather than document-based information exchange. As stated by the International Council on Systems Engineering (INCOSE), MBSE is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout the development and later life cycle phases.

With a particular focus on the safety-related aspects of complex systems, *Model-Based Safety Analysis (MBSA)* is an approach in which the design and safety engineers share a common system model issued through a model-based development process.

Concretely, MBSA employs models to describe the fault behavior of a system. Accordingly, safety analyses can be performed based on those models. Moreover, the reuse of modeling elements makes it possible to study various architectures with respect to safety properties without extensive manual effort and paves the way for partly automatized analysis.

The most prominent example of MBSE/MBSA modeling languages used in the industry are the famous UML, SysML, and LML notations.

- The Unified Modeling Language (UML) is a general-purpose, developmental modeling language for systems engineering applications. It is intended to provide a standard way to visualize the design of a system (Booch, Rumbaugh, and Jacobson 1999).
- The Lifecycle Modeling Language (LML) is an open-standard modeling language designed for systems engineering. It supports the full lifecycle stages and integrates all lifecycle disciplines (including systems and design engineering, verification and validation, deployment, and maintenance) into one framework (LML Specification 2022).
- The Systems Modeling Language (SysML) is an extension of a subset of the UML standard using UML's profile mechanism. The language's extensions were designed to support systems engineering activities. In particular, SysML supports the specification, analysis, design, verification and validation of a broad range of systems and systems-of-systems (SysML Specification 2019).

Formal Methods

The aforementioned model-based approaches (i.e., MBSE/MBSA) can be seen as a bridge between design engineers and safety engineers, reducing the time required to verify the safety of a new and complex system. Yet, such notations, considered as *Semi-formal notations*, still lack precise and unambiguously defined syntax and semantics and are, thus, subjected to individual judgment and experience.

In contrast, *Formal Methods* are techniques based on mathematical and logical foundations to rigorously describe the system behavior. Concretely and in contrast to natural language, these methods establish an explicit description of the system using non-ambiguous notations and language (e.g., mathematical equations). Such representations help avoid misunderstandings and errors resulting from the different potential interpretations of the same information. Depending on the objectives sought through the use of fully formal methods, multiple applications of those approaches can be distinguished.

- For instance, the B family methods are employed (Butler et al. 2020) as *Model-based development* solutions. Concretely, such rigorous approaches allow for reaching a concrete (low-level) implementation of a system from an abstract (high-level) specification through successive refinement steps based on model transformation (Mammar et al. 2018; Eschbach 2021; Comptier et al. 2017). For that, the specifications are iteratively complemented with details that are unnecessary at the early stages of the system development. Finally, automatic code generation is usually used in the sequel of formal development to obtain a source code that is by definition consistent with the model it is generated from.

- On the other hand, correct-by-construction approaches such as *supervisory control synthesis* (Caillaud et al. 2002) address the creation of system models that provably satisfy formal specifications. Concretely, a supervisory controller model is synthesized starting from a model of the uncontrolled system and using a model of the behavioral requirements. Consequently, the supervisory controller disables a set of controllable events to influence the system behavior and guarantee system correctness with respect to the defined requirements. Yet, such approaches do not provide means to address the uncontrollable events related to signal perturbation.

- Finally, *formal verification* is employed with the aim of proving that system properties related to safety are satisfied. Such usually automated verification helps to reduce the time and effort needed to prove the correctness of systems. As the contribution presented in this thesis falls in this context, particular emphasis will be devoted to formal verification in the remainder of this manuscript.

Over the past two decades, one can observe an increasing trend toward employing such formal methods in various industrial applications (Craigen, Gerhart, and Ralston 1993; E. M. Clarke and Wing 1996; Trouillet, Korbaa, and Gentina 2006; Woodcock et al. 2009; Hall 2007; Weyns et al. 2012; Boufaied, Thabet, and Korbaa 2016; Gleirscher, Foster, and Woodcock 2019; Thabet, Lamine, et al. 2020; Thabet, Bork, et al. 2021)

Formal Verification

A notable advantage of employing formal methods is that the formal system models may also be used to verify a set of properties and provide formal proofs of their correctness (e.g., the

absence of event sequences leading to an undesired situation). Thus, formal methods set a basis for automatic verification of a wide range of properties.

Two main types of formal verification approaches can be distinguished, namely:

- Theorem proving (Robinson and Voronkov 2001)
- Model-Checking (MC) (Konnov 2019)

On the one hand, theorem proving is based on deductive reasoning with the objective of providing proofs in symbolic logic by inference. Significant parts of this process can be automated by means of Theorem Provers (Nawaz et al. 2019). However, the adoption of such a deductive approach can be very tricky when dealing with systems of which the dynamcis can be impacted by uncertainties. In what follows, we will focus our interest on Model-Checking (MC) technique (including probabilistic and statistical approaches), as we will bring into play such techniques in our work.

Founded by the ACM 2007 Turing Award winners (i.e., Edmund Clarke, Allen Emerson, and Joseph Sifakis), the *Model-Checking (MC)* (E. M. Clarke and Emerson 1981; Queille and Sifakis 1982) is a state-of-the-art automated computer verification technique that allows for checking whether a system model meets some given specifications. Concretely, MC is based on the systematic exploration of the system state space representing all possible system behavior in the form of a reachability graph. Such state space can be represented either explicitly, or in a symbolic way.

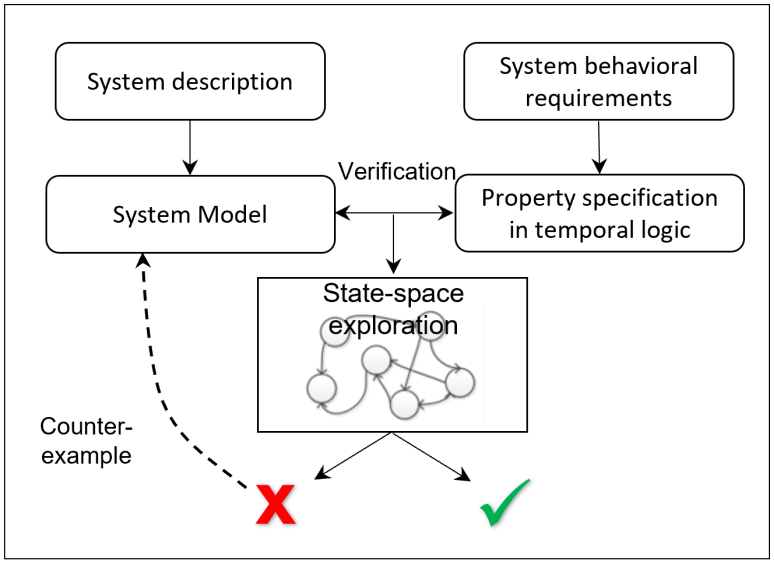


Figure 3.6: Schematic diagram of model checking.

More precisely, MC technique primarily involves two ingredients, see Figure 3.6 (Kumar 2018):

1. A formal model of the system: represented using formal notations such as state transition diagrams. The model translates the system behavior and shows how the system may evolve from one state to another.
2. Formal property specification: expressed as a logical formula over the state transition diagram of the modeled system and formulated by means of temporal logic assertions. Such specifications represent the desired/undesired behavioral property (e.g., deadlock) to be verified.

Model checking algorithms take the two aforementioned inputs and confront the investigated property with the system model. If the property does not hold true, the model checker provides a counterexample trace that demonstrates a possible event sequence path leading to a violation of the property. This enables, typically, to identify risky scenarios that have not been anticipated during the preliminary risk analysis.

It is straightforward that such reachability analysis approaches (i.e., based on the exhaustive state space exploration) suffer from the combinatorial state-space explosion problem, especially when dealing with complex systems as the number of state variables of a system increases. To overcome this limitation, methods such as the symbolic representation of state spaces, symmetry-based reduction methods, or partial order reduction methods have emerged, as solutions that enable reducing the state space (Burch et al. 1992; E. Clarke et al. 2001; Ehrig et al. 2010).

Statistical Model Checking (SMC)

Historically, Model-Checking techniques focused on the logical correctness of systems by verifying the absence of errors in a system model (exp., checking that some undesirable events never occur). Over the years, the scope of MC has been extended, allowing for the evaluation of quantitative and probabilistic safety and performance properties (Baier et al. 2005).

In contrast with classical Model-Checking, which only verifies the presence of some particular scenarios, quantitative MC techniques permit to address questions such as:

1. what is the probability of undesirable events ?
2. how long does it take until the occurrence of undesirable events ?

First, the SMC technique (cf. Figure 3.7, inspired from Agha and Palmskog 2018) was introduced in (Younes 2004) to address the qualitative question of whether a property is satisfied with a probability greater than a threshold. Then, SMC has been generalized to answer various quantitative properties (Hérault et al. 2004). In particular, the SMC technique is based on simulations and can be seen as a tradeoff between the traditional testing techniques and the complete model checking (Broy et al. 2005). Concretely, the key idea behind SMC is based on two concepts:

1. Monitor a number of individual paths of the system behavior stochastic model.
2. Use statistical evaluation (e.g., hypothesis testing) to infer whether the property is satisfied with a certain degree of confidence over those paths. It should be noted that the resulting statistical confidence intervals depend on the number of investigated paths in the system behaviour. Hence, when tight confidence bounds are needed, a large sample size must be considered.

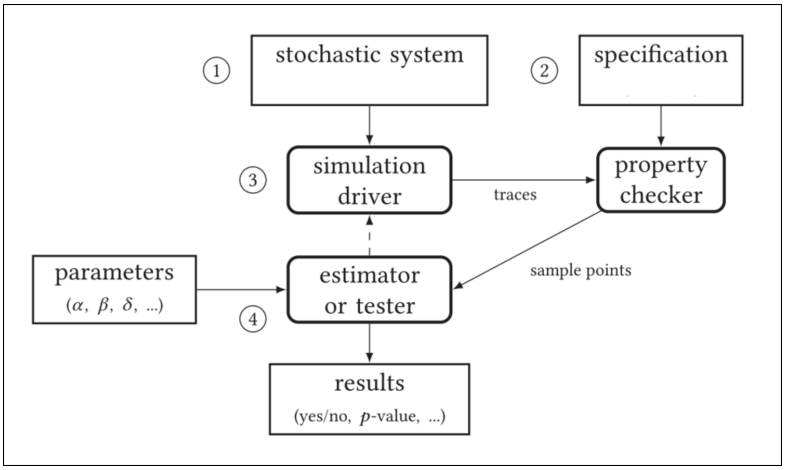


Figure 3.7: Schematic diagram of Statistical Model Checking (SMC) workflow.

In conclusion, the adoption of SMC techniques is particularly relevant when exhaustive state-space exploration is infeasible or not required if the results with a bounded error are acceptable. It has therefore been popularly deployed in a wide number of areas such as communication theory (Duflot et al. 2005) or cyber-physical systems (Kalajdzic et al. 2016). In particular, we can underline that the promising SMC technique has the potential to consider uncertainty aspects as those resulting from the use of GNSS receivers in a railway environment. Thus, such a technique will be further addressed in the rest of this thesis. Finally, complementary information on the diverse SMC technique applications can be found in the survey presented in (Agha and Palmskog 2018).

3.3.3 Use of advanced safety methods in railways

In the last decades, to meet new safety and performance requirements, more and more complex systems are developed in the different application domains. Safety-critical railway signaling systems have been no exception to this trend. Facing such a complexity, the safety requirements become even more stringent since railway safety is an indisputable variable that cannot be compromised. In this context, a continuous effort is directed towards the adoption of advanced safety methods in the railway domain. In this subsection, we present a number of works that fall within this context. In particular, this will allow us to highlight the remaining needs that are not covered in the literature and to better situate the contribution presented in this thesis with respect to relevant related works.

In order to underline the positioning of our contribution w.r.t. existing literature, the first relevant aspect to consider is the system addressed. In particular, three advanced ***railway control-command and signaling systems*** are identified : CBTC dedicated to urban guided transportation (ex. metro), CTCS and ERTMS/ETCS dedicated to regional and high-speed railway lines resp. in China and in Europe. On the one hand, most communication-based train control (CBTC) related contributions focus on the communication feature evaluation as it represents a crucial function, which is required for the proper functioning of the system (Mazzanti and Ferrari 2018; Comptier

et al. 2017). On the other hand, safety analysis of Chinese Train Control System (CTCS) can be found in (Li et al. 2015; S. Tang et al. 2018; T. Wang et al. 2018; Zhang et al. 2019). In this thesis, we address the train positioning function, as investigated in ETCS Level 3. Consequently, in the rest of this manuscript, we chose to focus on the relevant contributions dealing with the train localization within the ERTMS/ETCS.

From a ***methodological perspective***, we previously established that in light of the strict safety requirements in the railway sector, a long-standing effort concerns the use of formal methods and tools for analyzing railway signaling systems. In this context, one can specifically identify the contributions of (Basile, M. H. t. Beek, Fantechi, et al. 2018; M. H. t. Beek, Borälv, et al. 2019; M. H. t. Beek, Gnesi, and Knapp 2018; Boulanger 2014; Fantechi 2013; Fantechi, Ferrari, and Gnesi 2016; Qiu et al. 2014a; Qiu et al. 2014b; Gnesi and Margaria 2012; Ferrari, Fantechi, et al. 2013; Ferrari, Mazzanti, et al. 2020; Mazzanti and Ferrari 2018; Mazzanti, Ferrari, and Spagnolo 2018; Baouya et al. 2019). Besides, the reader can refer to the fairly recent survey in (Shift2Rail X2Rail2 2018), the more extended work in (Ferrari and M. H. t. Beek 2021) and (Ferrari, M. H. t. Beek, et al. 2019), which provided a mapping study describing the steps and tools related to employing formal verification methods in railways.

In a related context, it should be underlined that different ***subsystems*** have been investigated by means of formal methods. As highlighted in the survey presented in (Ferrari and M. H. t. Beek 2021), certain railway subsystems are more frequently treated in the literature. In particular, one can observe that the *interlocking subsystems* (Hartonas-Garmhausen et al. 2000; Zafar, Khan, and Araki 2012; James et al. 2014; Limbrée and Pecheur 2019; Linh Hong Vu, Haxthausen, and Peleska 2017; Linh H Vu, Haxthausen, and Peleska 2017; Bonacchi and Fantechi 2014; Winter 2002), and the *Level Crossing Control subsystem* (Mekki, Ghazel, and Toguyeni 2012; Huang, Weng, and M. Zhou 2010; Rehman, Latif, and Zafar 2019; Ghazel 2009; Ghazel and El-Koursi 2014; Ghazel 2017).

Yet, one can highlight here that the use of formal methods to investigate the deployment of GNSS in railway localization has not yet been adequately addressed in the literature. The contribution presented in this manuscript falls within this context. It represents a continuation of such an effort to adopt formal methods while addressing the impact of GNSS uncertainties on train positioning and railway performances.

With a particular focus on the ***quantitative studies in railway***, it can be noted here that a number of studies have considered quantitative assessment of safety and performance properties in railways while using Statistical Model Checking (SMC) (Guck 2017). For instance, (Cappart et al. 2017; Laursen, Trinh, and Haxthausen 2020) used SMC to verify the reliability of railway interlocking systems, while (Haxthausen and Hede 2019) focused on the study of railway timetables. Furthermore, (Basile, M. H. t. Beek, and Ciancia 2018) adopted the same technique to analyze a specific Moving Block railway signaling scenario.

In this context, it is reminded that Model-Checking makes it possible to accurately identify meaningful errors and provide strong guarantees for system correctness. Yet, it is worth recalling that the results obtained from the model-based approaches are obviously as good as the elaborated models are realistic, i.e., reflect the real behavior faithfully. Hence, the modeling activity remains a crucial phase in these approaches and is highly dependent on the user expertise, both in terms of modeling and system knowledge/ecpertise.

Therefore, numerous recent works focused on the ***modeling and analysis of ERTMS*** Hybrid

Level 3 with virtual fixed blocks (Abrial 2020; Arcaini, Kofroň, and Ježek 2020; Cunha and Macedo 2020; Dghaym et al. 2020; Hansen et al. 2020; Mammar et al. 2020; Tueno Fotso et al. 2020). Some other contributions focused on addressing the moving block principle (within ERTMS Level 3). In (Basile, M. H. t. Beek, and Legay 2020), a moving block signaling system endowed with autonomous driving is modeled and analyzed, while considering various driving strategies. In (Basile, M. H. t. Beek, and Ciancia 2018; Basile, M. H. t. Beek, et al. 2019; Basile, M. H. t. Beek, Ferrari, et al. 2022), the authors investigate specific MB scenarios by considering the ETCS on-board interface with the train localization unit, while abstracting away the specific localization functionalities based on balises or GNSS.

To the best of our knowledge, none of the studies that we can find in the scientific literature provides a comprehensive model-based approach that allows the use of formal methods to quantitatively assess safety and performance properties of GNSS-based train localization systems. In the following section, we address the existing works related to the use of GNSS-based systems in railway localization.

3.4 Analyzing GNSS-based systems in railway CCS: contribution proposals

Proposing a method to analyze the safety impact related to the use of GNSS systems in railway CCS still represents a challenge both for the academic and industrial actors. The contribution presented in this thesis falls in this context. The present section is dedicated to the description of the challenges related to the use of GNSS in the railway domain. Such a discussion further helps to position our contribution in relation to the GNSS-specific issues in railways, and w.r.t. existing related works.

3.4.1 Safety of GNSS-based systems

In this subsection, we give a brief overview of GNSS performance and safety-related metrics in addition to some existing works that tackle safety issues related to the use of GNSS-based localization systems in railways. In particular, we start by describing the various safety activities in the specific case of GNSS-based railway localization systems. Then, we expose the various parameters that are commonly used to characterize the performance and safety of GNSS systems. Finally, we focus on the analogy between the GNSS-related parameters and RAMS criteria previously presented, while pointing out a number of contributions that address such a link.

Safety activities in the case of GNSS-based railway localization systems

As stated earlier, the train localization function is a safety-critical function. Hence, railway positioning systems must undergo a certification process in order to be adopted in railway CCS systems (e.g., ERTMS/ETCS). Overall, such certification effort focuses on providing a set of evidences that endeavors to prove that the system fulfills the relevant safety and performance requirements. In compliance with the European railway regulatory and normative framework,

the safety activities related to the certification procedure are conducted according to the V-shaped life cycle process presented in Section 3.2.2 of this manuscript. In this regard, some existing works have intended to define safety requirements and allocate quantitative safety targets to the functional parts of satellite-based localization systems (Filip, Sabina, and Rispoli 2018; Filip, Rispoli, and Capua 2020). A preliminary apportionment of safety targets for Virtual Balise detection using GNSS in future evolutions of ERTMS was also proposed in Wullems et al. 2018. On the other hand, other contributions addressed the activities related to the demonstration of compliance with system requirements. In particular, some means to demonstrate safety performances of different technical architectures have been proposed in Lu, D. Tang, and Spiegel 2020; Nguyen, Beugin, and Marais 2015. Furthermore, the works of Beugin, Legrand, et al. 2018; Goya et al. 2018 focused on how to qualify hazardous positioning errors w.r.t railway safety criteria.

Nevertheless, it is important to notice that in the particular case of GNSS systems, the safety and performance of those satellite navigation systems are not expressed in terms of RAMS, but according to specific parameters related to the localization domain. In the following subsection, we will introduce these parameters.

Parameters for the characterization of GNSS systems

In contrast to the railway domain, where different European and national rules need to be applied, the satellites navigation parameters are defined by international avionic standards. Namely, the concepts of **accuracy, continuity, availability and integrity** are defined by the International Civil Aviation Organization (ICAO) to characterize the performance of satellite navigation systems. Based on the (Federal Radionavigation Plan. 2010) and (ICAO 2018) standards, the aforementioned parameters can be introduced as:

Accuracy is the degree of conformance between the estimated or measured position and/or velocity of a platform (ex., a vehicle) at a given time and its true position and/or velocity. The accuracy of a GNSS system is usually presented as a statistical measure of the system error.

Continuity of service is the capability of the system to achieve its function without unscheduled interruptions during the intended operation. More specifically, it represents the probability associated with the capability of the navigation system to provide a navigation output with the specified accuracy and integrity (cf. below) throughout the intended operation, assuming that the information was available at the start of the operation. Therefore, the occurrence of navigation system alerts (e.g., due to failures) constitutes continuity failures.

Availability (Service availability) of a GNSS system is characterized by the portion of time that the services of the system are usable. Hence, the availability is an indication of the ability of the system to provide reliable navigation information within a specified coverage area. It should be noted that the availability is dependent on both the physical characteristics of the environment, and the technical capabilities of the localization system.

Position integrity is the measure of the trust that can be placed in the correctness of the information provided by a navigation system. In addition, the integrity includes the ability of the system to provide timely warnings to users when the system should not be used for navigation. By analogy, the *Integrity Risk (IR)* refers to the probability of providing localization information that is out of some tolerance margin without warning the user in a given period of time. Besides, the estimation of IR is based on a set of parameters that are addressed hereafter:

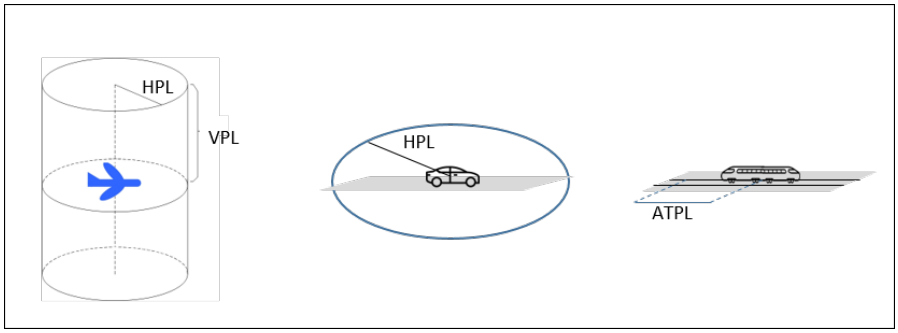


Figure 3.8: Protection Level (1D/2D/3D).

The first parameter is the *Position Error (PE)*, which is the difference between the measured position and the actual position (also known as ground truth). In relation with the PE, the *Alert Limit (AL)* is established to represent the largest position error that is allowable for safe operation. It particularly defines the error tolerance that cannot be exceeded without issuing a warning. Therefore, AL is considered as an application-dependent safety criterion. Nevertheless, it is not possible to know the actual position error during normal operation. Thus, a statistical bound, called *Protection Level (PL)*, is associated with the position error. Accordingly, the computed PL is associated with the risk that the alert limit is exceeded.

Recall that the GNSS was initially developed for avionic applications, and the ICAO standard distinguishes between two PL components: 1) *Horizontal Protection Level (HPL)*, and 2) *Vertical Protection Level (VPL)*. Concretely, the HPL provides a bound on the horizontal position error, while the VPL expresses the bound on the vertical position. It should be noticed here that the calculation of the horizontal component of the PL is sufficient for most land/maritime applications, since the position of users, such as cars or people, is restricted on the earth's surface. By adopting the same reasoning, as the railway track further constrains the train position, only a one-dimensional component of the PL, called the *Along Track Protection Level (ATPL)*, is needed. This magnitude can be determined based on the track description information (cf. Figure 3.8).

In practice, the expected nominal operation mode implies having a PE to be smaller than the calculated PL (cf. eq. 3.1 and Appendix E). Besides, the system is declared unavailable if the PL exceeds the AL value.

$$PE < PL < AL \tag{3.1}$$

In relation with the integrity concept, multiple integrity events or failure scenarios can be distinguished. In fact, before addressing the integrity failure concept, we should first introduce the related *Time To Alert (TTA)* parameter. Such a parameter defines the maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the equipment enunciates the alert. Accordingly, an integrity failure is an integrity event that lasts longer than the time to alert with no raised alarm within the TTA. Phrased differently, integrity events that either last for shorter than the TTA, or are detected within TTA (with corresponding alarm raised) do not constitute integrity failures.

In the following subsection, Finally, we will make the connection between these GNSS-related parameters and the RAMS criteria.

GNSS-related parameters vs. RAMS criteria.

The set of navigation parameters presented in the previous subsection allows for characterizing the performance of a GNSS positioning system, especially for aeronautical applications. Nevertheless, using these criteria in the context of a railway application is not straightforward due to the specific railway environmental constraints. As a result, railway safety stakeholders need to deal with interpretation issues regarding the adoption of navigation performance criteria in railway positioning. To overcome this issue, a number of studies have focused on the potential link between the specific criteria related to navigation and those associated with railway systems safety (RAMS). In particular, the works presented in (Filip, Beugin, et al. 2008; Beugin, Filip, et al. 2010; Beugin and Marais 2012; Lu and Schnieder 2014) revealed the existence of some analogy between these safety and performance parameters. Such an analogy can be synthesized as shown in Figure 3.9.

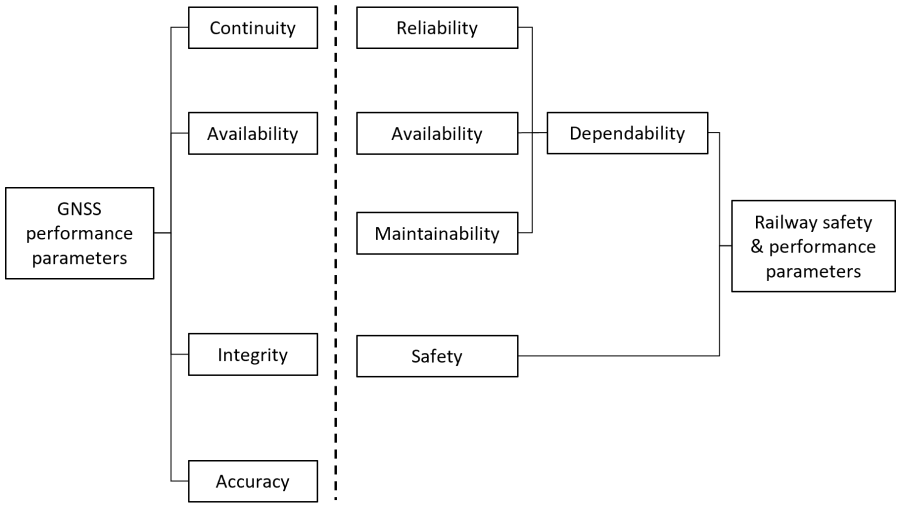


Figure 3.9: Analogies between GNSS and Railway Signaling safety and performance parameters.

In fact, the aforementioned studies have bridged the gap between the different concepts pertaining to navigation performance, on one hand, and railway dependability and safety, on the other hand. However, we should mention here that no study has yet provided a comprehensive process to reach the certification and deployment stage of GNSS systems for train localization due to the challenges encountered in the verification and validation activities. Hence, this issue remains a subject of research studies, currently.

3.4.2 Formal verification of GNSS related features

In this section, we aim to identify the features that we choose to focus on in our contribution. These features were determined in light of the discussions on the advantages and limitations of safety methods, combined with the identified issues related to the adoption of GNSS in the railway environment.

For instance, this grounding of methodology to be developed can be materialized through the selection of risk acceptance principles for risk evaluation and the adopted approach for

providing tangible evidence of compliance with system requirements.

Choice of risk acceptance principles for risk evaluation

As previously stated, the first activities of the life cycle process pertain to risk assessment. In this regard, a Risk Acceptance Principle (RAP) should be chosen prior to risk evaluation. In practice, three different principles can be adopted, namely:

1. the application of codes of practice.
2. comparison with similar systems.
3. explicit risk estimation.

All these principles are already recognized as possible practices in railway systems. Moreover, there is no priority on these principles. Besides, it is even possible to apply more than one principle at a time, depending on the system considered. As a result, the possibility of using one or more among these principles provides flexibility to decide which one is the most appropriate depending on the specific requirements of the project and the nature of the change affecting the railway system, to be examined.

Applying this first principle is not possible in the case of totally new systems, such as GNSS systems for railway localization. This is mainly due to the lack of feedback for such systems that involve important deviations from the existing code of practice. In contrast, achieving a comparison with a similar system may be applicable for new systems if an equivalent system already performs the functions involved. Therefore, this principle can a priori be adopted for investigating the use of GNSS-base train localization under ETCS-L3 operation, by referring to the localization function under ETCS-L2. However, although the final purpose of the train positioning function is the same, the risks generated by GNSS systems in the railway environment (e.g, risk related to multipath) cannot be assimilated to the risks covered in the current systems operating under ETCS-L2. Indeed, the localization function in ETCS-L2 is not subject to environment-related risks. Consequently, the adoption of the second principle alone is not sufficient in the case of GNSS-based railway localization, and must be complemented by other means. In fact, in this case where the hazards are not covered by one of the two aforementioned risk acceptance principles, the CSM regulation stipulates that the demonstration of risk acceptability shall be performed by explicit risk estimation and evaluation (i.e., third acceptance principle). Namely, the risks resulting from these hazards shall be estimated quantitatively and/or qualitatively, while taking existing and/or specified safety measures into account.

Moreover, the CSM-RA regulation (in its Section 2.5) discusses the situation in which the addressed system is a more cost-effective design that has not been experienced/deployed before. This situation is a typical example of a chosen design strategy that does not allow for using codes of practice or similar reference systems. This is typically the case for the introduction of GNSS on-board systems to reduce the costs related to the installation and maintenance of railway track equipment.

In conclusion, combining more than one principle is the most adequate option to deal with GNSS-based train positioning systems. Consequently, we chose to focus on the complementarity between the explicit risk estimation and the comparison with similar systems principles in the rest of this manuscript.

Adopted approach for providing evidence of compliance with system requirements.

The second set of activities in the life cycle process is pertaining to the demonstration of compliance with the system requirements, including performance and safety requirements. Such a demonstration relies on providing compelling pieces of evidence to support the claim that the requirements are met. With this aim, different approaches can be adopted.

- **Classical predictive approach:** the most traditional approach consists of employing the classical safety methods (presented in Section 3.3 of this manuscript) to support the expert's analysis. In particular, some methods such as FTA can take information such as predicted failure rates as input parameters and combine them according to the defined system architecture. The resulting calculation provides pieces of evidence on the compliance of the system with the specified requirements, based on the predicted performance and safety of the system. However, it should be noted that the system architecture is a major input parameter for those classical approaches. Yet, as the combinations of multiple sensors are still under investigation for on-board train localization, the final architecture of the GNSS-based train localization system is not defined. Furthermore, as most of those classical predictive methods are static, it is very challenging to provide persuasive evidence on the impact of the interaction of the system with its environment (e.g., performances of GNSS in dynamically changing environmental conditions). More importantly, predictive analysis mainly focuses on system component failures. Therefore, properly analyzing the effects of aspects that are not only related to the components of the systems (e.g., GNSS signals perturbation in space leading to multipath) remains a challenging issue when adopting such classical methods (Beugin and Marais 2012).
- **On-site testing:** In contrast with the classical predictive approach, on-site testing constitutes an alternative approach that allows dealing with the system-environment interaction. From an operational perspective, two possible observation conditions can be distinguished (Beugin and Marais 2012):
    1. A specific route is followed by a train equipped with a GNSS receiver. The evaluated characteristics are therefore only relevant to this train itinerary. Accordingly, the GNSS-based localization performance results represent average properties characterizing all the environment configurations encountered along the train route. Therefore, this approach does not permit to highlight particular places with poor visibility conditions, but provides a global GNSS performance characterization for this railway line.
    2. The environment configurations along the train itinerary present similar or comparable geometry conditions. In this case, the area around this train itinerary can be considered as a *"typical"* railway operational environment (or class). Thus, the results obtained provide a representative characterization of the typical environments observed.

Nevertheless, both observation conditions show limitations in covering the variations that may occur in the environment along the track over time. Non-exhaustively, it should be highlighted that the GNSS satellites are not stationary, thus, the exposition of the GNSS receiver to satellites and the GNSS-signals reception conditions differs from one moment to another (and so are the GNSS-based positioning performances). Furthermore, other kinds of variation, such as the appearance of new buildings in urban areas or the seasonal evolution of the vegetation, are additional causes that may alter the relevance of the obtained results Consequently, it can be concluded that a major drawback is that operational testing and analysis approach can only

show the presence of errors but does not demonstrate their absence. In other words, the non-occurrence of an "error" during a test campaign does not guarantee that no errors would occur in future situations, thus, limiting the efficiency of such methods in considering rare-event.

Moreover, since the associated safety target and specifications are very high for safety-critical railway systems (e.g., Tolerable Hazard Rate value of 10^{-9} for SIL4 functions), a tremendous amount of testing effort is needed to obtain a significant and trustworthy outcome allowing to reach an acceptable statistical conclusion about the system safety. Furthermore, the results obtained from a specific testing context depend highly on the environment in which the tests are conducted and cannot be generalized to different operational contexts. Knowing that, in the railway domain, the setting of an experimental testing environment is generally costly, the diversification of the testing configurations is often quite limited. As a result, it is awkward to study different contexts when adopting on-site testing for safety analysis.

In conclusion, even if on-site testing benefits from a great power of conviction and persuasion, the adoption of such an approach can show to be expensive and time-consuming. Thus, complementary and more effective analysis methods have to be adopted in order to reduce the number of tests required, especially during the early system design phases.

Zero on-site-testing approaches

To overcome the limitations of the previously presented on-site testing approach, the adoption of techniques that are based on models and simulations, and which do not require on-site testing, has emerged as a promising complementary alternative. In particular, the advanced model-based methods presented in Section 3.3 fall within this context. In fact, when dealing with GNSS-based train localization systems, the adoption of zero on-site testing methods paves the way to analyze different configurations and environments without the need for significant resources. It is then straightforward that such model-based approaches offer significant gains in terms of time and cost, in particular, compared to on-site testing. In addition, the use of rigorous mathematical demonstration (namely, formal methods) allows for providing tangible and highly persuasive proofs. This feature is of paramount importance when dealing with a safety-critical function such as train localization (Z. Peng et al. 2016; Lu and Schnieder 2014). Moreover, adopting such automatic verification techniques permits a more exhaustive analysis, compared to human expert-based provisional methods.

Based on the discussions above, we propose in the rest of this thesis to combine the results obtained from *On-site testing* (which are strongly dependent on the environmental testing conditions) with *'zero on-site testing approaches'* (based on models and simulation) in order to investigate safety features in relation with GNSS-based railway localization, while making it possible to examine different configurations and environments.

System analysis level and evaluation parameters

Before studying the performance and safety aspects of GNSS-based train localization systems, two further aspects should be considered. Namely, the relevant parameter to consider for the system evaluation and the system level at which the analysis should be conducted.

As previously discussed in Section 3.2.2, an important part of system requirements is pertaining to the RAMS indicators. Those parameters are adequate to represent the performance and safety of material components. However, when dealing with GNSS-based systems, the

RAMS parameters show limitations in covering some specific aspects related to the degradation of satellite signals (e.g., due to multipath scenarios). In particular, such effects do not result from the failure of a hardware component (e.g., a GNSS receiver), but are dependent on the environment in which the system evolves. Accordingly, it is for instance difficult to associate a failure rate with such a phenomenon.

On the other hand, the studies related to the GNSS domain usually consider the GNSS receiver as an isolated piece of equipment. However, to overcome the limitations related to GNSS signal perturbations, hybrid architectures combining GNSS receivers with other types of sensors, such as the IMU, are more likely to be adopted for train localization.

In this context, the study presented in (Legrand 2016) focused on the position integrity/safety integrity link, as a potential evaluation parameter for hybrid GNSS systems to be used for railway. In particular, such a link, which is strongly dependent on the quality of the integrity control mechanism employed, is the most relevant parameter to consider from a safety point of view. Yet, it should be noted that alternative metrics can be proposed in the rest of this thesis to investigate further specific aspects.

The second aspect to consider is the analysis level at which the study should be conducted. Not surprisingly, most contributions in the literature address the train positioning problem at a component level. This is mainly related to the considered evaluation criteria, as both RAMS and navigation parameters are associated with equipment performances. However, in the particular case of GNSS-based train localization, the ETCS on-board and trackside subsystems are tightly linked. Therefore, in the methodology presented in this thesis, we advocate for conducting our analysis at a system level. This choice is particularly relevant to help consider the railway environment conditions and their impact on the train localization performance. Moreover, considering the subsystem which is responsible for the train localization as a black box allows for overcoming the particular obstacles inherent to the various technological architectures. Hence, it becomes possible to address the GNSS-based positioning performances independently from the employed technological solutions (ex., sensors hybridization).

3.4.3 Discussion on the used modeling formalism

Along this chapter, we presented a set of existing safety techniques and methods. We provided discussions regarding the limitations of those existing approaches when addressing complex systems. Namely, it has been established that both 'classical predictive analysis' and 'on-site operational testing' methods show limitations when dealing with GNSS-based train localization systems. Thus, we identified the emergence of formal verification methods as alternative means that can bring a substantial added value towards tackling the limits that we have pointed out. In this section, we provide an insight on some examples of formal notations that are commonly employed to depict and and analyze the behavior of safety-critical systems. In particular, two categories of systems' modeling notations can be distinguished. Namely, textual and graphical models. The former is based on a rigorously defined textual syntax to translate the system behavior. However, such a representation is quite challenging when dealing with complex systems. Besides, textual representation is prone to errors, especially when several people perform the modeling task. Moreover, textual representations do not constitute a convenient communication means between the various stakeholders involved in a project (designers, developers, testers, ISA, etc.). Consequently, the adoption of more intuitive graphical representations, such as Petri Nets and Finite State Automata (cf. Figure 3.10), is highly recommended to represent complex systems.

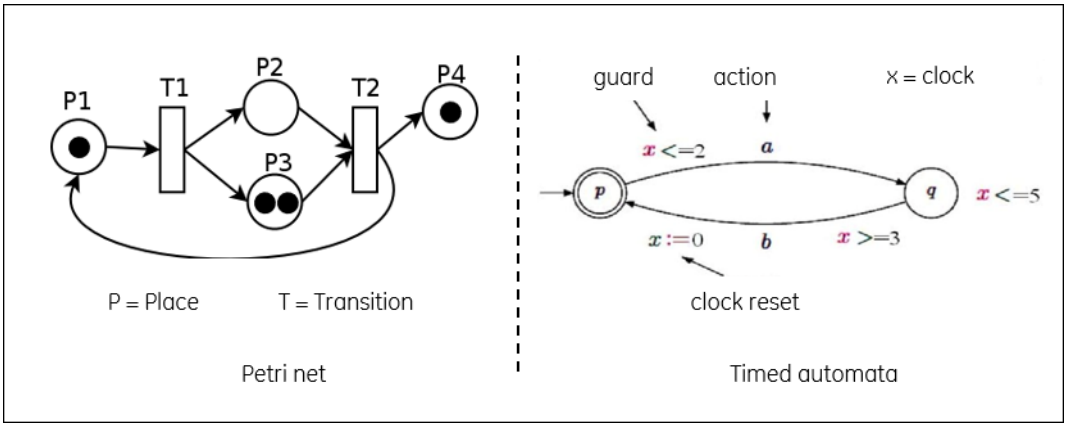


Figure 3.10: Example of Petri Nets and Timed Automata formal models

The *Petri Net (PN)* formalism was initially introduced by *Carl Adam Petri* in his thesis (Petri 1962) as a modeling solution allowing to represent discrete event control systems. Through the years, PNs have been extended to enhance their expressiveness. As a result, different variants, such as Colored Petri Nets (CPN), Stochastic Petri Nets, Time/Timed Petri Nets have emerged as powerful modeling solutions for complex systems, (Peterson et al. 1980; Cost et al. 1999; Liu et al. 2002; Jensen 1997; Jensen 2013; Jensen and Kristensen 2015), (Molloy 1982; Marsan et al. 1998; Hirel, Tuffin, and Trivedi 2000; Balbo 2000; Bause and Kritzinger 2002), (Ramchandani 1973; Jiacun Wang 2012). Furthermore, Petri Nets have been widely adopted in the industry (Zimmermann and Hommel 2003; Zimmermann and Hommel 2005; Barger, Schön, and Bouali 2009; Hörste, Hungar, and Schnieder 2013; Banik and Ghosh 2013; Ghazel 2009; Wu and Schnieder 2016; Vanit-Anunchai 2018; Cavone, Dotoli, and Seatzu 2017; Mazzanti, Ferrari, and Spagnolo 2018; Ferrari, M. H. t. Beek, et al. 2019).

On the other hand, *automaton-based models* are state-transition diagrams that define the behavior of a system through a set of states L and transitions between these states. The set of active states characterize the system at that specific point, while the transitions indicate how the system evolves from one state to another.

Depending on the dynamics to depict, different automaton formalism can be adopted. In fact, the elementary automaton theoretic framework consists of *Labeled transition systems (LTS)*, which is suitable to capture non-deterministic choices. In the same way as for PNs, different variants of automata can be found. For instance, *Markov* automata (or Markov chains) are suitable when dealing with random aspects. Concretely, *Markov Automata (MA)* are state/transition diagrams that support non-determinism and probabilistic transitions. Thus, various investigations can be conducted on the basis of MA, regarding reachability, likelihood of some particular scenarios, etc., (Guck 2017). *Timed Automaton (TA)* have been developed to make it possible the modeling of some real-time features. A TA is a finite automaton extended with a set of real-valued clocks. The *clock* variables are initialized with zero and progress synchronously during a run of a timed automaton, hence, allowing to keep track of the time. Moreover, clock values can be compared to integers and used as constraints to restrict the possible behavior of the automaton. For that, *clock guards* are put as enabling conditions over the transitions, and *clock invariants* are used to enforce the deadlines over locations. Along with the model transitions, each clock variable can be reset individually.

It is important to notice that, besides the intuitive graphical automaton representation, such a formalism is based on rigorous mathematical concepts. In particular, a timed automaton can formally be defined as the tuple $\mathcal{A} = \langle \Sigma, L, L_0, \mathcal{C}, F, E \rangle$ where:

- Σ is a finite set of **actions**, also called **alphabet** of $\mathcal{A}$,
- L is a finite set. The elements of L are called the **locations** or **states of** $\mathcal{A}$,
- $L_0 \subseteq L$ is the set of **initial** or **start** locations,
- $\mathcal{C}$ is a finite set of **clock** variables,
- $F \subseteq L$ is the set of accepting locations,
- $E \subseteq L \times \Sigma \times \mathcal{B}(\mathcal{C}) \times \mathcal{P}(\mathcal{C}) \times L$ is a set of edges, called **transitions** of $\mathcal{A}$, where:
  - $\mathcal{B}(\mathcal{C})$ is the set of clock constraints involving clocks from (C),
  - $\mathcal{P}(\mathcal{C})$ is the powerset of $\mathcal{C}$ (i.e., $2^{\mathcal{C}}$).

  Accordingly, the edge $(l, \sigma, g, r, l') \subseteq E$ represents a transition from location l to location l' taking the action σ. Such a transition can only be taken when the corresponding clock constraint g is true. Finally, the set $r \subseteq \mathcal{C}$ defines the clocks to be reset within this transition.

Over the years, further extensions of these timed automata models have been developed, allowing to address more advanced features. For instance:

- *Priced timed automata (PTA)* are TA models with additional modeling features in the form of costs. Such formalisms have been adopted to study resource-optimal reachability problems (i.e., the minimum cost to reach the goal location) (K. Larsen et al. 2001; Behrmann, Fehnker, Hune, K. Larsen, Pettersson, and Romijn 2001; Behrmann, K. G. Larsen, and Rasmussen 2004; Behrmann, Fehnker, Hune, K. Larsen, Pettersson, Romijn, and Vaandrager 2001; Basile, M. H. t. Beek, and Legay 2020).
- *Stochastic timed automata (STA)* are TA models with extended semantics to define a purely stochastic process. In this context, the STAs are TA augmented with both the sojourn time probability density function, and a probability mass function over the enabled transition. The automaton model evolves following a random delay and choosing a random edge among the enabled ones from the active model location (Bertrand et al. 2008; Avram et al. 2018).

In contrast with Petri Nets, a key advantage related to the adoption of automaton formalism is their inherent compositionality (i.e., a large model can be constructed from smaller ones). Hence, such a feature permits a modular representation of complex systems through their decomposition into subsystems. Furthermore, each sub-model can be extended, allowing to address the system complexity gradually.

As will be discussed in Chapter 4, we will adopt an extension of TA in our work, namely *UPPAAL TA*.

Tools supporting the formal verification technique

One can notice that several tools have been developed to implement the formal verification technique. Some of them have gained wide popularity. For instance, *NuSMV* is a model-checking tool that allows for performing the analysis based on symbolic representations of the system state

space as Binary Decision Diagrams (BDD) (Cavada et al. 2010). The *CPN-Tools* is a commonly used tool adapted to the modeling and analysis of colored Petri Nets. We should also highlight that there exists a variety of tools that implement the SMC techniques (cf. Agha and Palmskog 2018), such as the PRISM probabilistic model checker (Kwiatkowska, Norman, and Parker 2011). The *UPPAAL SMC* model checker, which permits to take extended timed automata models as input (David et al. 2015) will be presented and used in the following chapters of this thesis (see Part 2).

3.5 Chapter conclusion

In the previous chapter, we presented the real stakes behind adopting GNSS-based train localization and we discussed the main relevant technical issues related to implementing such an embedded positioning function. Besides, it has been pointed out that a significantly challenging issue in this regard is related to the assurance of operational safety when using GNSS systems in a railway environment. In the present chapter, we first presented the European-specific regulatory and normative framework related to railway safety. In particular, the overview of the most relevant regulations and standards allowed us to list the various safety activities to be conducted along the system life cycle in order to provide a compelling safety demonstration.

With the aim of conducting such safety-related activities, different approaches and methods can be employed. Thus, the second section of this chapter was dedicated to the review of the common safety methods available in the literature. In particular, it has been argued that traditional safety methods show limitations when dealing with complex and dynamic systems. Thus, they need to be completed by employing advanced model-based approaches. We then dedicated a part of this chapter to discuss the peculiarities that are related to the safety and performance issues for GNSS systems. Finally, we listed some modeling formalisms that are relevant for the contribution that will be discussed in the remainder of the manuscript. Furthermore, numerous contributions from the state of the art, which are related to our work were presented all along this chapter to allow a better understanding of the global scientific context in which this work is conducted. In particular, it should be highlighted that a thorough focus needs to be put on the verification and validation activities, as those tasks are particularly challenging when addressing the GNSS-based train localization.

In the light of the conclusions drawn throughout this chapter, the second part of this manuscript presents our contribution about the elaboration of a model-based approach that serves as a basis for quantitative safety evaluation of GNSS-based railway localization.

Part II

Contributions

Chapter 4

Formal Model-Based Approach to Address the GNSS-based Train Positioning

Outline of the current chapter

4.1 Introduction

The first part of this manuscript allowed us to provide an insight into the background and the safety issues related to the deployment of GNSS-based localization solutions in railway CCS. Most importantly, it has been concluded that the currently adopted safety analysis and demonstration approaches do not efficiently manage the verification and validation process w.r.t safety when dealing with such a complex system. Therefore, we proposed to investigate an adapted formalism to establish a new methodology that is able to tackle the lack of safety evidence. This chapter introduces a new approach based on employing formal methods to address safety and performance properties, while considering GNSS-based train localization.Concretely, we focus on a model-based analysis of the train localization process using GNSS-based solutions. In particular, we seek to finely and rigorously investigate the localization uncertainties induced by the use of VBs in railway CCS. Namely, even if the characterization of these uncertainties is out of our scope, our objective is to faithfully represent their impact on the localization performance, through the proposed formal model, and relying on various parameters. In this way, we can assess how well (from a probabilistic perspective) the safety requirements are fulfilled in a railway operation context where VBs are used for train localization. We should also mention that the elaborated models intend to be as generic as possible to allow for coping with different operational configurations. Hence, this chapter also discusses model adaptability, incrementalism, and reusability.

The sequel of this chapter is organized as follows. Section 4.2 focuses on presenting the ingredients and the key features of the proposed methodology. In particular, various aspects pertaining to the implementation of the model-based approach are addressed. Besides, the set of relevant resources to be investigated prior to the model development are discussed in this section. Then, Section 4.3 provides an in-depth presentation of the formal model development task. Such a model is elaborated in a modular and parametrizable manner to expand its potential utilization. Accordingly, Section 4.4 finally explores how various input parameters should be set in order to adapt the model instantiations. In particular, such model adjustments should permit addressing specific operational conditions.

4.2 Ingredients and key features of the proposed methodology

The proposed methodology aims at verifying different safety and performances properties. The core part of our methodology corresponds to the formal model that is intended to integrate nominal/degraded/operational-related behaviors of the GNSS-based train localization function. Moreover, the set of activities around the model are also considered as part of the methodology (an overview of the proposed method is shown in Figure 4.1). Accordingly, the next three subsections will address the three ingredients of our methodology, and their specific key features:

- the prerequisites to build the model, namely the different resources, inputs, and information supporting the model elaboration (i.e., how to gather the required information to build the model),
- the targeted features that the model has to fulfill in order to manage the complex behavior of the localization function (i.e., the model features),
- the formal method endowed with an adapted tool able to analyze the model w.r.t the defined objectives, i.e., how the model will be employed.

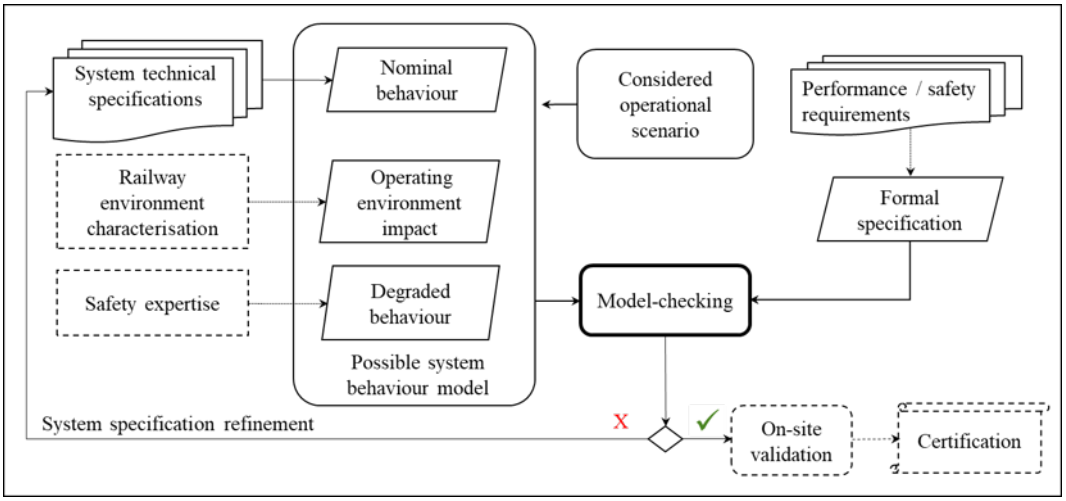


Figure 4.1: Overview of the proposed method

4.2.1 Prerequisites to build the model

Since the outcomes of our model-based approach are as good as the developed models are, it is straightforward that the system modeling phase is of paramount importance in the whole process. Namely, it is crucial that the elaborated models faithfully reflect the actual behavior of the system in the model. With the aim of adequately performing such modeling activity, a set of relevant resources needs to be employed. Namely, the system technical specifications provide valuable information permitting to represent the nominal system behavior. On the other hand, the accurate representation of the environmental conditions in which the train evolves remains a key aspect that needs to be considered carefully when dealing with GNSS-based localization solutions. Therefore, the present approach should include the results of the projects (cf. the introduction section) that have dealt with the railway environment characterization, from a GNSS localization perspective, as an additional input parameter. Besides, the appropriate user expertise, both in terms of system knowledge and modeling, prevails as a fundamental prerequisite conditioning the proper implementation of the proposed approach. Non exclusively, such expertise particularly affects the representation of the system degraded behavior, and the identification of the relevant operational scenarios to be investigated.

4.2.2 Targeted features of the developed model

Model re-usability

as discussed explained in the manuscript, the GNSS-based train localization system is a complex system including various interacting elements. Moreover, multiple technical implementations of on-board railway localization solutions are still investigated. Consequently, no final system architecture is yet defined. Hence, it is crucial to think about the re-usability of the models involved in the methodology.

Modular representation of the system behavior

We opt for a modular approach that helps tackle the system complexity issue and permits for an incremental representation of its behavior. Concretely, the modular aspect consists in developing a number of *generic* modules to translate specific features of the system. The composition of *instances* of the individual modules provides a representation of the modeled system behavior. Moreover, the developed module can easily be refined and extended iteratively in the future to represent more advanced details, without impacting the other modules. As a consequence, the system complexity can be tackled gradually, and different (heterogeneous) features can be represented separately in the model, and various (performance and safety-related) properties can be evaluated.

Address temporal and probabilistic aspects

Beyond emulating the system behavior, the objective pursued via the model-based approach is to check a number of properties related to the train localization function. In this context, one can note that such properties typically involve temporal and probabilistic aspects. Consequently, these features should be supported in the chosen notation for our modeling activities.

Support the representation of dynamically changing parameters

Since the properties related to the GNSS-based localization function are highly dependent on the dynamically changing reception conditions. Besides, these reception conditions variate significantly according to the rail environmental conditions. Such as should, hence, be considered in our modeling activities.

Parameterization

In this respect, the modeling process should permit addressing a set of different configurations and operational scenarios. To this aim, the generated models need to be associated with a number of adjustable input parameters, enabling to examine various configuration setting with a minimum of effort.

4.2.3 Formal method and adapted tool

Along with the system behavior modeling task, the third key activity pertains to the adoption of the model-checking technique. It consists in formally expressing the set of properties to be investigated. Concretely, such properties need to be formulated as temporal logic assertions. Subsequently, the execution of particular algorithms should permit verifying whether the property is satisfied. If the investigated property does not hold, the verification engine automatically provides a counter-example. In particular, such evidence illustrating the behavioral sequence (run) leading to the violation of the verified property constitutes a substantial support for the model debugging activities. In addition, the employed model-checking algorithm should be able to provide both qualitative and quantitative results to further expand the scope of potential applications. When the modeled system behavior is finally deemed to satisfy the investigated properties, a number of identified relevant test cases can be addressed by means of on-site validation to provide complementary evidence, for the safety demonstration process.

Choice of an adapted formal modeling and verification tool

Keeping in mind the set of conditions to respect in order to properly implement the approach presented in this contribution, an adapted tool has to be chosen. In this regard, we propose to investigate the *UPPAAL* model-checking tool (Behrmann, David, and K. G. Larsen 2006). *UPPAAL* is an integrated environment for modeling, validation, and verification of real-time systems modeled as networks of timed automata. In particular, *UPPAAL* combines an intuitive graphical representation of the model with simulation facilities and various MC algorithms. Concretely, a model in *UPPAAL* consists of a network of interacting components (Timed Automata modules). To generate such a Networks of Timed Automata (NTA), the individual TAs communicate via binary and broadcast channels, as well as shared variables. Accordingly, the actual behavioral model is generated as a product of timed automaton models instantiated from these template modules. Moreover, each of these templates is associated with an independent declaration section permitting to set a number of input parameters. Hence, it makes it possible to establish modular and parametrizable models. Furthermore, time representation is addressed (in the automata formalism supported by *UPPAAL*) through a set of clock variables represented in the model. These clocks evolve in parallel and can be reset via update instructions. In contrast, the model defines a global system clock that is never reset to monitor the model reference time. However, basic timed automata models present expressiveness limitations to encompass the behaviors of complex cyber-physical systems (e.g., train GNSS-based positioning). In fact, the continuous-time behaviors of those systems often rely on complex dynamics and stochastic behaviors. Hence, the model checking problem for such systems remains undecidable, and approximating those behaviors with timed automata was, for a long time, the only possible option (Henzinger and Ho 1995).In this context, (David et al. 2015) introduced the *UPPAAL SMC* as an enriched version of the *UPPAAL* tool that proposes an alternative solution to the time representation problem. In particular, *UPPAAL SMC* makes it possible to model systems via networks of automata whose behavior may depend on both stochastic and non-linear dynamical features. Concretely, each component of the system is described with an automaton whose clocks can evolve at various rates. By default, the rate of a clock is set to 1. Yet, such rates can be specified by modifying the value of the primed (') version of the clock (e.g., $c' == 3$ denotes that the clock 'c' with a rate of 3 evolves three time faster than a default clock). Accordingly, ordinary differential equations can also be used to describe more particular clock behavior (e.g., ${c_1}' == c_1 \times c_2 + c_3$, where c_1, c_2, and c_3 are three clock variables). Besides, it should be noted that to model an n-degree derivative, one can use a clock variable for every intermediate derivative. For instance, instead of modeling $y'' == -9.81$ for a falling object, one should declare $y' == v$ and $v' == -9.81$.

On the other hand, the *UPPAAL* tool further extends the TA formalism with specific urgent (no elapsed time) and committed (meaning that the state shall be exited before any interaction occurs) model-locations, marked with the symbol ('U') and ('C'), respectively. In particular, time is not allowed to pass when the TA is in such locations.

Finally, in terms of verification, it is worth noticing that *UPPAAL* includes a model-checking engine that allows the evaluation of various types of properties expressed as temporal logic assertions. Besides, *UPPAAL* offers simulation facilities that can be advantageously used for both modeling and verification phases.

4.3 Modeling of the behavioral aspects related to train positioning

In the modeling phase of our methodology, among other objectives, we aim to establish a formal model to represent the aspects related to the GNSS-based localization function. In fact, the underlying idea is to set up a modular approach that can be employed to address various functional architectures and operational contexts. Accordingly, we seek for representing an abstraction of the system behavior with a particular focus on the relevant features that are related to the train localization aspect. In this context, it is important to identify the main relevant aspects to be modeled. Accordingly, we choose to particularly focus on the following features:

1. Modeling the train dynamics as it moves on the rail line, i.e., representing the measured train position and speed to be updated according to a set of parameters.
2. Modeling the evolution of the train position error bound, i.e., the continuous evolution of the maximal position error permitted according to the measured traveled distance.
3. Modeling the activation of physical and virtual balises by the train as it moves along the line.
4. Depicting the localization error when a PB or a VB is encountered. Concretely, this induces a punctual down jump of the error bound due to the resetting function, while the corresponding residual error is kept.

In what follows, we introduce a set of automata modules that we developed to represent the above-mentioned features.

4.3.1 Model of the train dynamics

Real dynamic variables and associated issue

To represent the behavior related to the train position, we first intend to address the dynamics of the trains as they run on a rail line. Accordingly, the present subsection introduces the various steps to translate the desired behavior throughout the *UPPAAL* formalism. Concretely, the approach consists in considering the value of the train acceleration as a variable in the model. In particular, the variations of the train speed following the different acceleration and braking phases can be represented accordingly. With this aim, the integral mathematical function is employed to infer the instantaneous speed of the train. Likewise, the relative distance traveled by the trains can easily be estimated from the calculated velocity. For this purpose, various modeling features provided by the Uppaal tool are employed to represent the train accelerations, speeds, and relative position. Broadly speaking, the supported hybrid clock variables are employed in the following of this contribution to translate the basic ordinary differential equations defining the above-mentioned physical relations. For instance, the acceleration can mathematically be defined as the derivative of the velocity with respect to time (see equation 4.1).

$$a = \frac{\mathrm{d}v}{\mathrm{d}t} \tag{4.1}$$

Similarly, the velocity represents the variation rate of the position with respect to time (see equation 4.2).

$$v = \frac{\mathrm{d}x}{\mathrm{d}t} \tag{4.2}$$

By making use of the Uppaal hybrid clock variable type, the above relations can be expressed using the notation presented in the equation 4.3, and represented in the automaton model as illustrated in Figure 4.2:

$$V' == A \;\&\&\; P' == V \tag{4.3}$$

Where:

- P denotes the relative position of the moving train.
- V represents the train speed.
- A is the acceleration value of the train.

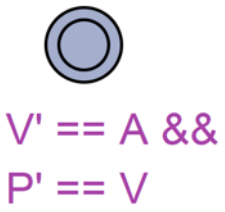


Figure 4.2: Ordinary differential equations as Uppaal model-location invariants.

Adopting such a representation makes it possible to emulate and continuously monitor the train traveled distance and velocity according to the associated acceleration value. Nevertheless, a drawback inherent to the Uppaal tool is that such double-precision type variables (i.e., floating-point variables) are only supported to monitor *'costs'* (such as in UPPAAL CORA extension for cost optimal reachability analysis) over the model evolution, and should not affect the control of the automaton. In other words, the model-checking algorithms implemented within Uppaal do not support double-type variables in transition guards or location invariants. In fact, in the current Uppaal SMC algorithms, the hybrid clock values are neglected and cannot influence the evolution of the verified models (i.e., deemed as inactive variables). When addressing the particular case of the train localization function, it is obvious that the train position is a key element impacting a number of relevant aspects represented through the model. Moreover, the execution of various functions such as balise activation is conditioned by the value *'P'* of the train position parameter. Accordingly, we propose to adopt complementary integer type variables to represent the train dynamics, by discretizing the continuous variables and, hence, overriding the aforementioned tool limitations.

Considering integer dynamic variables

With this aim in mind, we define the integer variable P_{int} and V_{int} as discretized variants of the double type variables denoted by P_{dyn} and V_{dyn} to represent the train relative position and velocity, respectively. The obtained model is shown in Figure 4.3. In this automaton, functions $ComputeA()$, $ComputeV()$ and $ComputeP()$ associated with the reflexive transition on location $MovingTrain$ allow for updating the train acceleration, velocity and position values.

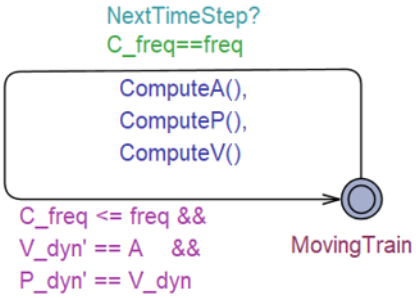


Figure 4.3: Train dynamic module including integer variables

Accordingly, we introduce a new automaton module to manage the proper incrementation of the integer variables. Concretely, the module behavior consists in repetitively firing a specific transition at regular time steps. Besides, the involved transition is associated with a broadcast transmitting channel variable that ensures the synchronization of various communicating modules. Consequently, the parallel evolution of the receiving modules can be timely controlled, permitting the update of the integer variables according to the defined execution frequency (see Figure 4.4).

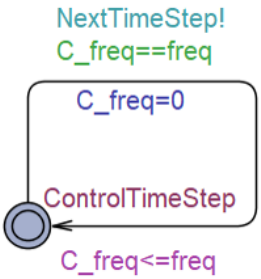


Figure 4.4: Modeling of repetitive time controlled operations (discrete time step synchronization module)

In this regard, since we assign an invariant $C \leq freq$ to location $ControlTimeStep$, and given that a guard $C == freq$ is associated with the reflexive transition on that location, this transition is activated precisely when the guard is satisfied (i.e., when the clock $'C'$ reaches the $'freq'$ parameter). Thus, such a transition allows for implementing periodic operations carried out every period of time $'freq'$.

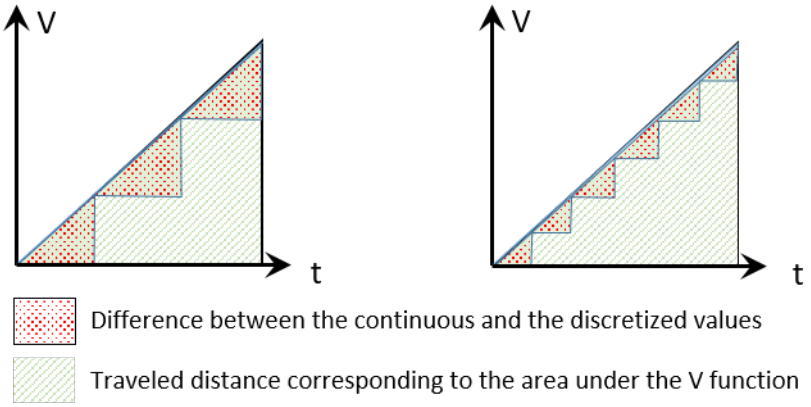


Figure 4.5: Illustration of the impact of different time discretization values on the deviation between continuous and discrete variables

Yet, we underline that such a representation mechanism may result in a deviation between the values of discrete and the continuous variables. Indeed, the deviation is mainly due to the delay related to the iterative update of the integer variables (see Figure 4.5). Therefore, one must be particularly mindful of the fact that the integer update function has to be executed following an adapted frequency. Namely, relatively small time steps (e.g, 100 *ms*) are adopted to define the periods of the update operation and keep the deviation relatively small to tackle the impact of such approximations in the whole analysis.

States of the dynamic of a moving train

Having addressed the representation of the train speed and relative traveled distance throughout integer type variables, we propose distinguishing between three states in the dynamic of a moving train. Such a distinction is performed depending on the acceleration of the train. Namely, we obtain:

- The train is in its acceleration phase (i.e., $A > 0$)
- The train is running at a constant speed (i.e., $A = 0$)
- The train is breaking (i.e., $A < 0$)

Accordingly, three distinct locations are set in the train-dynamic module and associated with invariants related to the acceleration parameter (see Figure 4.6). Besides, we should mention that the speed and relative position are computed/updated in a similar way at each of the three locations.

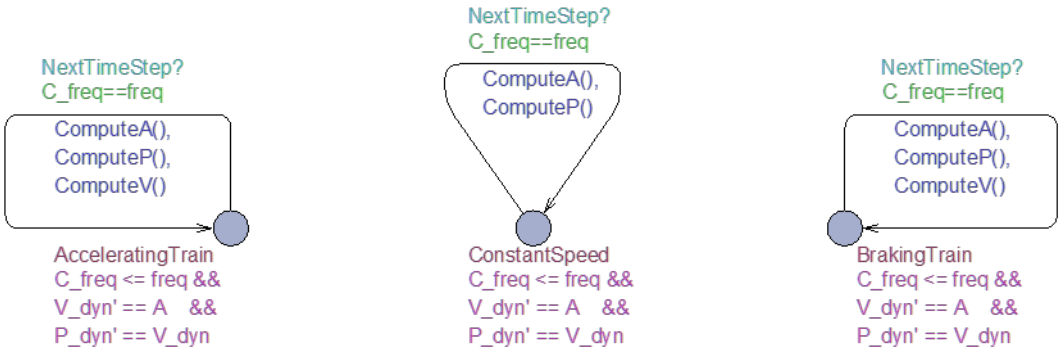


Figure 4.6: Representation of the three distinguished statuses of the train dynamics

Naturally, the following step of the modeling process consists in defining the specific conditions that will permit the evolution of the train-dynamics from one model-location to another. With this aim, a new variable denoted $'V'_{target}$ is introduced as an input parameter of the model (in the declaration part of the model). In fact, this variable represents the speed at which the train is expected to run all along the rail line. In particular, the use of such input allows us to address a set of relevant aspects, including the various speed limitations pertaining to the line configuration and the specific acceleration and braking instructions received by the train during its journey. Accordingly, the train target speed is periodically compared to the current train speed (at the same time as the position, velocity, and acceleration are computed). Depending on the comparison results, the value of the acceleration parameter is adapted when needed. Moreover, Boolean type variables denoted $'Brake'$ and $'Accelerate'$ are updated consequently and used as guards conditioning the transitions between the different model-locations of the module. For instance, let us consider a train running at a constant speed. If the current train speed is deemed different from its target speed, the train acceleration parameter is adapted, and the aforementioned boolean guards are updated accordingly. Hence, the train-dynamics module evolves following the corresponding transition (see Figure 4.7).

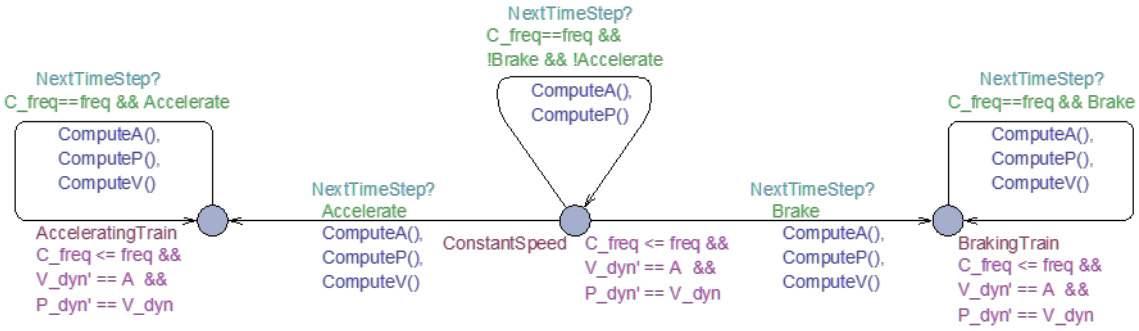


Figure 4.7: Representation of the transitions allowing for exiting the steady-state model-location in the train dynamics module

Comparably, the transitions toward the constant speed location are activated when the train running speed matches the target speed. For instance, let us assume that the train target speed is set to $0km/h$ (standstill) following the reception of a brake instruction. In this case, the model-location denoted $'BrakingTrain'$ becomes the active state of the module, and the train speed is

decreased gradually. When the train running speed reaches the target speed (i.e., $0km/h$), the train acceleration and the boolean parameters are updated. Hence, the associated transition is enabled, and it constrains the module to evolve automatically toward the *'ConstantSpeed'* model-location.

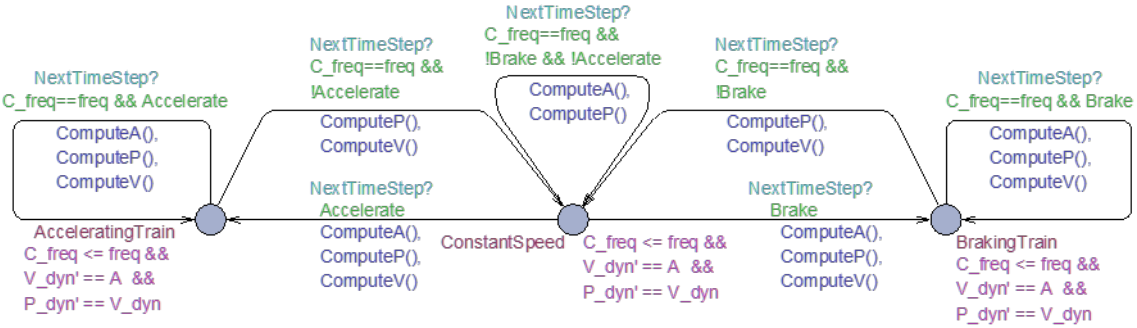


Figure 4.8: Representation of the transitions allowing for entering the steady-state location in the train dynamics module

Finally, it should be noted that the module should accept various initial inputs depending on the needs of the user (e.g., $A = 0$, $A < 0$, $orA > 0$). To this aim, we define an additional initial model-location denoted *'ModelInitialization'*. In fact, this model-location does not represent a particular system state, but is only used to handle the input values and activate the corresponding model-location as needed. Therefore, time is not allowed to pass when the timed automaton is in this location, which is marked as *'urgent'*.

Besides, it is important to underline that all the actions that are not explicitly disallowed in the module configuration are assumed as permitted. Therefore, complementary guarding conditions are set to further restrict the possible evolution of the module and obtain the desired behavior (see figure 4.9.)

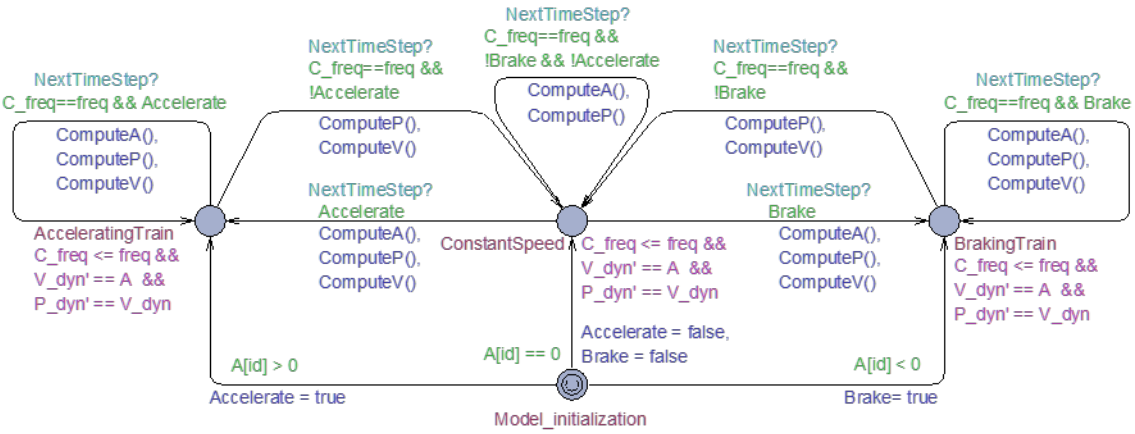


Figure 4.9: Train dynamics representation module.

4.3.2 Modeling the train position error bound

Having detailed the modeling of the train dynamics in the previous subsection, the second modeling phase to be addressed focuses on representing the evolution of the error-bound associated with the estimated train position. In particular, such uncertainty depends essentially on two main parameters, namely:

1. The accumulation of the errors that are inherent to the odometry,

2. The residual uncertainties related to the balises activation.

Accordingly, the TA-based modules described hereafter are dedicated to the representation of these two above aspects.

Odometry error accumulation with real and integer variables

As discussed in Chapter 2, the adoption of the odometry as a train positioning solution implies the accumulation of error on the estimated train position. In particular, such a position uncertainty directly depends on the traveled distance from the last known reference position. Accordingly, the confidence interval associated with the train position estimated by the odometer increases linearly as the train moves away from the adopted reference position. To comply with the technical specifications relevant to the odometry, the acceptable error bound of the odometer should not exceed 5 % of the measured traveled distance (Subset 041: 2015). On the other hand, we know that the actual odometry error can obviously be smaller than this tolerated bound. Nevertheless, the maximum error value (i.e., the worst case) has to be considered from a safety point of view. Regarding the modeling of the bound of the error accumulated by the odometer, we recall that the train-dynamics module includes hybrid clocks variables to represent the integral function of the train speed and compute the train traveled distance. By adopting a similar process, we define a hybrid clock variable, denoted by $'OdoError'$. Accordingly, it is sufficient to set a clock rate value equal to '0.05' so as to obtain '5 %' of the traveled distance and model the evolution of the odometry error bound (based on the relative traveled distance). Adopting the Uppaal specific syntax, the above relation can be concretely noted as follows:

$$\boxed{OdoError == 0.05 * V'}$$

Consequently, the value of $'OdoError'$ is continuously incremented as the train runs, allowing to model the odometry accumulated uncertainty (i.e., 5 % of the traveled distance from the last reference position). In parallel, we define a function denoted $'ComputeOdoError()'$ to compute the associated error employing only integer variables. For that, the function firstly estimates the train traveled distance as the difference between the current train position and the last considered reference position. Therefore, '1/20' of the previously obtained result is calculated to model the odometer error.

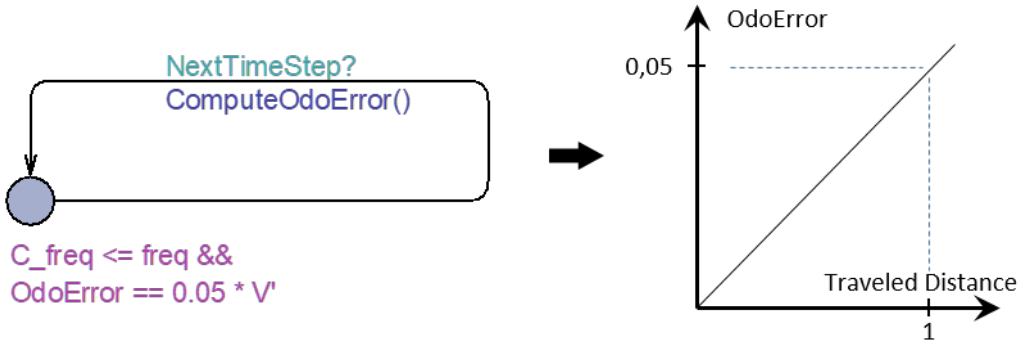


Figure 4.10: Preliminary representation of the odometer accumulated error on the estimated traveled distance.

Hence, we define the associated model-location in the errors on the train estimated position module as represented in Figure 4.10. On the other hand, we underline that for operational reasons, the odometry-related error obviously needs to be bounded. In this respect, the odometry uncertainty is periodically reinitialized, employing eurobalises (see Chapter 2). Nevertheless, such an error resetting mechanism introduces additional train position uncertainty related to the balises detection process itself. Hence, the balises activation mechanism needs to be further explained in order to ease the understanding of such residual error causes. In this context, the following subsection is dedicated to addressing the balise activation process in addition to its representation in our models.

Physical Balise activation

When dealing with the balises activation mechanism, it is essential to distinguish between the physical balises and the virtual ones. In both cases, the use of the balises helps to tackle the inherent error related to the odometry (it is here assumed that the train knows the sequence of balises to be encountered on the itinerary). However, the balises activation mechanism differs considerably depending on the balise type. Regarding physical balises, the activation process can be summarized as follows:

1. The train continuously emits an electromagnetic wave as it runs.
2. When the train passes over a PB, the EM signal energizes the passive PB placed on the track.
3. Once activated, the PB transmits a telegram containing information about its position to the train on-board.
4. Accordingly, the train processes the received telegram to obtain the balises information.
5. Finally, the balise position is adopted as a new reference position, enabling to eliminate the odometer accumulated error and to reset the estimated position confidence interval.

In our modeling approach, an abstraction of the aforementioned process is represented through the automata module named *'Balise Transmission Module (BTM)'* (see Figure **??**)

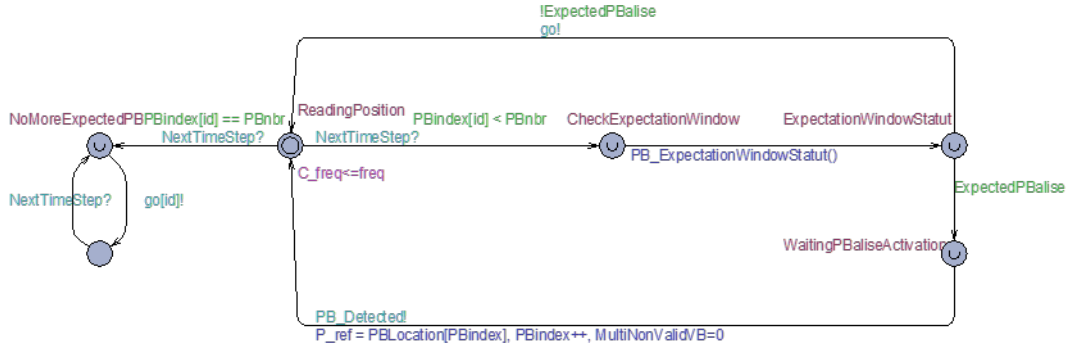


Figure 4.11: Balise Transmission Module (BTM) representing the PB activation.

Firstly, the model-location denoted *'ReadingPosition'* is defined as the initial location of the *'BTM'* module. From this initial model-location, and at each time step, the module compares the current position of the train to the next expected balise known position. Accordingly, the obtained output is used as Boolean variable conditioning the future module evolution.

- If the difference between the two positions is relatively significant, the executed function (*'PB_ExpectationWindowStatut()'*) returns *False*. Consequently, only the transition associated with the guard *'!ExpectedPBalise'* can be activated. Thus, the module returns to its initial state, and the process is repeated at the next time step. In fact, such a sequence models the situation where no physical balise can be activated (i.e., the EM signal emitted by the train does not reach the PB).

- In contrast, if the train position is deemed close to the next expected balise, the comparison function returns *True* and updates the Boolean variable *'ExpectedPBalise'* accordingly. Consequently, the module evolves following the transition guarded with the *'ExpectedPBalise'* condition and reaches the location denoted *'WaitingPBaliseActivation'*.

From the *'WaitingPBaliseActivation'* model-location, the current train position is further compared to the position of the expected PB in order to determine the exact moment of the balise activation. Finally, the corresponding transition is fired once the two positions match each other and before the module returns to its initial location. Finally, it is important to underline that a number of operations are associated with this last transition. In particular, the balise identifier index is incremented to correspond to the following balise on the train itinerary. Accordingly, the activated balise position is adopted as a new reference position and now used for the estimated distance traveled by the train. Moreover, a synchronization message is transmitted to the module representing the uncertainty on the estimated train position. Hence, such synchronization represents the communication between the activated balise and the train, thus allowing the exchange of information between the involved modules. In the end, the model-location denoted *'NoMoreExpectedPB'* is defined as a final state of the *'BTM'* module and can be reached after the activation of all the expected balises.

Virtual Balise Activation

Unlike the PBs placed on the rail track, VBs are abstract entities that allow for emulating the functions provided by eurobalises. Concretely, the VB concept consists of storing the balises data in the on-board train computer and associating such encoded data with geo-referenced

points. In fact, each of these points represents a VB position. Similar to the case of PB, the train has a prior knowledge of the list of VBs that it should encounter on its itinerary. In contrast, the VB activation process presents significant differences compared with the PB one. In particular, the EM wave emitted by the train to energize PBs is no longer needed, as the virtual balises are abstract entities that do not need to be energized. Accordingly, the adopted VB activation mechanism can be summarized as follows:

1. Firstly, a VB reader periodically computes the train position using a GNSS-based localization solution. In fact, this on-board estimated position, known as the Virtual Antenna reference mark, corresponds to the position of the GNSS Antenna mounted on the train roof and projected on the track.
2. Secondly, the computed position is continuously compared with the model-locations associated with the virtual balises.
3. When the GNSS-estimated train position matches the VB position stored on-board train, as part of the track description, the corresponding VB is activated.
4. Finally, the embedded balise information is obtained from the on-board stored database and is transmitted to the EVC.

Consequently, we develop the *'Virtual Balise Reader(VBR)'* model depicted in (Figure 4.12) to translate the behavior described previously.

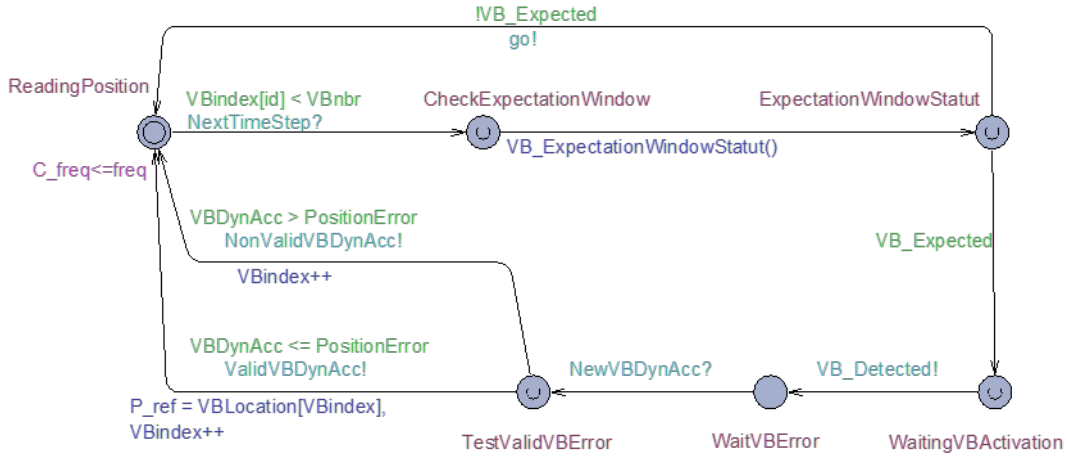


Figure 4.12: Virtual Balise Reader module (VBR) representing VB activation

In particular, we note that the overall structure of the obtained model is quite analogous to the PB activation model. However, it is important to underline that a certain number of operations and transitions represented in the VB activation module (cf. Figure 4.12) do not precisely express the same aspect as in the PB activation module (cf. Figure 4.11). Non-exclusively, we note that the *'no VB expected'* condition, denoted *'!VB_Expected'*, does not mean that the EM signal cannot reach the balise anymore, but depict the situation in which the estimated GNSS-antenna is relatively distant from the position of the next VB. Now that the balises activation process was represented, the following step of our modeling approach consists in addressing the resetting of the uncertainty on the train position.

Updating the uncertainty on the train estimated position following the Balises activation

The development of the modules depicted in Figure 4.11 and Figure 4.12 permitted us to represent the physical and the virtual balises activation process, respectively. In both models, the next expected balise is activated when the train relative position (i.e., the distance traveled by the train, denoted as P_{int}) matches the position of the next expected balise. In this context, we recall that a key function accomplished through the activation of the balises is to reset the odometry error accumulated during the train journey. Concretely, the upper bound of such uncertainty on the train traveled distance can be formulated as follows:

$$\textit{Accumulated odometer uncertainty} = 5\% \times \textit{distance from the last reference position}$$

Accordingly, we note that the distance from the last reference position is the main parameter influencing the odometry uncertainty. Thus, the re-initialization of such parameter makes it possible to reset the odometer accumulated error. For that, the known positions of the activated balises are retained as new reference positions. Consequently, the odometry accumulated error can be reinitialized following each balise activation. To translate this uncertainty resetting process in our model, a synchronization variable ($VB\_Detected!$ / $PB\_Detected!$) is associated with the transitions representing the activation of a balise (in the balises activation modules). In parallel, the module (cf. Figure 4.13) representing the uncertainty on the train position is enriched with new transitions associated with *receiving synchronization variables*. When a balise is activated, the associated transitions are triggered in the corresponding modules. Accordingly, the value of the reference position is updated to match the position of the activated balise, thus, resetting the odometry accumulated uncertainty. Nevertheless, it is essential to underline that even following the odometry accumulated error reset, a residual uncertainty on the train position always persists. In fact, such uncertainty is inherent to the balises activation process and cannot be eliminated. Accordingly, the *global uncertainty on the train position* can be represented as follows:

$$\begin{aligned}&\textit{Global uncertainty on the train position} = \\ &\textit{balise activation uncertainty} + 5\% \times \textit{distance from the last reference position}\end{aligned}$$

In particular, we note that such residual error is encountered in both the physical and virtual balises activation process. Yet, the source and the value of the corresponding uncertainty are considerably different depending on the balise type (i.e., PB or VB). Namely, in the case of PB, the signaling designers establish the track positions where the eurobalises have to be installed. However, the actual positions of the installed PBs may differ from the positions defined during the design phase of the trackside subsystem (e.g., due to physical constraints pertaining to the rail line configuration, or to the slippers' position). Moreover, the PB activation introduces additional uncertainties related to the balises energization mechanism (employing EM signals). Accordingly, the aforementioned error sources have been addressed by defining a corresponding confidence interval value of 5 m. On the other hand, we underline that, since VBs only exist logically on-board the train computer, the VB positioning on the line is not constrained by the physical line conditions. Thus, no uncertainty is associated with the VBs positions. Moreover, we note that the EM-energization process is not employed in the case of VBs activation. Hence, the residual error is independent of such a mechanism. Finally, we recall that in contrast to the PB case, the actual train position cannot control VB activation. Instead, VBs are triggered depending on train position as estimated using on-board localization solution (i.e., GNSS-based localization system). Nevertheless, such localization solutions cannot compute the exact train position with certitude, and a confidence interval (i.e., a Protection Level 'PL') is always associated with the estimated train position. Accordingly, the value of such PL (representing the error bound

computed at the moment of the VB activation) is retained as an uncertainty on the global train position. Phrased differently, it defines the residual error upon the resetting of the odometer error using a VB.

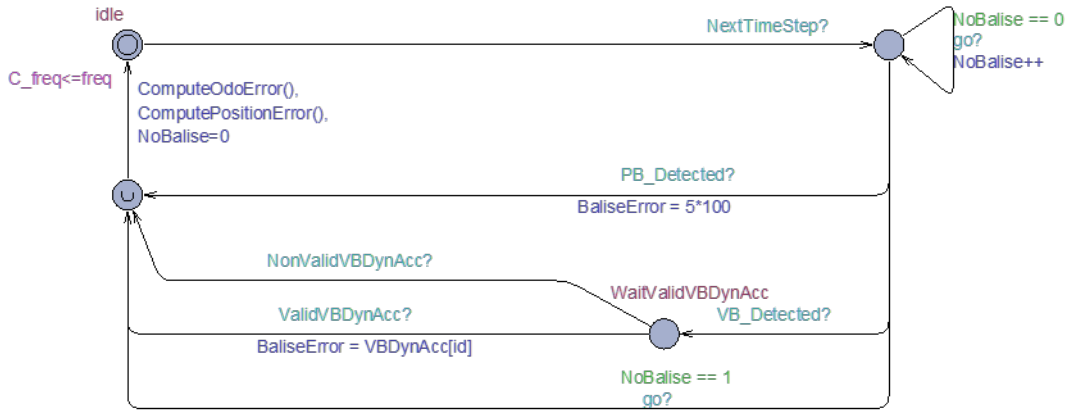


Figure 4.13: Automata module representing the evolution and resetting of the uncertainties on the train position

In order to consider such residual uncertainties in our model, the module introduced in Figure 4.10 is further enriched with a set of transitions, locations, and functions. In particular, the functions in charge of updating both the global train uncertainty and the odometer accumulated error values are executed periodically in the enriched automaton module (cf. Figure 4.13). Besides, the reference position is updated upon each balise activation. In particular, we note that considering the constant 5 m residual uncertainty (related to PB activation) in the model is straightforward, as such a fixed value is common to all the physical balises. In contrast, the PL value associated with a VB activation may variate according to various parameters (e.g., reception conditions of GNSS signals). It is, therefore, trickier to represent such dynamically computed value in our models. To tackle this issue, we chose to develop a new module dedicated to representing the computation of the PL values (cf. the following subsection).

Generating the VB activation related uncertainty

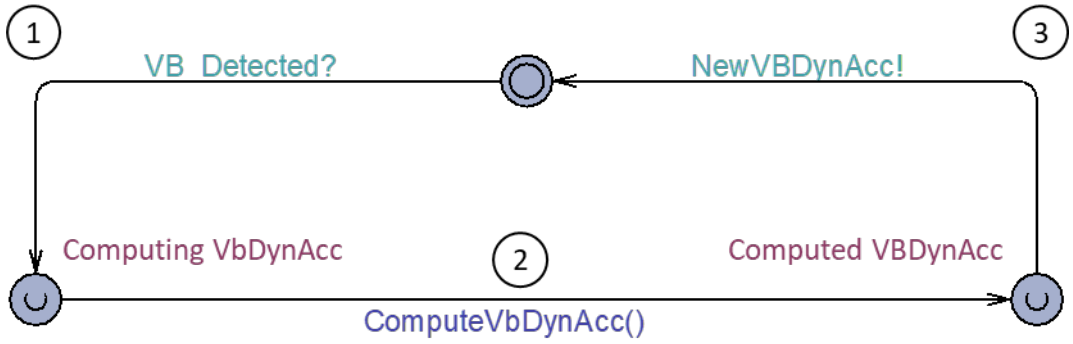
The role of this module (see Figure 4.14) is to dynamically generate the computed values that represent the PL associated with the estimated train positions used to activate VBs. Moreover, such VB Dynamic Accuracy ('$VbDynAcc$') needs to be accepted by the model to reset the uncertainty on the estimated train position following each VB activation. In its simplest form, the module translating the '$VbDynAcc$' generation can be abstracted as a three-steps process:

1. Starting from its initial model-location, the module waits for the reception of the synchronization message '$VBDetection$' *emitted by the 'VB activation module' (VBR)* (variable $VB\_Detected$!).

2. When the message is received, the associated transition is fired and the module state reaches the urgent model-location '$ComputingVbDynAcc$'. In fact, such intermediate model-location represents the source location of the transition implementing the VB dynamic accuracy computation function, denoted as '$ComputeVbDynAcc$'. Concretely, the execution of this function permits to obtain a random value representing the estimated

PL associated with the VB activation. In particular, we note that the computed values are generated according to the specific probabilistic distributions defined by the user in the declaration section of the module.

3. Finally, the transition linking the urgent model-location *'ComputedVBDynAcc'* and the initial model-location of the module is associated with a synchronization message *'NewVBDynAcc'*, enabling to communicate the generated value.




```
void ComputeVbDynAcc(){
    int PL = 0;
    PL = fint(random_normal(mean, std));
    // normal distribution with predefined mean and std values
    if(PL > 0){
        VBDynAcc = PL;}
    else {VBDynAcc = 0;}
}
```

Figure 4.14: Referential module representing the generation of VB activation related uncertainty

Depending on the specific operational scenario that one wish to investigate, numerous variants of the present module can be developed. In particular, the module instantiation presented in Figure 4.14 only considers a single probabilistic distribution conditioning the computed PL values. However, we must recall that the actual PL values are influenced by several parameters, mainly pertaining to the rail environmental conditions. Consequently, the resulting behavior related to the VB detection process cannot be modeled by means of a single distribution. Instead, multiple distributions need to be employed in the module to express the impact of various GNSS-signals reception conditions. In this context, the reader can find a set of module implementation-examples in the following section of this manuscript.

4.4 Setting the relevant model input parameters

The main objective pursued throughout our model-based approach is to help investigate the uncertainty related to the estimated train position, especially following the introduction of

virtual balises. With this aim, a preliminary step is to investigate the various factors that can impact such uncertainty. In this context, we mainly identify three important parameters:

1. The protection level associated with each virtual balise activation, since the PL is used to reset the uncertainty on the estimated position.

2. The space distance separating consecutive balises, as this distance determines the odometry error accumulation.

3. The ratio between the number of PBs and VBs, as the use of VBs is likely to introduce more uncertainties compared to PB.

The three previous aspects having been identified, the proposed methodology (cf. Fig 4.1) considers their representation in the developed model. In this regard, the present section addresses the inclusion of these parameters as configurable inputs in our models.

4.4.1 Parameters related to the PL associated with each VB

As previously established, the PL plays a central role in resetting the errors on the estimated train position following the detection of a VB. Therefore, the developed behavioral model must permit considering the parameters associated with the PL values generation. To this aim, we implemented a Uppaal module whose objective is to generate the PL values according to specific probabilistic distributions. Note that in the literature, a number of works have dealt with the characterization of the PL (Blanch, Walter, and Enge 2008; Drevelle and Bonnifait 2009; El-Mowafy and Kubo 2017; Tijero et al. 2017; Zhu et al. 2018; Zabalegui et al. 2020; Kazim, Nourdine Aït Tmazirte, and Marais 2020; Nourdine Ait Tmazirte, Kazim, and Marais 2020). In general terms, such works aim at predicting the PL values according to the surrounding environment in which the GNSS receiver evolves. In contrast, we recall here that the objective of the present work is rather to establish adequate means to assess safety features and operational performances when GNSS-based systems are used for railway localization. Consequently, the PL characterization is out of the scope of our contribution, and we assume that the adequate bounds of the PL are known for the different considered operational contexts with an associated localization integrity risk (cf. Section 3.4.1). Accordingly, the PL value is represented in our model by the random variable denoted 'VbDynAcc'. The values of this variable are generated according to some predefined probabilistic distributions, making it possible to implement the uncertainty on the PL value. Finally, it is worth noticing that some works focusing on the characterization of the PL are still in progress; hence, the distributions used in the sequel of this manuscript are chosen only for the sake of illustrating our approach. Nevertheless, different distributions can easily be considered by simply adapting the variables in the model (e.g., type of distribution, mean value, standard deviation).

Based on the contributions addressing the modeling of the PL, we conclude that one of the most relevant approaches consists in associating different PL distribution with the different classes of GNSS signal reception conditions. In practice, one can identify various environment types along the rail line. For the sake of illustration, let us address the representation of a rail line passing throughout four distinct surrounding classes. Namely:

1. Environment 1: Open-sky,

2. Environment 2: Semi-urban,

3. Environment 3: Forest,

4. Environment 4: Urban.

In this case, each of these environment class is further associated with a specific probabilistic distribution. For the sake of illustration, examples of potential distributions are depicted in Figure 4.15.

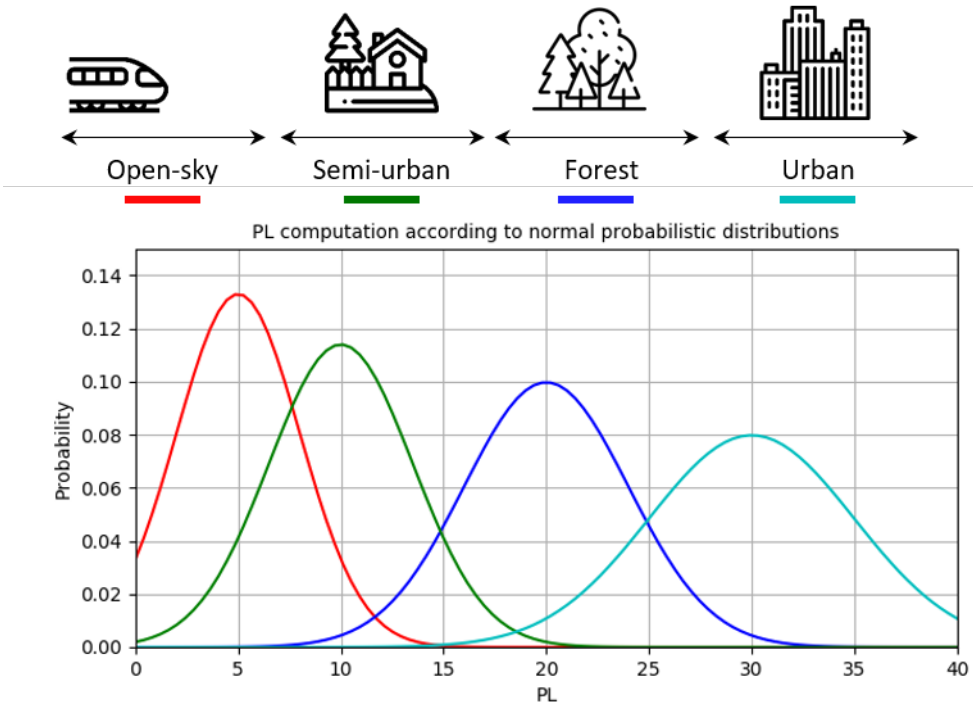


Figure 4.15: Distinction of particular environmental classes along the rail line

To represent such a feature in the automaton model, the original module presented in Figure 4.14 is enriched with additional transitions. Concretely, the central transition of the automaton is replaced by four distinct transitions (one transition per environment class). Accordingly, guard conditions ($'EnvClass == i'$, i being the index of the class) are assigned to each transition in order to constrain the choice of the associated PL distribution (cf. Figure 4.16). Finally, it is sufficient to adapt the variable representing the active environment class to comply with the associated guard conditions and obtain the appropriate PL values range.

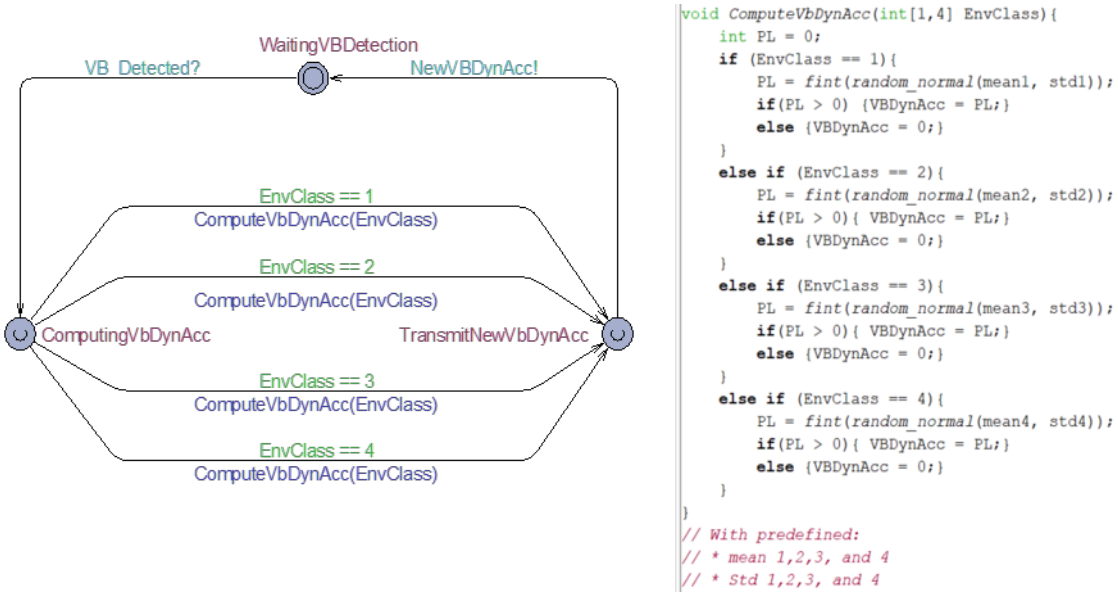


Figure 4.16: Module representing the PL generation according to the active environment class.

Furthermore, let us recall that the modular representation adopted in the present approach permits to address the complex behavior of the system by means of relatively simple modules. Hence, thanks to this modularity, it is notably easier to integrate further features progressively since only the module related to the specific aspect needs to be adapted.

In particular, let us consider the case where each environment class is no longer associated with a single probabilistic distribution, but rather includes a set of different distributions. In fact, this case represents the variation in the GNSS-signal reception conditions within the same environment type. Concretely, such a situation may express the result of satellites positions changing during the day. In this context, the module depicted in Figure 4.17 illustrates a case in which two satellites configurations can be distinguished in each of the previous four environment classes. Accordingly, the condition parameter is further accepted as an additional input, conditioning the choice of the associated probabilistic distribution used to compute the PL.

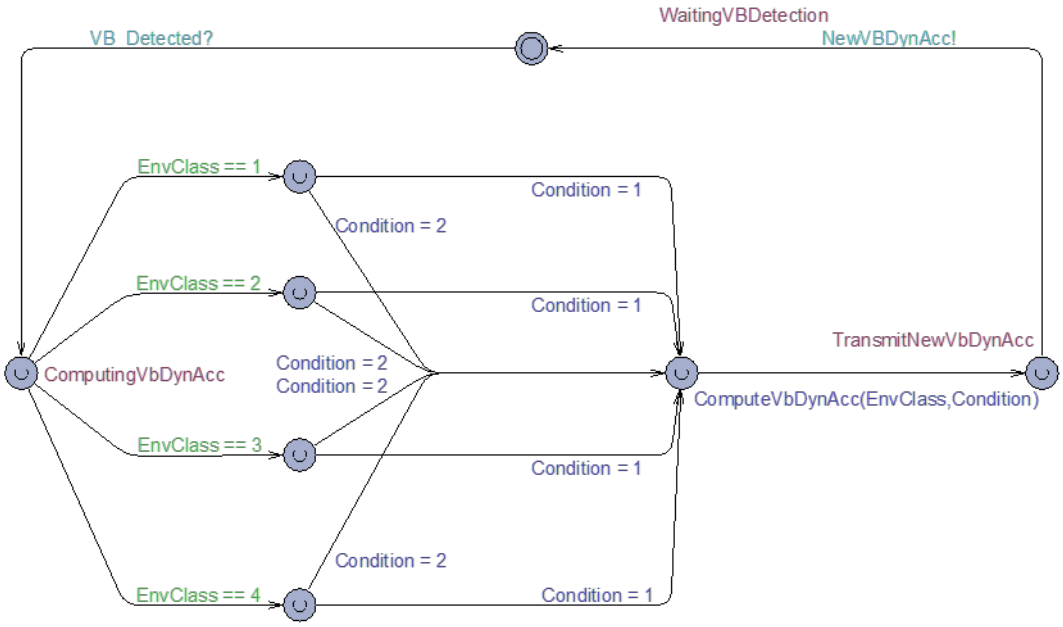


Figure 4.17: Case of PL generation following a pseudo-deterministic choice of the probabilistic distribution within a defined environment type

Finally, one can also use the current approach to address less deterministic behavior. For that, the Uppaal tool permits to employ probabilistic transitions in the model. For instance, such a feature may illustrate the case where no predefined setting on the specific environmental conditions along the rail line is available. Accordingly, the module can simply be adapted to represent a random selection of a PL distribution from a set of possible predefined options. In this context, the module associated with the implementation of such a particular case is illustrated in Figure 4.18. This aspect could be of interest to investigate various GNSS environmental conditions generated randomly.

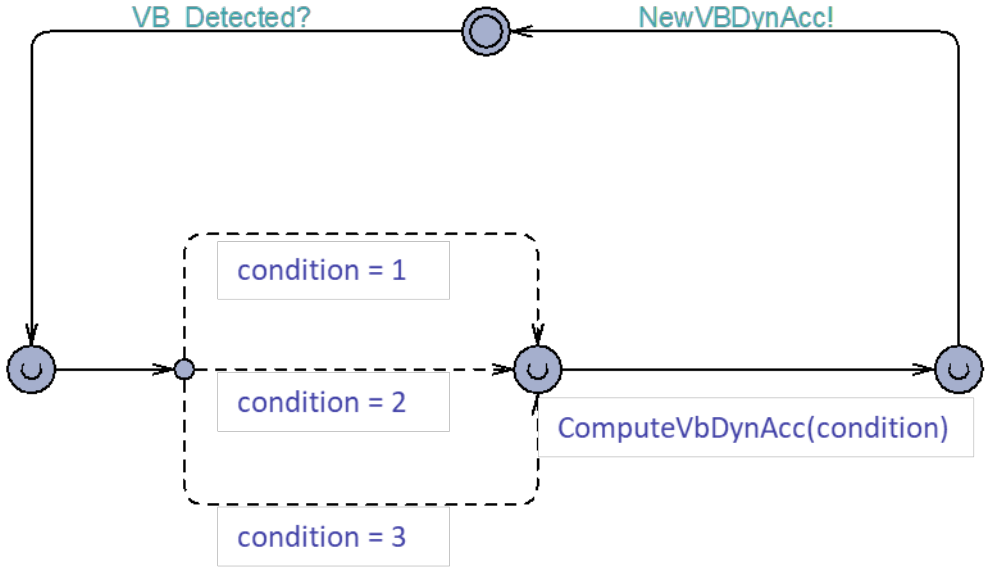


Figure 4.18: Case of PL generation following a non-deterministic choice from a set of probabilistic distributions

4.4.2 Parameters related to balise configurations on the rail line

In practice, balises play a central role in resetting the odometer errors; thus, their arrangement along the rail line highly impacts the global uncertainty on the estimated train position. Therefore, a further important aspect to consider when setting the model inputs is the balises related parameters. One should keep in mind here that, in general, the goal is to minimize the resort to PBs; by rather recurring to VBs. Precisely, the present subsection mainly deals with the representation of the balises positioning on the train itinerary. In this regard, we firstly underline that the train position is always determined as a longitudinal (1D) variable along the train route. Therefore, by considering such along-track referencing principle, the position of a train can mainly be defined in relation to the traveled distance from the Last Relevant Balise Group (LRBG) encountered. Moreover, we note that even if the train planned route is part of a complex track layout (due to possible track junctions and switches), such itinerary can be referred to as a simple series of successive balises (see Figure 4.19). Hence, a list of the balises to be encountered on the assigned train itinerary is typically communicated to the on-board train computer. Such a balise list is defined in the declarations section of the model to represent the train routes. In particular, the corresponding variable vector should contain information on the specific balises positions. If parallel tracks need to be represented, it is sufficient to add an identifier allowing to distinguish between the distinct portions of the track.

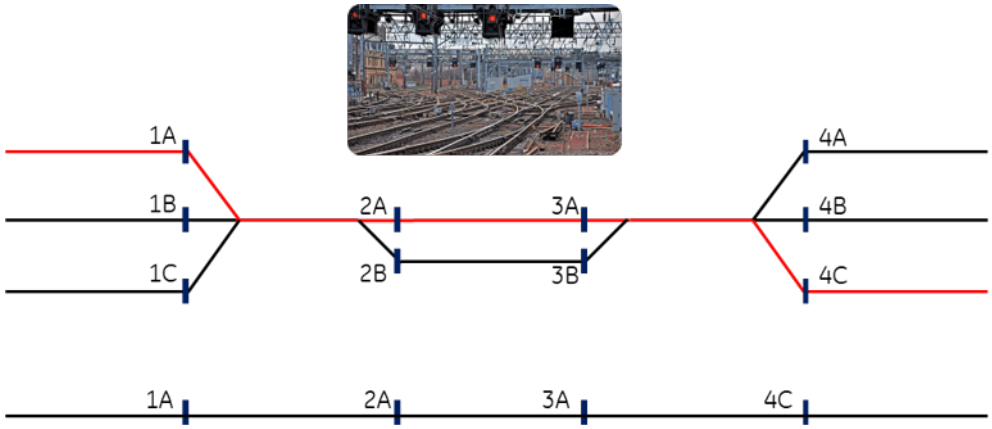


Figure 4.19: Representation of train routes as perceived by the train on-board

Furthermore, one should notice that two aspects must be distinguished when dealing with the setting of balise parameters. Namely:

1. The distance separating two consecutive balises (d), since this parameter particularly impacts the bound value on the accumulated odometer error.

2. The balise type (i.e., PB or VB), as the calculation of the residual uncertainty value upon the activation of a balise depends on the balise type.

Regarding the first parameter, we note that a typical case encountered implies that the balises are spaced on the track according to a regular arrangement. Hence, we denote (d) the variable representing distance separating two successive balises. Furthermore, one can easily imagine defining a function that takes such a parameter as an input to automatically set the balises positions on the line.

When dealing with the balise type parameter, one can logically admit that an infinite number of combinations is possible. Yet, it could be assumed that particular layouts can be distinguished in some rail line configurations. In this context, let us denote ($PB - n.VB$) the balises type pattern in which (n) represents the number of VBs separating two consecutive PBs. Assume a repetition of such a pattern is identified in the addressed rail line, the corresponding balises representation can be performed automatically (based on the (n) variable taken as an input parameter) and the distance d separating two consecutive balises.Accordingly, balise configurations such as those illustrated in (Figure 4.20) can easily be represented in our model simply by adapting a set of input parameters in the corresponding balise initialization function.

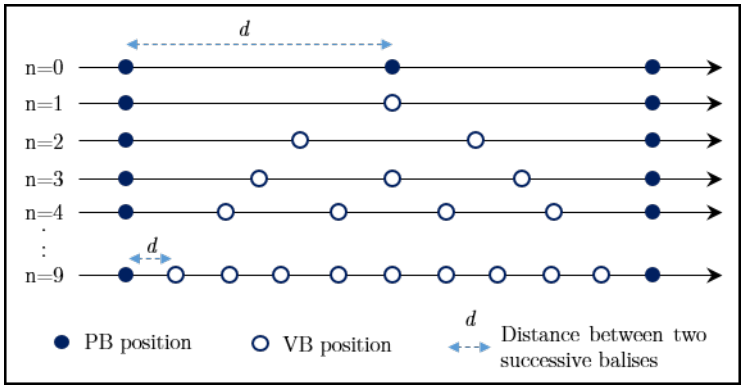


Figure 4.20: Illustration of potential balises configuration along the rail track.

Finally, if a more specific line configuration needs to be analyzed, the different balises related parameters can be defined manually in the model. Hence, particular implementations can be addressed based on the available knowledge about the investigated track layout.

4.5 Conclusion

To conclude, we proposed a modeling approach that is adapted to the analysis of GNSS-based train localization function both from a safety and performance points of view. The proposed approach is defined with the prospect of reducing on-site tests. In fact, the developed model-based approach allows us to emulate the relevant system behavioral aspects related to the train positioning. Concretely, we developed in this chapter formal models with the intent of describing various train positioning relevant features. In particular, we adopted a modular representation of the system in order to provide an abstraction of the GNSS-based train localization process. Concretely, the available technical specifications of the system were used to extract relevant information about the estimation of the train position. Accordingly, odometry error accumulation, physical and virtual balises activation, and the rest of the uncertainty on the train position were modeled while employing a number of communicating automaton modules. Moreover, a specific module was dedicated to the representation of the train dynamics as they move on a rail line. Eventually, translating such dynamic aspects into the model allows for addressing particular operational scenarios in the next chapter.

Indeed, considering the particular GNSS-based train localization application, the train interaction with its surroundings plays a central role and highly impacts the performances of the train positioning solution. Therefore, the developed model supports the inclusion of a module representing the potential uncertainties related to the activation of the virtual balises. Concretely, such a module permits to generate random values to represent the GNSS-related errors. Moreover, it is worth noting that such values are obtained based on various probabilistic distributions that allow for translating the GNSS-signals reception conditions. Yet, we underline that establishing such mathematical models to characterize the rail environment is out of the scope of our contribution. However, the potential results pursued through dedicated studies can be considered as input parameters of our models.

Finally, the last section of this chapter was dedicated to the illustration of the various model parameters setting, in order to investigate specific operational scenarios and consider different rail line configurations, and according to various environmental conditions.

In conclusion, a natural prolongation of this work consists in investigating a set of safety and performance properties to illustrate the added value brought by the proposed model-based approach. Accordingly, the following chapter of this manuscript is dedicated to this purpose.

Chapter 5

Model-based analysis of safety and performance properties

Outline of the current chapter

5.1 Chapter Introduction

The major stakeholders in the rail industry are constantly trying to get the most out of the existing infrastructure. In this context, running as many trains as possible on a railroad line while maintaining operation safety remains an ultimate goal from the railway operational and safety points of view. In particular, the train collision avoidance function plays a crucial role in ensuring safe rail operations. That is why various interacting elements of the rail Control Command and Signaling (CCS) system are combined to accomplish such a safety-critical function. Concretely, the train movement authority is calculated in such a manner so as to always guarantee a safe train separation distance. Besides, service and emergency brakes shall be automatically activated in case the driver does not respond appropriately to the provided instruction. Yet, the confidence level that can be associated with the estimated train position is a key parameter conditioning the effectiveness of the implemented safety barriers, as most of the collision avoidance features are triggered depending on train position information. In this regard and to illustrate how our model-based approach can be advantageously used to perform safety and performance analysis, we chose to focus in this contribution on the impact of the uncertainties resulting from the position calculation process and its associated risk.

The previous chapter has allowed us to represent the behavior of the GNSS-based train positioning by means of a number of formal models that we have elaborated. The obtained models are employed in this chapter to address a set of safety and operational properties according to the SMC technique. The present chapter is structured as follows. The employed SMC verification principle is briefly reminded in the first section of this chapter. In the second section, a study investigating the impact of the parameters related to GNSS-based train positioning on developing a new ETCS-L3 line is presented. To this aim, different balise dispositions on the line are analyzed while considering various GNSS-reception conditions, and the impact of such parameters on the global uncertainties associated with the estimated train position is assessed. Accordingly, a number of recommendations on the appropriate positioning of the balises along the case-study line are provided. On the other hand, not only the expected behavior of the system in nominal conditions needs to be investigated prior to the implementation of a new rail line. In the third section of this chapter, we mainly discuss the potential behavior of the system, under non-nominal conditions.

5.2 SMC Verification Underlying principle

Unlike classic model-checking (MC), which issues a binary result on whether the verified property is satisfied or not, statistical model-checking (SMC) involves probabilities and permits providing quantitative results in the form of a likelihood of a feature to be fulfilled. For that, the associated SMC algorithms basically run a number of simulations on the model (i.e., network of stochastic timed automata (NSTA)) in order to estimate how likely (i.e., as a probability value) the examined property is satisfied. Beforehand, the SMC investigated properties must be expressed according to the formalism of the Weighted Metric Temporal Logic (WMTL) (Bulychev et al. 2012). Namely, WMTL is an extension of the Metric interval Temporal Logic (MITL) (Koymans 1990; Alur, Feder, and Henzinger 1996), and can be defined by the following grammar:

$$\phi ::= p \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid X\phi \mid \phi_1 U_{x\leq t} \phi_2 \tag{5.1}$$

where p is a conjunction of predicates over the state of a NSTA, t is a natural number ($t \in \mathbb{N}$), and x is a clock. Besides, the classical logic operators (i.e., conjunction and negation) are interpreted as usual, i.e., $\neg(\phi_1 \wedge \phi_2) = \neg\phi_1 \vee \neg\phi_2$. X is the usual *neXt* operator from temporal logic. Accordingly, $X\phi$ states that the formula ϕ is satisfied in the next state of the run. U denotes the time-bounded *Until* operator. Hence, the weighted MITL formula $\phi_1 U_{x\leq t}\phi_2$ is satisfied if the formula ϕ_1 holds in all the states along the run until the formula ϕ_2 becomes satisfied, and this must happen before the clock x exceeds time t.

Using the above concepts, it is also possible to obtain the *eventually* and *always* operators. Concretely, let the abbreviation tt denote $true$ as $\phi \vee \neg\phi$; thus:

$$\Diamond_{x\leq t}\phi = tt \;\; U_{x\leq t}\phi \tag{5.2}$$

and

$$\Box_{x\leq t}\phi = \neg\Diamond_{x\leq t}\neg\phi \tag{5.3}$$

In particular, the notation $\mathbb{P}_M(\phi)$ is further used to denote the probability that a random simulation run of a model M satisfies the formula ϕ. In fact, *UPPAAL SMC* holds simulation-based algorithms (i.e., SMC) to approximate the evaluation of three types of queries over the model. Namely:

1. **Probability estimation**: $\mathbb{P}_M(\Diamond_{x\leq t} \;\; p)$
   How likely ($\Diamond_{x\leq t} \;\; p$) holds on the NSTA model M.

2. **Hypothesis testing**: $\mathbb{P}_M(\Diamond_{x\leq t} \;\; p) \geq P$? with ($P \in [0,1]$)
   Is the probability that ($\Diamond_{x\leq t} \;\; p$) holds on M is greater or equal to a certain threshold P.

3. **Probability comparison**: $\mathbb{P}_M(\Diamond_{x_1\leq t_1} \;\; p_1) \geq \mathbb{P}_M(\Diamond_{x_2\leq t_2} \;\; p_2)$?
   Is the probability that ($\Diamond_{x_1\leq t_1} \;\; p_1$) holds in M is greater than (or equal to) the probability that ($\Diamond_{x_2\leq t_2} \;\; p_2$) holds in M.

Note that in the remainder of this chapter, we will only employ the probability estimation query to evaluate a set of performance and safety-related properties. From a conceptual perspective, solving such a question using SMC can be achieved by employing an estimation algorithm that is analogous to the Monte Carlo simulation approach. Concretely, each run of the system is first encoded as a Bernoulli random variable that is true if the run satisfies the property, and false otherwise. The obtained outcomes are then aggregated by a statistical algorithm to quantitatively estimate the probability of the property being satisfied. Here, it is relevant to underline that the results obtained from such a process are based on a sufficiently large number of simulation runs,

and by using sampling. Thus, the results should be seen as an estimation. In other words, the SMC technique does not guarantee the exhaustiveness of the state-space exploration, in contrast to the classical MC. Consequently, exact results (with 100 % confidence) can not be obtained when using the SMC technique. This justifies the fact that the generated results are associated with a confidence interval. In practice, the Uppaal SMC algorithm computes the number of runs needed in order to produce an approximate interval $[p-\epsilon; p+\epsilon]$ for the probability p with a confidence $(1-\alpha)$, where:

- ϵ is the probability uncertainty.
- α is the probability of false negatives.

In fact, the interpretation of these parameters is that if the interval estimation is repeated N times, with $(N \rightarrow \infty)$, then the true (unknown) probability will be contained at least $(1-\alpha)N$ times in the estimated confidence interval $[p-\epsilon; p+\epsilon]$. In particular, the relation between the estimated probability confidence intervals and the true (unknown) probability $\mathbb{P}$ can be illustrated in Figure 5.1, taken from (David et al. 2015).

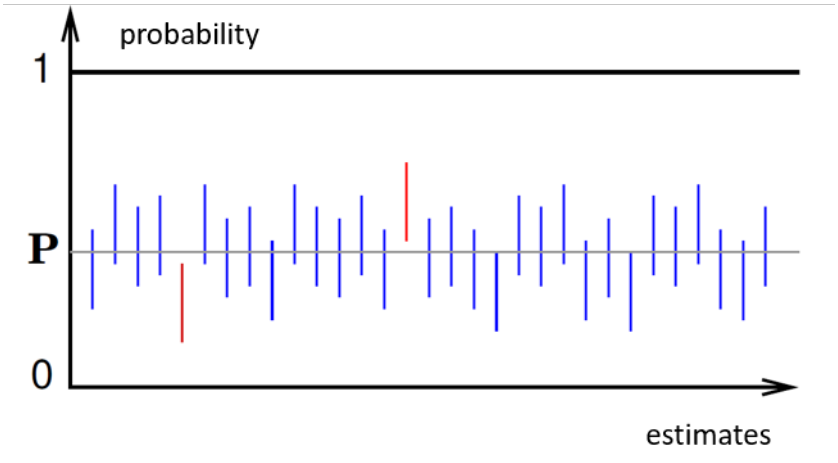


Figure 5.1: True probability $\mathbb{P}$ and confidence interval.

Furthermore, the authors in (David et al. 2015) explain that the number of the simulation runs which are needed to comply with the aforementioned parameters is decided *a priori* by using the *Chernoff-Hoeffding* inequality (Chernoff 1952; Hoeffding 1994), and based on the values of α and ϵ.

Besides, Uppaal SMC implements a sequential method where a probability confidence interval (for a given α) is derived with each new simulation measurement, and the simulation generation is finally stopped when the confidence interval width is smaller than $(2 * \epsilon)$. Finally, we should also underline that the Uppaal SMC further supports a *simulate* type query that allows for visualizing the values of expressions (evaluating to integers or clocks) along the simulated runs. For that, the applied syntax is structured as follows:

$$simulate\ [<= bound\ ;\ N]\ \{E_1, .., E_k\} \tag{5.4}$$

where:

- *bound* is the time bound on the simulations
- $N \in \mathbb{N}$ refers to the number of simulations to be performed
- E_1 ; .. ; E_k are the k (state-based) expressions to be monitored and visualized

In particular, such a facility provides insight into the behavior of the modeled system. It is used, among probability estimation, in the following of this chapter to address a set of case studies.

5.3 Case Study 1: Analysis of a railway ETCS-L3 line under nominal conditions.

As discussed earlier in the manuscript, the underlying idea behind using VB is to emulate the behavior produced by PB without resorting to physical devices (Eurobalises). **In general, balises can be placed to coincide with blocks' limits**. Hence, by using VBs, it becomes possible to virtually split the line into shorter sections without using additional physical devices. However, choosing the location of balises is an engineering matter since no rules in the specifications address this aspect. Besides, when upgrading existing lines toward ETCS L3 with the possible use of VBs, the presence of some existing PB in addition to (new) VBs has to be considered. The question of line migration is of paramount importance since building a new line induces not only excessive infrastructure costs, but can even be technically impossible due to space unavailability, especially in dense territories. Finally, an interesting trade-off solution is to upgrade existing lines that are operated with classic fixed blocks by enabling the use of FVB, while using both PB and VB. That is why the analysis process proposed in the present manuscript considers the presence of both types of balises along a line. Such a process can advantageously serve as a guide for railway signaling engineers to set a safe configuration of PBs and VBs along a given railway track. Throughout the case study addressed in the present section, our objective is to address the following question: *What is the probability that the uncertainty (i.e. error-bound) on the train position exceeds some predefined threshold value ?*. By setting an objective threshold value from a level 2 reference line, we will try to draw conclusions on the conditions to be respected in a level 3 line in order to reach similar performances. This will notably allow for defining some specifications on the placement of the balises in order to minimize the risk of exceeding the uncertainty threshold on the train position.

5.3.1 Motivation of the use-case and related problem statement

From a general point of view, the use of VBs to implement the train localization function under ETCS L3 can be envisaged in two main situations, namely:

1. The design of a new railway line under the ETCS L3.
2. The upgrade of an existing line (e.g. operated in ETCS L2) towards ETCS L3.

In both situations, the pursued objective is to reinforce the capacity of the rail line while maintaining and guaranteeing an acceptable safety level. To monitor such an objective, the impact of the GNSS-based localization function on operational safety and performances has to be evaluated. In practical terms, this involves studying the optimal capacity that can be achieved by a railroad line while guaranteeing the absence of collisions between the succeeding trains. In this regard, it should be noted that railway line capacity can be measured depending on two main parameters:

1. The speed at which the operated trains are allowed to run on the line.
2. The distance interval between two consecutive trains.

Both of these parameters constrain the number of trains that can be operated on a rail line during a certain time period. Thus, influencing the transporting capabilities in terms of *passenger number and freight load*. However, we should underline that the train speed parameter is, in fact, not impacted by the type of the balises employed (i.e., being physical or virtual), as the information provided by the balises specifically focuses on correcting the estimated train position. Consequently, we conclude that *addressing such speed-related parameter is not relevant under this particular case study objective (i.e., investigating the impact of the GNSS-based localization function)*.

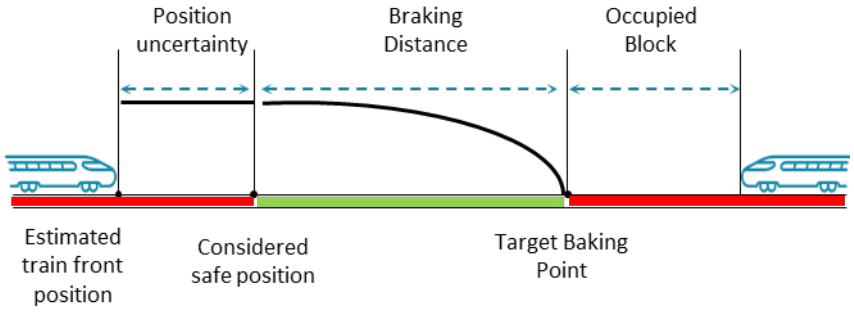


Figure 5.2: Impacting Parameters for the distance interval between two consecutive trains

On the other hand, we observe that the distance interval between two consecutive trains further depends on three parameters (under the FVB operating principle). Such parameters are represented in Figure 5.2 and can be listed as follows:

1. The length of the (virtual) fixed blocks,
2. The braking distances needed by the operated trains,
3. The maximum uncertainty value on the estimated train position.

If we analyze these three parameters in more details, we notice that the *"braking distances needed by the operated trains"* are primarily conditioned by the *"braking characteristics"* of the operated rolling stock, regardless from the track equipment (e.g. balises). Thus, the value of such a variable will remain unchanged despite the use of virtual balises. In contrast, we note that the length of the rail fixed blocks is a parameter that can be influenced depending on the distance interval between successive balises groups. Besides, we remind that the (logical) VB placement on the rail lines does not obey to the same engineering rules previously adopted for the physical balises, as a VB is not constrained by the physical conditions of the track anymore. Accordingly, the balise separation distance parameter needs to be considered in the remainder of this case study. Finally, we underline that the *"uncertainty on the estimated train position"* is obviously the most impacted parameter when employing GNSS-based train localization. Indeed, VBs are more prone to uncertainties than PBs when used to reset the estimated train position error. Therefore, the *"uncertainty on the estimated train position"*, in conjunction with the "balises separation distance", will be particularly scrutinized in what follows. The aim is to address the potential variation in terms of line capacity when introducing a GNSS-based localization function according to the FVB operating principle, relatively to a L2 operation reference.

Having identified the most relevant parameters to analyze in the remainder of this chapter, let us now consider the study of the design of a new ETCS L3 line to be operated according to the FVB principle. Concretely, such L3-FVB line should be designed to provide at least the same capacity that would have been obtained under ETCS L2 operation (i.e., with PBs exclusively). In order to accomplish such a comparative study, the configuration of the rail line to be used as a comparison basis is presented hereafter.

Setting the L2 reference line configuration

The purpose of this subsection is to present the configuration of an illustrative rail line to be used as a reference in the following of this chapter. In this context, we assume that such a line configuration can be described as follows:

- The line is operated according to the ETCS L2 principle,
- Only physical balises are used for odometry calibration (i.e. resetting the accumulated errors),
- All the PBs are equivalently spaced on the track (which is a simplification assumption, here),
- The distance separating two successive (group of) balises is $d = 2000\ m$.

Based on the aforementioned line configuration, the uncertainty of train position can be depicted as in Figure 5.3. In particular, such illustration permits to simultaneously outline the *"uncertainty on the estimated train position"* and the *"balises separation distance"* corresponding to this ETCS L2 line (since both parameters have been identified as relevant earlier in this section).

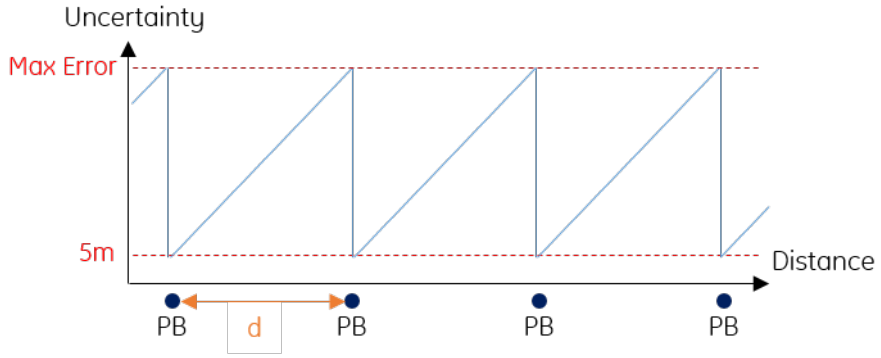


Figure 5.3: Evolution of the uncertainty on the estimated train position according to the configuration of the ETCS L2 line

As shown in this chart, the assumed ERTMS L2 line configuration implies that the global train position uncertainty varies between 5 m (immediately upon the activation of a PB) and 105 m ($5 + 5\% \cdot d$ with $d = 2000\ m$, right prior to the activation of the following PB).

Defining the specific criteria to perform comparison

In the case of ERTMS-L2, one can note that the error bound on the estimated train position can easily be predetermined, as it depends only on the distance between balises and the odometric

maximum error accumulation which, in turn, can be characterized linearly. However, the determination of such an error bound is substantially trickier when it comes to ERTMS-L3 line, as the GNSS-related uncertainties need to be further addressed. In particular, an evolution towards L3-FVB implies the introduction of a new source of uncertainty related to the use of the Protection Level assigned to VBs as a reset value on the estimated train position (see Figure 5.4). Yet, although being challenging, the consideration of such aspects remains necessary in the design phase of any new ERTMS-L3 line.

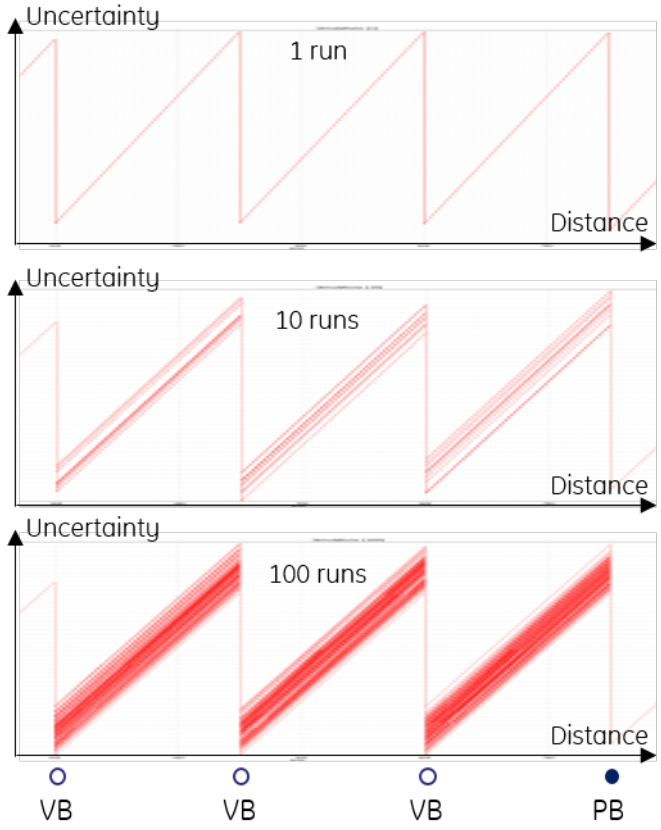


Figure 5.4: Evolution of the uncertainty on the estimated train position following the use of Virtual Balises

Through our case study, we seek to illustrate how to address the position uncertainties under FVB operation based on the developed models, and by means of formal verification. In particular, the *PL* characterization related to VB activation will be analyzed in the sequel, and their impact on train position uncertainty will be investigated. Namely, we will address the following question: *"How should the balises be arranged on the L3-FVB line in order to guarantee that the uncertainty on the train estimated position does not exceed a predetermined threshold?"*.

Characterizing the new L3-line

Before answering the above question, some characteristics of the new L3 line should be predefined in an analogous manner to the L2 line. More precisely, such a line description might be

indicated through a set of parameters including the following elements:

- The adopted operational principle (e..g. Fixed Virtual Blocks),
- The ratio of the number of VBs used along the rail line (e.g. 90 % of VBs) and the associated type of balises pattern (i.e.: $PB - n.VB^*$),
- The homogeneity of the distance separating two successive (group of) balises: (e.g. Constant distance to be defined),
- The models of the Protection Level used for odometry calibration following the activation of a virtual balise (e.g. using one probabilistic distribution per environment type).

We should underline here that one can logically accept that an infinite number of L3 line configurations combining different variants of the above-mentioned factors can be designed. Therefore, we should focus our analysis on a subset of these possible cases. Accordingly, relevant cases shall be identified based on the feedback provided by the different actors involved (e.g., engineers) and taking into account the technical constraints related to the particular context of the studied line (e.g., environment type), as well as the intended objectives in terms of limited use of track equipment.

Defining the properties of the ETCS L3 line to be addressed

The objective of this case study being rather to outline the proposed approach for dimensioning the line instead of dealing with a specific line; it is then sufficient to define a realistic configuration that shall serve in the continuation of this case study. In this context, we choose to address a level 3 line operated according to the FVB principle. Moreover, we admit that only 10 % of the balises employed in the investigated new ERTMS L3 line are physical. In other words, 90 % of the balises are VBs. Accordingly, a balises pattern of *(1PB - 9VB)* can be adopted for this line. In particular, this means one (group of) balise is physical while the 9 next successive (group of) balises are virtual (VB), etc. In regard to the distance separating two successive balises, we recall that the results sought via our analysis intend to provide indicators regarding the PB and VB positioning along the new line. Such indications should permit setting the L3 line in order not to exceed the maximum value of the error on the estimated train position obtained in the case of the L2 reference line. Therefore, the value of this distance will only be established as a result at the end of the analysis. Besides, we recall that such analyzed *PositionError* can further be decomposed into two elements:

- *BaliseError*,
- *OdoError*.

In particular, the *OdoError* (i.e., the odometer accumulated error) component of the *PositionError* is independent of the GNSS-based functions, and only depends on the traveled distance from the last balise. As such behavior remains unchanged in the new L3-FVB line, we can assume the distance separating successive balises (denoted as *d'*) to be constant. Accordingly, one can easily infer the maximum value of *OdoError* from *d'*. In contrast, the *BaliseError* variable (resulting from the activation of a VB) depends on the various *PL* values associated with the GNSS performances, and represents the most uncertain part of the *PositionError*. Therefore, such a variation needs to be finely investigated and is the central focus of the remainder of our case study.

Having outlined the impact of the *PL* values on the studied *PositionError*, it then remains to set the parameters allowing to represent the behavior of such *PL* element. In this context, we already concluded in Section 4.4.1 that a promising approach consists in associating a *PL* generation model with each class of GNSS signals reception condition. Accordingly, we choose to distinguish three types of environments along the L3 Line investigated in this case study. Then, a mathematical model consisting of a probabilistic distribution is used to characterize the *PL* values in each of these conditions (cf. Table 5.1).

GNSS reception condition	*PL* Distribution	Mean	Standard deviation
Env1	A	10	5
Env2	B	10	3
Env3	C	5	3

Table 5.1: Parameters related to PL

Note here that, for each (Normal) distribution, we define a minimum accepted *PL* value equal to 3 *m*. Hence, if the generated *PL* value is smaller than this bound, a new value is generated until obtaining an accepted *PL* value. Such a setting aims to obtain realistic *PL* values and can be further adapted to represent different *PL* distributions.

Finally, having represented the relevant L3 line parameters, the following step of our process consists in making use of the various formal artifacts that we have elaborated to study the impact of these three illustrative distributions on the *PositionError* in order to properly set the balises separation distance. To this aim, the investigated query needs to be translated as a logical expression.

Expressing the investigated query as a temporal logic formula

In what follows, we mainly analyze how likely the uncertainty on the train position can exceed a certain threshold during the whole run of the train along the investigated L3 line, while considering specific PB/VB arrangement. As explained earlier in the manuscript, the property has to be expressed as a temporal logic formula to be analyzed by the model-checker. In this regard, the aforementioned feature can be formulated as follows:

$$Pr\,[<= bound\,]\,(<>\,PositionError > threshold) \tag{5.5}$$

where:

- *bound* denotes the time bound of the simulation procedure,
- *PositionError* is the allowed train position error variable,
- *threshold* is the monitored limit value for the allowed error (e.g., 105 *m* obtained from the reference L2 line),
- <> is the *eventually* temporal operator. Namely, for φ some given predicate, <> φ means that there exists some state from now on that satisfies φ.

Furthermore, it is sufficient to adapt the threshold value in the previous formula in order to evaluate various error bounds. Accordingly, the SMC tool executes an important number of runs on the system model to explore the reachable states, for each generated query (representing a different threshold). At the end of each run, the algorithm checks whether or not the query is satisfied.

5.3.2 Analysis phase

Our analysis is performed by means of the model-checking facilities offered by UPPAAL. As a matter of fact, we should indicate that we used both the graphical TA models discussed in the previous subsections, but also a number of textual TA models (".xta" files) and ".q" query files that we generated automatically by means of Python scripts we have developed. Indeed, since we seek to investigate different track (PB/VB) configurations, while considering various uncertainty levels, we took advantage of the possibility offered by UPPAAL to perform model-checking using command-lines on the basis of TA models and query textual files. It is also worth mentioning that depending on the available computational capabilities, we can easily adapt the levels of accuracy and confidence of the model-checking results (resp. ϵ and α statistical parameters), as well as the level of details in the investigated models.

In this subsection, we are interested in obtaining the numerical results allowing to answer the previously raised questions, namely:

- *"How likely the uncertainty (i.e. error-bound) on the train position can exceed a certain value?"*
- *"How should the balises be arranged on the L3-FVB line in order to guarantee that the uncertainty (i.e. error-bound) on the train estimated position does not exceed a predetermined threshold?"*

With respect to the first question, one should consider the fact that the distance separating two (group of) balises is assumed to be constant. Therefore, the estimation of the bound of the *OdoError* component of the *PositionError* can be achieved without resorting to the use of formal models and associated verification techniques. Accordingly, the query expressed in formula 5.5 can further be specified to focus on the *BaliseError* parameter. Hence, the following query can be obtained:

$$Pr\,[<= bound\,]\,(<>\, BaliseError > threshold) \tag{5.6}$$

Basically, the results hence obtained shall be combined with the *OdoError* component related to the odometer error in order to answer the second question. Taking into account the particular configuration of the line studied in our case study, an additional decomposition of the analysis may involve the distinction between the track sections associated with each specific GNSS reception environment. In particular, this approach makes it possible to consider the parts of the track that share the same characteristics simultaneously and to draw common conclusions for these specific parts. In this regard, a condition on the active environment type is aggregated to the predicate of query 5.6.

$$Pr\,[<= bound\,]\,(<>\, ActiveEnvironment\ \&\&\ BaliseError > threshold) \tag{5.7}$$

where *ActiveEnvironment* represents either *Env1*, *Env2*, *or Env3* (cf. Table 5.1).

For various threshold values (e.g., from 1 to 35m), the SMC algorithm handles the associated query and estimates the probability that the *BaliseError* exceeds the investigated threshold in the active environment type. The obtained results are processed to obtain the charts shown in Figure 5.5. In particular, the results pertaining to the balise error are depicted via the orange plots, which establish the relation between the various error thresholds and the probability that these limits are exceeded by the balise detection uncertainties.

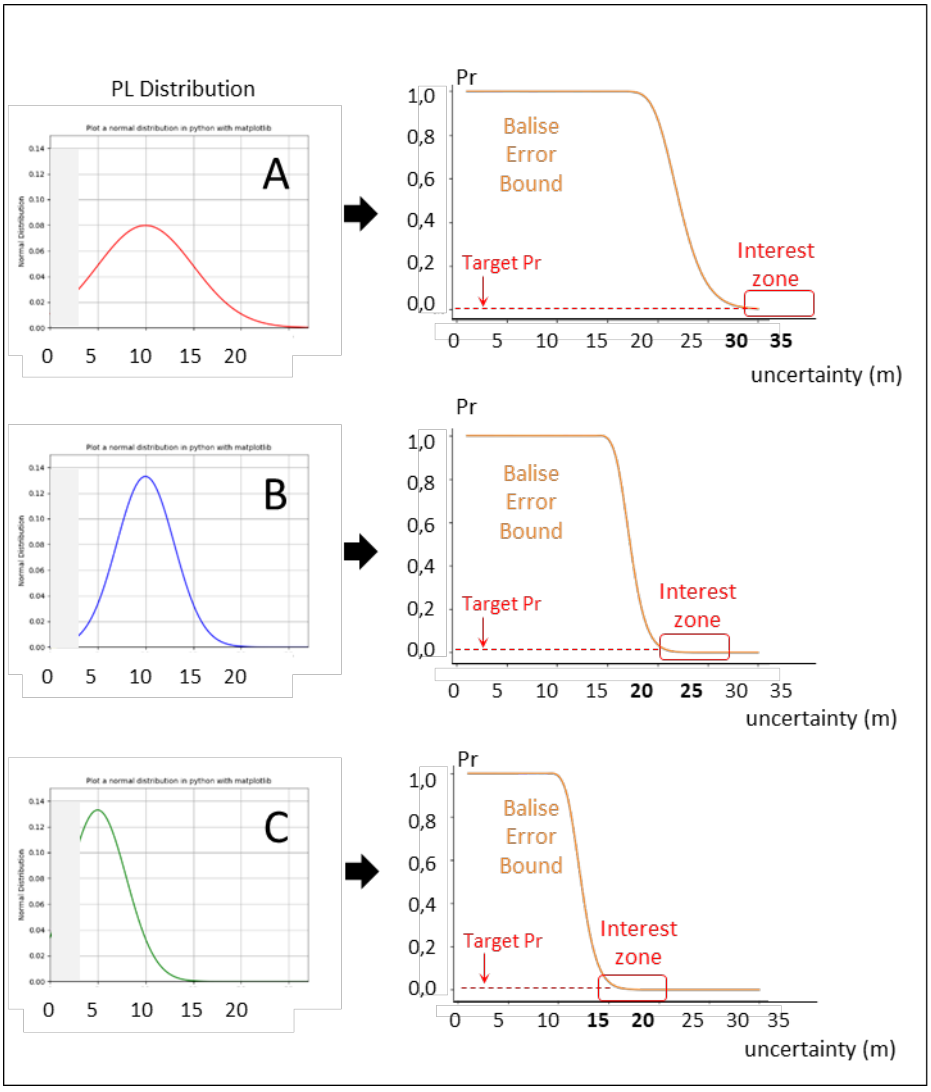


Figure 5.5: SMC Results on the Balise activation error bounds following the *PL* characterization models A,B, and C (with statistical parameters $\alpha = 0.00001$ and $\epsilon = 0.0005$)

At this stage, we recall that the objective of our current analysis is to define specifications on the positioning of the balises in order to constrain the uncertainty on the estimated position of the trains with a threshold value predetermined in advance. Moreover, we remind that such uncertainty includes the *BaliseError*, which depends strongly on the GNSS reception conditions at the time of the activation of a VB (via the PL) and, thus, cannot be known with certainty beforehand. Yet, a trustworthy value of this PL-related parameter still needs to be estimated as a reference indicator to set the balises locations. To this end, the results presented in Figure 5.5 are used, by estimating the probability of *BaliseError* exceeding a threshold value and further associating a degree of confidence to the individual values of the statistically predicted *BaliseError*. Accordingly, an adapted reference *BaliseError* can be fixed depending on the *'target confidence level'* (i.e. representing the accepted residual risk according to the safety targets).

5.3.3 Results interpretation and discussion

In this case study, let us consider a safety-related target defined as follows:

> *'The probability that the PL (actually computed following the activation of a balise) exceeds the pre-estimated reference BaliseError must be smaller than* 10^{-5} *with a confidence of* $0,99999$*.'*

Deduction of the *BaliseError* corresponding to the target probability objective

Considering this target probability objective (i.e., 10^{-5}), particular zones of interest (i.e., the uncertainty value corresponding to the target probability) are identified according to the results obtained previously. Especially, these zones (illustrated with red boxes in Figure 5.5) require an in-depth exploration. For that, the SMC tool parameters are further adapted accordingly as follows: $\alpha = 1 - 0.99999$ and $2 \times \epsilon = 10^{-5}$). In fact, such parameters tuning intends to generate more precise results around the identified zones of interest. Consequently, the interest zones corresponding to the *PL* distributions addressed in this case are zoomed in for more precision. For instance, the results associated with the $Normal(10:3)$ distribution are presented in Figure 5.6.

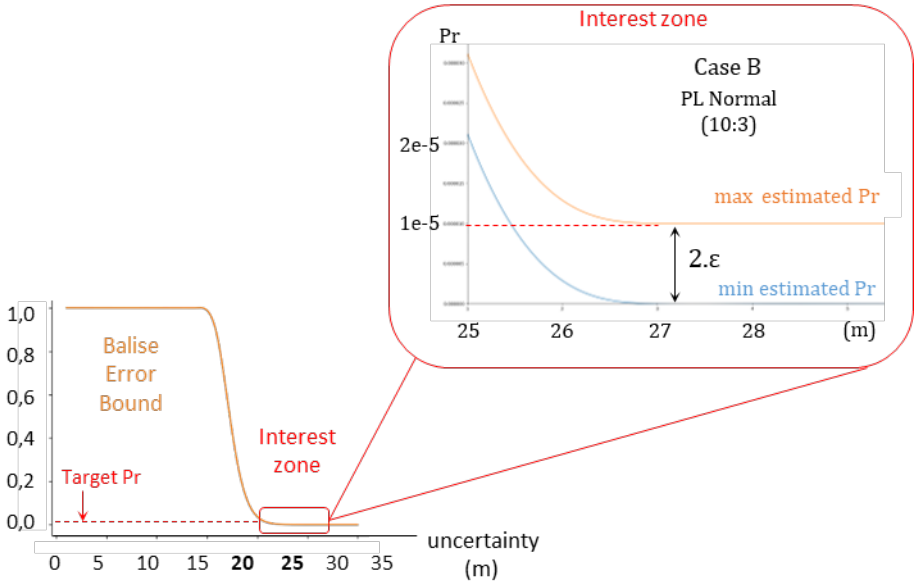


Figure 5.6: Zone of interest with PL: $Normal(10:3)$, $\alpha = 1.e{-}5$ and $\epsilon = 5e{-}6$

Finally, the other *PL* distributions are addressed similarly, and the *BaliseError* values 37, 27, and 22.5 are retained based on the *PL* distribution $Normal(10:5)$, $Normal(10:3)$, and $Normal(5:3)$, respectively.

Investigating the *OdoError* component of the *PositionError*

Having established the *BaliseError* values associated with the balises activation, it is now necessary to consider the *OdoError* component of the *PositionError* before concluding on the balises

arrangement on the L3-FVB line. To do so, let us first denote by *MaxPositionError* the maximum tolerated value of the *Global train position uncertainty*. Then, we seek to allocate a margin on the potential Position Error to the two uncertainty sources (i.e., odometer and Balise activation). Concretely, the *MaxPositionError* can be expressed according to the following equation:

$$MaxPositionError = MaxOdoError + BaliseError \tag{5.8}$$

where:

- *BaliseError* represents the value obtained in the previous step of the analysis (i.e., see Figure 5.6),
- *MaxPositionError* is considered as an input parameter in our analysis (i.e., $105m$ obtained from the reference L2 line),
- *MaxOdoError* is the margin of position uncertainty allocated to the odometer system (see Figure 5.7).

In particular, we note that *MaxOdoError* is the only unknown parameter in equation 5.8, and can therefore be obtained easily:

$$MaxOdoError = MaxPositionError - BaliseError \tag{5.9}$$

On the other hand, as we assume the balises are arranged homogeneously in each environment type, the *MaxOdoError* parameter can be expressed as:

$$MaxOdoError = 5\,\% \times d'_{max} \tag{5.10}$$

where d'_{max} represents the maximum allowed distance between consecutive balises in the new L3-FVB line. Accordingly, it is therefore straightforward to infer d'_{max} as in relation (5.11) below:

$$d'_{max} = 20 \times (MaxPositionError - BaliseError) \tag{5.11}$$

Reporting the final results obtained

The results obtained following the previously presented methodology are reported in Table 5.2:

PL Distribution ($mean : std$)	*BaliseError* *(m)*	*MaxOdoError* *(m)*	d'_{max} (km)	PBs separation (km)	PB ratio (L2/L3)
(10:5)	37	68	1.360	13.6	14.7%
(10:3)	27	78	1.560	15.6	12.8%
(5:3)	22.5	82.5	1.650	16.5	12%

Table 5.2: Results

In the first column of Table 5.2, the different probabilistic distributions modeling the GNSS-signals reception conditions along the addressed L3-FVB line are displayed. In the second column, the associated *BaliseError* values established previously for each environment type are recalled (see. Figure 5.6). Then, considering a target *MaxPositionError* value of $105m$ (equivalent to the reference L2 line), the error margins allocated to the *OdoError* component of the *PositionError* (obtained using equation 5.9) are presented in the third column of the table. Based on such *MaxodoError*, the d'_{max} values are calculated according to the relation 5.11, and the corresponding results are presented in the fourth column of the table.

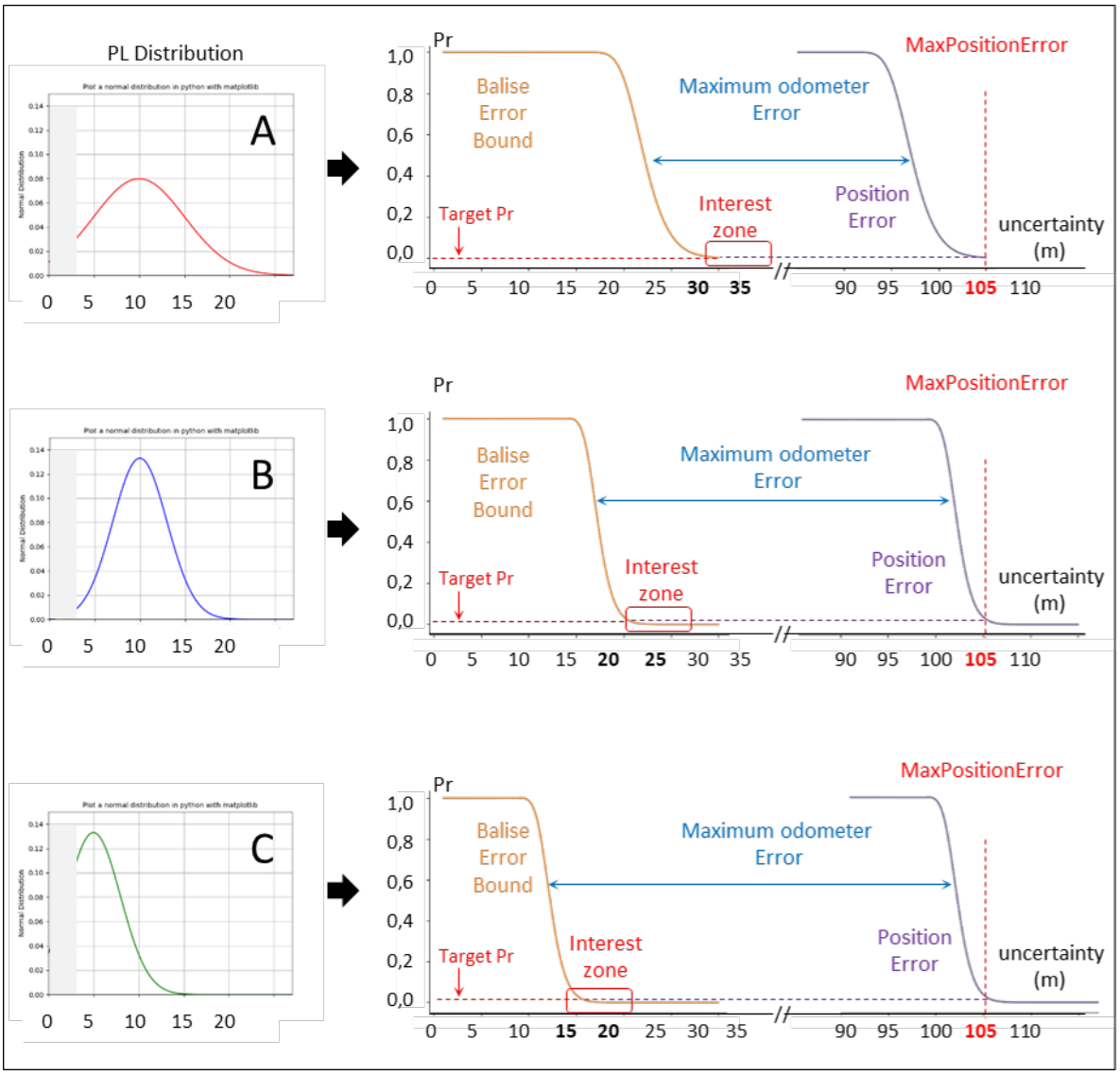


Figure 5.7: Calculation of the maximum odometer error according to each probabilistic *PL* distribution

Assuming the *PB-9VB* pattern adopted for the L3-FVB line covered in this case study, such configuration implies that only one out of ten balises is a physical balise. Thus, even if the balises are closer to each other in the new line, the PBs, in contrast, are much more widely spaced from each other (see the fifth column of Table 5.2).

In order to highlight the implications of these results, we note that for a similar uncertainty accumulation threshold ($105m$), the distance between two consecutive (groups of) PBs in this L3-FVB line is between 6.8 and 8.25 times greater than the equivalent distance in the reference L2 line ($13.6\ km - 16.5\ km$ compared to $2\ km$). In other words, this notably means that considerably fewer physical balises are required in the new L3-FVB to achieve comparable positioning performance as in the reference line. Concretely, if we compare the number of PBs needed in the new L3 FVB line respectively to their number in the reference ERTMS L2 line (see the last column of the table), one can notice that the number of PBs is reduced by more than 85% in the three investigated environments. For instance, this signifies that for a $100\ km$ long L3-FVB track section along which only the three types of environment studied in this case study are present (with a homogeneous arrangement of the balises *PB-9VB*), only 6 to 7 (groups of) physical balises are sufficient, whereas 50 (groups of) PBs are necessary under L2 operation (to achieve the same positioning performances). Furthermore, one can also notice that the lower the uncertainty on the value of *PL*, the more the balises can be spaced out on the line, which means fewer balises to be deployed (e.g., 12% for $PL\ Normal(5:3)$ vs. 14.7% for $PL\ Normal(10:5)$). It is therefore relevant to note that the obtained results highly depend on the *PL* distributions adopted as input parameters. From a more general perspective, we underline that the obtained FVB lengths (d'_{max}) are smaller than the block length of the reference ERTMS L2 line ($2\ km$). Consequently, more adapted MA can be computed as the MA stopping point can be selected with more flexibility. Hence, the line capacity can be increased. Besides, it should be noted that as such d'_{max} values stand for the maximum distance separating consecutive balises, the actual balise separation distance to be adopted can be smaller than the calculated d'_{max} value. As a result, less odometry error accumulation and even shorter FVBs can be obtained, thus making it possible for further increasing the line capacity. In this context, it is important to point out that such increase of the balises number is particularly justifiable and worthy, since 90% of the balises are virtual. Nevertheless, a physical limit for line capacity increase is related to the braking capabilities of the operated trains. Finally, it is worth noting that an analogous reasoning can be adopted to investigate different line layouts and *PL* distributions, so as to determine optimal cost/benefit ratio, while keeping control on the related risks.

5.4 Case Study 2: Addressing scenarios related to non-nominal situations

In the previous case study, we have presented an analysis that deals with the positioning of PB and VB balises on a new railway track to be operated according to the L3-FVB principle. In our study, we have assumed a nominal behavior of the GNSS positioning solution. Especially, such nominal conditions in which '$PE < PL < AL$' refer to the white triangle in the Stanford diagram presented in Figure 5.8.

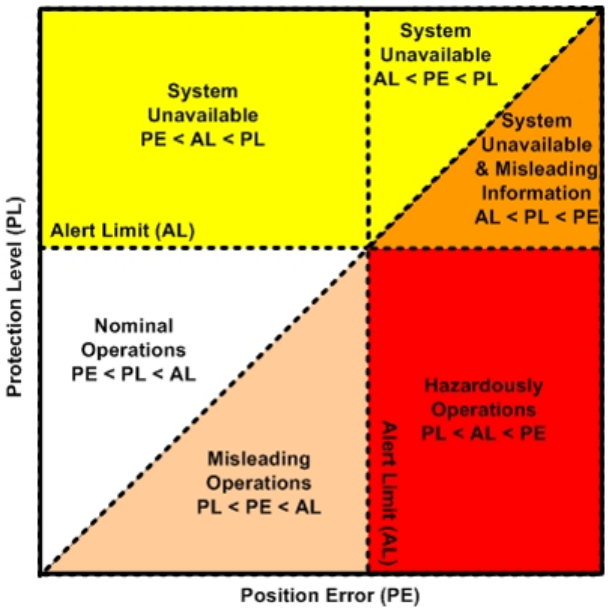


Figure 5.8: Operational conditions classification according to the Stanford diagram

However, it is logically admissible that more-or-less faulty behaviors can be encountered in reality; namely:

- Case 1 : $PL > MaxPositionError$
- Case 2 : $PE < AL < PL$
- Case 3 : $PL < PE < AL$

Accordingly, we are interested in these particular non-nominal cases in order to provide a more comprehensive analysis in the present section of this chapter.

5.4.1 The particular case of: $PL > MaxPositionError$

Here, we should first recall that upon the activation of a PB, the associated *BaliseError* uncertainty margin is bounded by the fixed value of 5 m. In contrast, no such a fixed maximum limit is defined for the uncertainties associated with the activation of a VB. Besides, large PL values can be reached, especially in harsh GNSS reception conditions. In this context, the *Alert Limit* (AL) parameter is used as an upper bound on the accepted PL values, instead. Consequently, if the

estimated *PL* is lower than the value of AL, the computed position is accepted and associated with a *PL* and a *'confidence level'*. On the contrary, if the estimated *PL* exceeds AL, the GNSS position is deemed unavailable and, hence, is rejected by the on-board system. This choice of considering an upper bound on the acceptable *PL* is particularly meaningful from an operational point of view. Indeed, a very high *PL* value implies an increased uncertainty on the estimated position of the trains. This translates directly into a significant increase of the operation 'headway' to be envisaged, and would significantly degrade the capacity performances of the concerned railway line. However, the appropriate value for this *AL* has yet to be determined. On the other hand, since the *PL* can reach important values, one could consider the case where the value of this latter is greater than the *PositionError* at the instant of the activation of a VB. It would therefore be reasonable to exclude such a *PL* value for the calibration of a more accurate position estimation (see Figure 5.9).

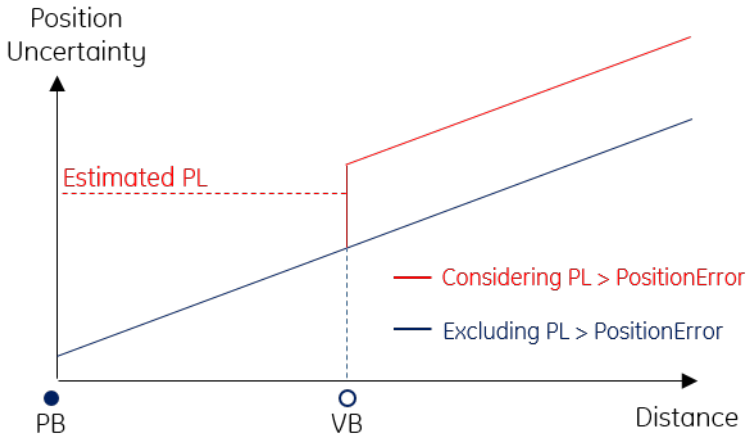


Figure 5.9: Comparison of the position uncertainty evolution following the consideration or exclusion of the *PL* values exceeding the current position uncertainty at the time of a VB activation

Following the same reasoning, it can then be established that the value of the *AL* to be fixed must not exceed *MaxPositionError*. In fact, setting such an upper bound (equivalent to the maximum uncertainty that could be reached) on the value of *AL* is justified as *PL* values exceeding *'PositionError'* ($PL > PositionError$) are, automatically, not considered for the recalibration process.

5.4.2 Unavailability of the GNSS position

As previously stated, the *AL* value indicates the threshold value that the *PL* can take and below which the GNSS position is accepted. In the opposite case (i.e. $PL > AL$), the GNSS position is declared as unavailable. Moreover, if this unavailability of the GNSS position persists during the whole activation area of a VB (i.e., its expectation window), the 'position matching' condition (necessary for VB activation) cannot be satisfied. Therefore, the corresponding VB position cannot be used as a new reference position to correct the odometer error accumulated until that point. In particular, this non-activation of the balise location is referred to as the *'missed balise'* event. In this case, the on-board system of the train must react to this situation by updating the identity of the expected balise so that it corresponds to the next expected balise (in the list

of balises to be detected along the train itinerary). Nevertheless, it should be noted that the uncertainty component *OdoError* is no longer bounded by the threshold value corresponding to the distance between two successive (group of) balises, but is instead proportional (i.e., by 5%) to the double of this distance (under the assumption that only one group of balises has been missed).

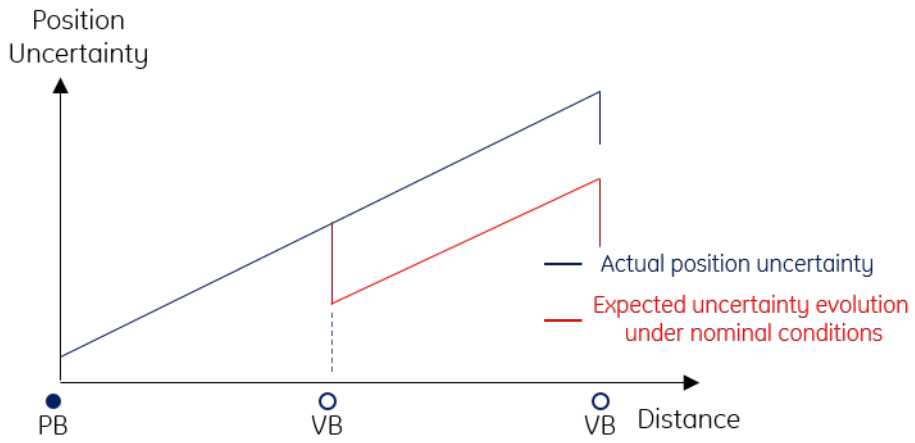


Figure 5.10: The evolution of the position uncertainty following the non activation of a single VB.

Together with the residual uncertainty related to the last balise activation *(BaliseError)*, one can easily observe (cf. Figure 5.10) that the global uncertainty threshold on the train position *(PositionError)* surpasses the value established according to the nominal conditions (i.e., following the approach used in the first case study treated in this chapter). In order to deal with this challenge, a more extensive probabilistic analysis must be performed with the objective of better characterizing and understanding the possible outcomes following such a balise missing scenario. With respect to this same perspective, a risk acceptability threshold must be fixed beforehand, and the system specifications must be adapted to ensure that the probability of occurrence of such a situation is sufficiently low. At the same time, protective barriers need to be set so that such a feared event does not result in undesired safety events.

On the other hand, it should be noted that if several balises are missed successively, the value of *PositionError* increases further and can largely exceed the desired margins (see Figure 5.11).

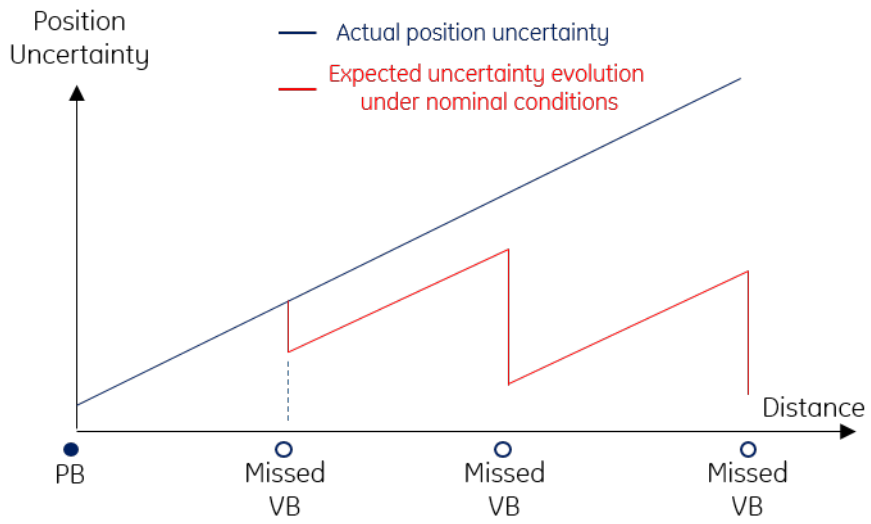


Figure 5.11: The evolution of the position uncertainty following the non activation of multiple VBs in a row

In this context, the requirements on the positioning system can be further specified in order to avoid such large overruns. For instance:

> *'It is not allowed to miss two balises in a row.'*

Or alternatively:

> *'the probability of missing a balise, provided that the previous balise was already missed is below a certain specific threshold.'*

Regarding the above properties, it is important to recall that the activation process of VBs depends only on the GNSS position computed within the expectation window. Therefore, the probability of detecting or missing a balise is independent of the detection history (i.e., if the previous balise was missed or not). This concept of independent probability can be translated mathematically through the following equations:

$$P(X_1 \cap X_2) = P(X_1) \, . \, P(X_2) \tag{5.12}$$

where X_i denotes the event *missing the* i^{th} *balise*.
Accordingly, the probability of X_1 knowing X_2 becomes:

$$P(X_1 \mid X_2) = \frac{P(X_1 \cap X_2)}{P(X_2)} \tag{5.13}$$

$$= \frac{P(X_1) \,.\, P(X_2)}{P(X_2)} \tag{5.14}$$

$$= P(X_1) \tag{5.15}$$

Which means that the probability of $P(X_1 \mid X_2)$ is equivalent to the probability of X_1 independently from $P(X_2)$. Therefore, this notably implies that the probability of missing multiple balises consecutively can be expressed by the following formula:

$$P(X_1 \cap X_2 \cap .... \cap X_n) = \prod_{i=1}^{n} P(X_i) \tag{5.16}$$

Thus, the resultant of this formula should naturally be relatively small compared to the probability of missing a single balise.

Nevertheless, the presence of common causes of failure, such as those related to the GNSS receiver itself or the GNSS signal reception conditions, further complicates this study. Furthermore, the potential vulnerability of GNSS systems facing spoofing and jamming phenomena is an additional parameter to consider. Consequently, guaranteeing that the probability of ending up in an undesirable situation is sufficiently low to be accepted (when using GNSS-based train localization) remains an open issue. Therefore, given the above-mentioned considerations, it might be advisable to maintain a PB ahead of some points that are considered critical (such as the junctions between several lines), as long as these challenges have not been overcome.

5.4.3 The misleading information case: *PL < PE & PL < AL*

The case discussed in this subsection is related to the so-called *'GNSS Miss-leading Information'*, including both:

- Miss-leading Information, denoted *MI*: $PL < PE < AL$
- Hazardous Miss-leading Information, denoted *HMI* : $PL < AL < PE$

Concretely, these situations are obtained when: $PL < PE$ while $PL < AL$ and represent the consideration of a position judged by the system as valid, while it is not, actually. Therefore, this particular state represents the most critical case from a safety point of view. In the context, we are particularly interested in the considering the *IR* associated with the estimated GNSS-positions and the impact of this *IR* parameter on the headway. The findings of this investigation are of particular relevance in the context of the evolution towards implementing the *'Full Moving Block'* operation principle. Indeed, contrary to the cases we have discussed previously (dealing with the 'FVB' principle), the block length is no longer a parameter to be considered for spacing trains on the lines operating according to the *'FMB'* principle. On the other hand, the risk that the *PE* might exceed the estimated *PL* boundary without the system noticing it has to be carefully anticipated and concretely translated into a safety distance to be included in a comprehensive *safety margin*.

Engineering safety margins

It should be noted here that the engineering of margins is a topic that has already been raised in various projects such as S2R-X2R1 [1]. In particular, the parameters to be considered when calculating safety margins have been discussed as part of the development of the system requirements. In fact, it has been agreed that a safety margin has a safety justification in a set of scenarios, whereas it provides for performance or operational stability in other scenarios. Furthermore, it has been mentioned that the safety margin is entirely dependent on the specific situation and is not always needed, as reported in section 8.2 of the deliverable "D5.2: Moving Block Operational Engineering Rules" (Shift2Rail X2Rail1 2016). Finally, it has been admitted that the engineering of margin function remains a pending open issue, and therefore concluded that future work needs to be planned in this regard. Concretely, the involved tasks should focus on identifying the particular scenarios where a margin is needed, in addition to the various parameters to be considered in each situation. Consequently, a set of engineering rules needs to be developed to support the infrastructure managers in engineering safety margins. In particular, the analysis provided in this subsection falls within this context. Concretely, we identify the use of GNSS-based solutions to perform the train localization function as a scenario that requires the adoption of a safety margin. Moreover, we point out the probability of being in a misleading information situation (i.e., $PL < PE$) as a relevant parameter to be considered in order to set the related safety margin. In other words, we can infer that the IR parameter impacts the size of the safety margin to be adopted. We consequently investigate the translation of such information into a tangible result to be used as a safety-related rule constraining the safety margin to be implemented. From an operational perspective, one should underline that such a safety margin directly impacts the headway, i.e., the distance separating two succeeding trains, together with the uncertainty of the position and the braking distance (see Figure 5.12).

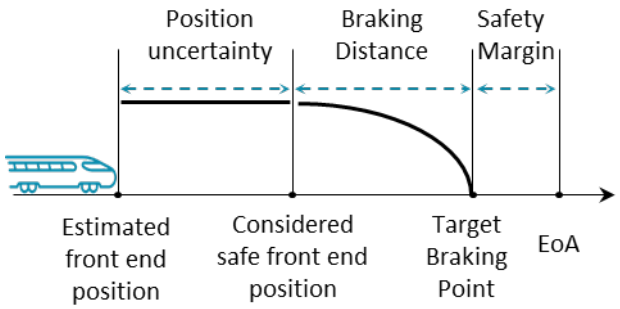


Figure 5.12: The various components of the safety distance to implement

Besides, it should be noted that this margin also includes a number of distances that are set to encounter the potential effects of various phenomena, including:

- Communication delays between train and trackside equipment,
- Human factor such as those related to the reaction time of the driver (for braking for instance),
- Intrinsic response time for the on-board technical systems such as when an emergency braking is activated.

[1] www.projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

Focus on the GNSS IR-related safety margin

In our case study, we pay particular emphasis to the safety margin component related to the *IR* parameter. Moreover, as the formal model developed along the present work is based on modular features, it is made possible to perform the assessment of this specific *IR-related* parameter while preserving the flexibility of including the complementary aspects gradually. This further justifies the adoption of a model-based analysis to address such questions.

In a comparable manner to the one employed for the *PL* investigation discussed in the first case study of this chapter, we propose to consider the *IR* parameter through a probability distribution to be included in the Uppaal automata model. In fact, since the *IR* is intended to represent the risk that the information provided by the GNSS system is unreliable, the objective of the derived probabilistic distribution is to assign a probability value to the gap values $PE - PL$, given that the *PE* exceeds *PL*. Accordingly, we should underline that only positive values are addressed in the probabilistic distribution, since the *IR* related case is conditioned by the fact that *PE* is larger than *PL* ($PL < PE$). In probability theory and statistics, such a case where only the positive magnitudes are recorded, may be addressed by adopting *"a folded distribution"*. Concretely, a distribution is called "folded" when probability mass to the left of $x = 0$ is folded over by taking the absolute value. An illustration of such *"a folded distribution"* is presented in Figure 5.13, where the folded normal distribution ($Y = |X|$) is a probability distribution related to the normal distribution (Given a normally distributed random variable X).

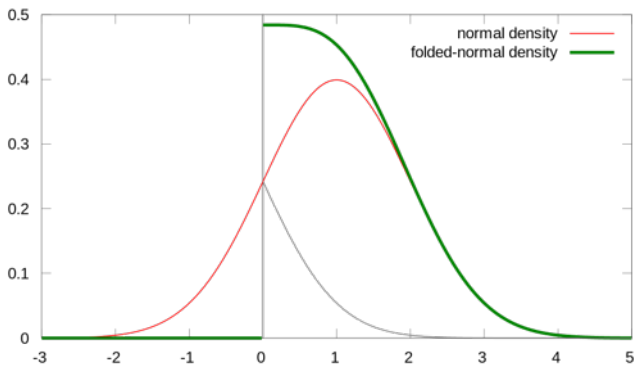


Figure 5.13: Probability density function for a folded-normal distribution (*mean* = 1 and *standarddeviation* = 1).

Realistic characterization of the IR parameter

If we consider the multiple contributions dealing with the "Fault Detection and Exclusion" issue in the context os GNSS based localization, a common point that emerges is that the vast majority of these works aim to improve the confidence that can be placed in the GNSS positioning information (Jinling Wang and Ober 2009; Nourdine Aït Tmazirte et al. 2014; Yang et al. 2014; Zhu et al. 2018; S. Wang et al. 2020; Sun et al. 2021). This includes minimizing the risk that the actual PE exceeds the estimated *PL*. Thus, this can be translated statistically by a maximum probability around of the difference value $PE - PL = 0$, which decreases as the PE value deviates from *PL*. In other terms, it is less likely to reach a large gap between *PE* and *PL*, than to slightly exceed the *PL* value. On the basis of such a reasoning, the above example of folded distribution can be further adjusted to correspond to a "half-normal distribution" (see Figure 5.14). In fact, the

half-normal distribution is a special case of the folded normal distribution, with the particularity of representing a fold at the mean of an ordinary normal distribution with mean zero.

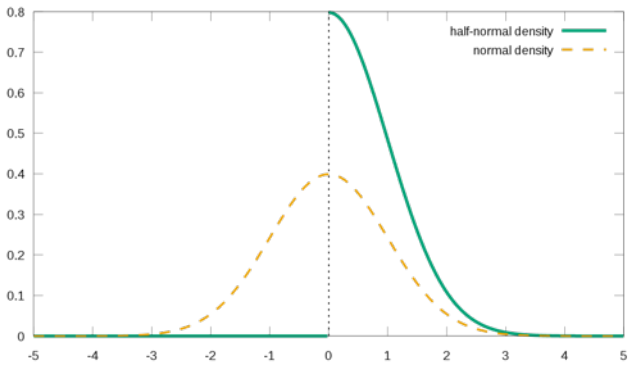


Figure 5.14: Probability density function of the half-normal distribution (*mean* = 0 and *standarddeviation* = 1).

At this stage, it is important to recall that our objective is to conceptualize an approach that investigates the impact of the IR on the safety margin to be maintained. Therefore, the employed probabilistic distributions are intended to be purely illustrative of the approach. Complementary work must be conducted to provide more realistic models. Nevertheless, it should be noted that the model is developed in such a way that allows the inclusion of different distributions according to the specific needs of the study.

If we refer to the case of a *'Half Normal distribution'*, the Uppaal tool used to develop the formal model based on automata supports two basic functions that can be combined to obtain the desired *'Half Normal distribution'*, namely:

- *doublerandom_normal*(*doublemean*, *doublestddev*): to generate a pseudo random number that is distributed according to *Normal* (Gaussian) distribution for a given standard deviation *stddev* and a *mean* = 0,

- *doublefabs*(*double*): to obtain the absolute value of double argument, and only consider the positive values generated according to the previous normal distribution.

Finally, it remains to define the value of the parameter *stddev* so that the distribution obtained is representative of a realistic situation. To this aim, we propose to adapt this value so as to obtain a maximum probability equal to the IR when ($PE - PL = 0$) (see Figure 5.15).

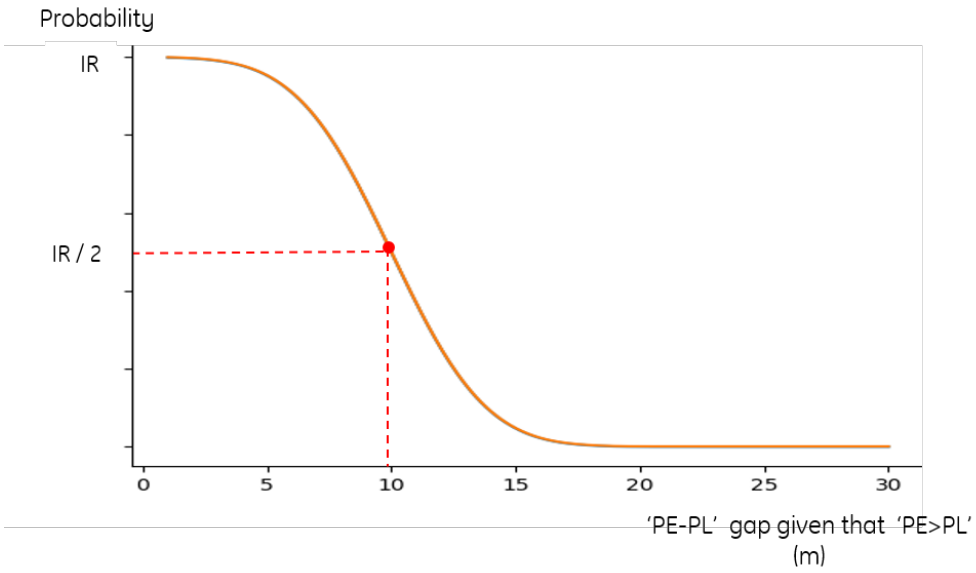


Figure 5.15: Setting the Safety Margin related to the IR.

Results interpretation

In conclusion, the obtained results may serve as a basis to perform the Engineering of margin task in respect to the risk of using misleading position information. Concretely, the interpretation of such data means that, for instance, the risk that *"the calculated safety distance to maintain from a danger point is actually not sufficient"* is equal to the IR if no safety margin is employed (provided that the safety distance is calculated based on potentially misleading information). In contrast, such probability can be reduced if a safety margin is adopted (e.g., considering the illustrative distribution depicted in Figure 5.15, the adoption of a 10 m safety margin reduces such probability to half).

However, we should underline that allocating a more important safety margin increases the distance separating two succeeding trains. Thus, leading to a fall in the potential line capacity. Besides, not allocating a sufficient safety margin implies that the risk that *the actual train position violates the necessary safety distance from a danger point* is higher. Accordingly, the probability of activating an emergency brake, whenever the system notices afterward that the information used is faulty, increases. Recall here that such a braking has a prejudicial impact on the overall train traffic schedule (e.g., discontinuity and disruption) which further impairs the performance of the line. Not to mention the physical damage that can be inflicted on the infrastructure due to such braking. All these elements explain the importance of well-balanced safety margin parameters, both from a safety and operational stability points of view.

5.5 Conclusion

The introduction of GNSS-based solutions for train positioning has been consistently deemed to be promising. Yet, the adoption of this localization system for such a safety-critical function is conditioned by the procurement of sufficient safety evidence.

With this aim, we suggested in the first chapters of this manuscript to employ a model-based approach. In particular, the research work conducted during this thesis resulted in the development of a set of formal models that represent the behavior of the train localization system, as presented in the precedent chapter of this dissertation.

This model is structured according to a modular and parameterizable representation logic, which allows for emulating the behavior of the expected train localization performances along a railway line involving some given configuration of PBs and VBs. On the other hand, the analysis carried out throughout this thesis allowed us to identify the statistical model-checking (SMC) technique as being adapted to the investigation of such GNSS-related issues. Accordingly, on the basis pf the elbaorated models, we took advantage of the SMC feature supported by UPPAAL to check a number of performance and safety-related properties while considering specific operational scenarios. Concretely, we firstly recalled the functioning principle of the SMC in addition to the formalism to be adopted in order to express the investigated properties. Then, three illustrative classes of GNSS-signals reception conditions along a rail line were represented in our models, and analyzed to study the impact of these parameters on the global uncertainties associated with the estimated train position. The results obtained based on the formal model and the probabilistic estimation feature of the SMC permitted us to set recommendations on the balise configuration and positioning along a newly designed ETCS-L3 operated according to the FVB principle and under nominal conditions.

Since a safety-related study cannot be considered as complete without considering degraded operation aspects, in a second case study, we addressed the outputs of the GNSS-based location system under non-nominal operating conditions. In this context, we covered three distinguished situations, including the non-obtention of a valid uncertainty reset value at the time of the activation of a VB, and the unavailability of the GNSS-position leading to the non-activation of VBs. Finally, the use of misleading information was examined, with a particular focus on the associated Engineering of the Margin Task to prevent the risks resulting from such a hazard.

Part III

Conclusions

Chapter 6

Conclusion

6.1 Contributions

Satellite technologies are considered as a strategic facility in the rise of advanced railway Control-Command and Signaling systems. This means is particularly beneficial in the advent of the ERTMS CCS standard, in which the foreseen introduction of embedded GNSS-based solutions to fulfill the railway localization function represents a major breakthrough in terms of railway operation and asset management. Besides modernizing and optimizing railway operation, thanks to the benefits brought by the deployment of GNSS-based localization solutions, the economic viability of certain regional railway lines can be restored, hence preventing their closure. Nevertheless, despite the recognized benefits that such a technological solution can bring to the railway sector, the use of GNSS to perform such safety-related localization function raises many issues for railway stakeholders, particularly in terms of specification and safety management.

Furthermore, as the classical safety methods commonly employed in the railway domain do not permit to consider some particular aspects related to the use of GNSS in the railway environment, more adapted safety analysis methods must be deployed to deal with the specific issues related to this system. In particular, such methods shall enable considering the impact of the dynamic environment surrounding the GNSS-based localization system. Thus, it is necessary to carry out research works aiming to help make it possible to certify such satellite-based train positioning solutions. One can also mention that deploying GNSS-based train localization is key to implement autonomous train operations.

The present thesis was conducted in the above-mentioned context, with the objective of contributing to the proposal of a safety assessment means adapted to the challenges related to the use of GNSS-based positioning solutions embedded on board trains. On the whole, the contributions presented in this manuscript can be synthesized as follows:

Chapter 2: *Safe train localization including satellite positioning: rail context, challenges, and research issues*

- This chapter has presented the importance of the localization function in railway control-command and signaling (CCS) systems. As the European CCS is considered in this thesis, particular attention has been paid to the different levels of ERTMS.

- The analysis of the currently deployed ETCS Levels 1 and 2 has emphasized that the reliance on trackside equipment to detect train positions and determine track occupancy status represents a physical limitation inhibiting the increase in rail capacity. The ERTMS Level 3 requires embedded localization solutions to overcome such limitations. In fact, the features offered by realizing the train localization on-board potentially allow for totally or partially replacing the physical equipment installed today along railway tracks to ensure train localization and occupancy detection (e.g., track circuits, balises, axle counters). Consequently, such reduction of physical devices leads to direct savings in terms of infrastructure installation and maintenance costs. Furthermore, a substantial capacity gain is expected since more flexible and efficient operation modes can be implemented, such as *Full Moving Block (FMB)*, *Fixed Virtual Block (FVB)*, or *virtual coupling*.

- A common aspect connecting FMB and FVB consists in the fact that their implementation relies on the introduction of satellite localization, especially to enable the adoption of the VB concept, which is the reason behind the specific focus on how localization is currently performed and how GNSS can intervene.

- Finally, the description of the operating principle of GNSS systems allowed us to highlight various challenges related to the safety of using GNSS systems in the railway domain, namely:

  – the new risky behaviors related to the uncertainty on the computed results,

  – the dynamic context in which trains evolve on a railroad line,

  – the fact that functional behaviors have to be tested under multiple conditions in order to manage safety.

Chapter 3: *Which safety approach for complex railway systems?*

- The certification of GNSS-based train localization solutions is a prerequisite for their actual deployment. However, as the GNSS was initially developed for avionic use, the investigation of their employment in the constrained railway environment has brought to light new and previously unaddressed challenges. For instance, the satellite signals used to calculate the train position can be blocked or reflected by various elements in the railway environment, such as buildings, tunnels and vegetation. Thus, as the environment in which the train evolves may affect the obtained result, guaranteeing the proper functioning of the components intervening in the localization function is not sufficient anymore to ensure the reliability of the output position information.

- To overcome the new challenges that are specific to the use of train positioning through GNSS, the development of a systemic approach is required. Accordingly, in this chapter, we first present the current railway safety framework on which we must rely in order to propose the new methodology. Along with this presentation, a range of existing methods for operational safety analysis has been explored.

- Given the complexity of the system under study, as well as the financial and temporal costs resulting from on-site experimental studies, the use of zero-on-site methods has been shown to be essential. This conclusion has notably oriented our attention towards model-based methods, while stressing the importance to establish a faithful transcription of the behavior of the studied system.

- In addition, this chapter described the methodological framework for modeling complex systems with an emphasis on the complex behaviors associated with GNSS, as well as the modeling techniques that can be employed to describe them.
- Considering the robust logical foundation associated with the mathematical reasoning used in the framework of formal methods, we were able to conclude on the relevance of adopting such approaches to address our research problem.
- In conclusion, this chapter has allowed highlighting guidance on an appropriate methodological basis for handling the safety issues related to GNSS systems. Consequently, our choice is directed towards a model-based approach that relies on the use of the Model-checking formal-verification technique.

Chapter 4: *Formal model-based approach to address the GNSS-based train positioning*

- The second part of the manuscript has been dedicated to the presentation of our contribution. In this context, Chapter 4 has focused on the detailed description of the methodology developed during this thesis.
- The first step consisted of identifying the main relevant aspects that must be addressed throughout the application of the proposed approach.
- The main features of the approach have been summarized through a methodological scheme, including: the various aspects to be addressed during the development of the behavioral model, the data sources to be explored in order to feed the knowledge on the represented system, as well as a reminder on the significance of the inputs related to the properties to be verified at the end of the study process.
- A set of modeling requirements were established to help obtain a faithful representation of the modeled system, especially considering the specificities of the studied system (i.e., dynamic evolution, probabilistic behavior).
- Accordingly, the appropriate modeling tools were selected, and the following step addressed in this chapter focused on the representation of a number of features related to the behavioral model of the system (i.e., a transcription of the train dynamics, the evolution of the train position error bound, and the balise activation process).
- Finally, as the developed modules intend to be re-usable, a set of configurable parameters related to the surrounding environment, the balises configuration on the lines, and the expected behavior of the virtual balises in each environment type, were set. Accordingly, the adaptation of such input parameters allows for representing various scenarios that can be encountered in railway operational conditions.
- In the end, we brought the attention of the reader to the fact that the models proposed during this instantiation of the approach have been developed using the formalism of communicating timed and probabilistic automata that offer a modular representation adapted to complex systems.

Chapter 5: *Safety and performances analysis: two case studies*

- In the last chapter of this manuscript, we intend to highlight the applicability of the methodology detailed in this thesis to practical use cases of railway operation.
- Accordingly, we first distinguish two types of situations: operation under nominal conditions, and operation under non-nominal conditions.
- Then, adopting the SMC verification principles, we addressed the problem regarding the positioning of the virtual balises along an ERTMS L3 line.
- This first case study has allowed us to highlight the benefits that railway stakeholders can gain from using the proposed model-based methodology. Concretely, the probabilistic and dynamic features supported in the model permit to emulate the expected behavior of the virtual balises in each environment. For that, a set of probabilistic distributions are used to represent the potential outputs calculated following the activation of the VBs. Moreover, we show that other mathematical models can easily be encoded as model inputs for a more accurate description of the VB related results.
- According to the statistical results obtained using the SMC algorithms, the user can conclude on recommended specifications related to balises' spacing in order to meet some predefined performances in terms of estimated position uncertainties and bounds.
- The second part of this chapter illustrated how various properties describing the risks encountered following some identified errors can be addressed using the same approach. Thus, by taking advantage of the modularity and configurability of the developed models, a wide range of relevant operational situations can be addressed.
- Accordingly, one can conclude that the approach proposed in this thesis clearly illustrates how formal methods can be advantageously used as a decision support tool for both the design of the system and its safety analysis for certification.

6.2 Perspectives

Whilst the present contribution investigated a roadmap towards Safety and Operational Performance Evaluation of GNSS-based railway localization systems using a formal model-based approach, several issues have been raised and still remain to be addressed. Accordingly, further extensions need to be introduced in the next improvements of the proposed approach. More specifically, such iterative improvements, in the short and long term, should cover several areas, including: refinement of the behavioral model, expansion of the scope of the investigated safety and performance properties, and the development of a more structured process for the application of the methodology. More details are given in what follows.

Refinement of the behavioral Model

In our contribution, the behavioral aspects related to the GNSS-based train localization are represented throughout a set of synchronized and communicating modules. Such a modular representation is intended to tackle the complexity of the addressed system, and paves the way for incremental modeling of various relevant features.

Taking advantage of such a characteristic, a natural progression of this work is to represent the Movement Authorities (MA) communication mechanism between the train on-board and the

RBCs. MA is, indeed, the primary means of providing instructions regarding the safe operation of trains, by taking into account the constraints of the railway network and the positions of the trains operating on this network.
In a different context, a number of research works that are available in the literature are interested in improving the performance of GNSS localization systems through the adoption of algorithmic solutions, such as Fault Detection and Exclusion (FDE) or Receiver Autonomous Integrity Monitoring (RAIM) (Jinling Wang and Ober 2009; Blanch, Walter, and Enge 2010). In the current version of the models, such features are not represented. Hence, further studies regarding the role of these barriers (i.e., FDE and RAIM) would be worthwhile. Besides, despite addressing the VB concept, the work presented in this manuscript did not focus on the settings of the '*expectation window*'. Thus, further research investigating a more accurate representation of this aspect is strongly recommended. Moreover, it is worth noticing that all the automata models implemented via the Uppaal tool are considered as templates. In particular, such a feature enables duplicating each of the automata modules via a set of identification variables. Hence, the emulation of multiple trains operating in a rail network can be achieved in order to investigate specific multi-trains scenarios. Finally, the modeling work carried out during this thesis has been hindered by some limitations inherent to the chosen modeling tool. Indeed, despite the numerous functionalities supported by Uppaal, Version 4.1.26 does not support the analysis of floating-point variables and operations in the symbolic queries (only integer variables are allowed). Concretely, the only valid use of floating-point operations is when they do not influence the behavior of the model (i.e., floating-point can be safely ignored and abstracted away). Thus, the variable expressed using hybrid clocks (e.g., train speed and acceleration) had to be further represented in a discretized manner. However, besides the combinatorial explosion, such a discretization process introduces an offset gap inherent to the model. Consequently, further research might explore formal modeling tools that allow for tackling such a limitation while proposing a Statistical Model Checking means that can be used for the verification of safety and performance properties.

Expansion of the scope of the investigated safety and performance properties

In the present work, we mainly focused on the uncertainties related to the protection level in order to provide at least the same capacity that would have been obtained under ETCS L2 operation. In future works, we intend to consider specific hazardous scenarios that can arise, such as the train collisions, by considering a given localization integrity risk. Some comprehensive safety indicators can then be determined to such scenarios. In so doing, the outcomes of our study can be integrated to characterize the likelihood of the initiating events related to the localization function, in the scope of these scenarios. In addition, we intend to extend our models to cope with further operational principles, such as the case of operation under full moving block or virtual coupling. In a related context, operational performances related to such advanced and dynamic principles can be investigated. For instance, future contributions might focus on the probability of emergency brakes following the violation of safe separation distances between trains. It should also be noted that the resulting abrupt train deceleration often leads to noteworthy alteration of the operational schedules, in addition to damage of the railway infrastructure. Accordingly, further optimization work can be conducted on the speed profiles of the running trains to avoid such unwanted braking. Regarding the Movement Authorities (MA), the related transmission mechanism may induce temporal delays prior to applying the instructions communicated to the trains. Thus, the impact of such a response time must be investigated (Baccelli et al. 1992; Addad, Said Amari, and Lesage 2011; Ammour and Saïd Amari 2015; Lajimi et al. 2016; Tamssaouet and Saïd Amari 2018; Himrane, Ourghanlian,

and Saïd Amari 2022).
While the quantitative results exposed in the present thesis mainly focused on train operations under nominal conditions (i.e., the appropriate positioning of the balises along the railway line in order to maintain a satisfying train-position uncertainty under nominal conditions), a natural progression of this work is to consider the analysis of the performances of the system in faulty and non-nominal conditions. Accordingly, discussions in Section 5.4 illustrates the use of the elaborated model to cover such a non-nominal behavior. In particular, the works of (Sallak 2007; Sallak, Schön, and Aguirre 2013; Martinez, Sallak, and Schön 2015; Qiu et al. 2014a; Akrouche et al. 2022) should be explored to allow the assessment of reliability and availability parameters despite the presence of uncertainties related to the use of GNSS-based train positioning. Moreover, such a study can cover the impact of Electromagnetic interference (EMI) caused by electric/electronic devices that are present in the railway environment. Furthermore, the analysis of security against adversarial attacks (i.e., intentional perturbations resulting from spoofing and jamming) remains a critical aspect that should be covered in parallel to safety analysis (Aktouche et al. 2021). Finally, specific faults can be explicitly injected into the models to simulate the malfunction of particular features of the system.
In the end, the deployment of the proposed approach in a real case study is essential to confirm the benefit of adopting such a formal model-based methodology to address the introduction of GNSS-based train localization.

Development of a more structured process for the application of the methodology

Broadly speaking, a number of issues still need to be addressed to help implement formal models and verification techniques in evaluating the safety of GNSS-based localization function in railways. In particular, a fine characterization of the rail environmental conditions in terms of GNSS reception quality remains a key element conditioning the adoption of GNSS-based train localization. This can be obtained by means of measurement campaigns. In fact, such a characterization allows for establishing realistic models that describe the behavior of the on-board localization function in a trustworthy way. In the same context, further specification of requirements work is needed to address the structuring of GNSS databases so as to cover the reception conditions along the rail lines in the most extensive and accurate possible manner. On the other hand, the present contribution was initiated with the objective of laying the foundations of a methodology that can be adapted to address the particularities of GNSS positioning systems in the railway context, especially to evaluate safety and performance properties. Nevertheless, additional work must be carried out in order to better structure the modeling process related to the proposed approach. Such a task could be inspired by the contributions of (Kamdem Simo et al. 2021), and should help to better associate the various modeling activities to the different phases of the system development process. For example, such structuring may involve adopting an explicit and formalized goal-based approach to help build a compelling safety case.

Finally, these complementary efforts will enable to better specify and highlight the intertwining of this approach in a global certification process involving railway localization systems using GNSS.

Bibliography

(EU) No 2015/1136 (July 2015). *Commission Implementing Regulation, Amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment*. European Regulation. The European Commission, Official Journal of the European Union.

(EU) No 402/2013, Commission Implementing Regulation (Apr. 2013). *On the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009*. European Regulation. The European Commission, Official Journal of the European Union.

Abrial, Jean-Raymond (2020). "The ABZ-2018 case study with Event-B". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 257–264.

Abril, Montserrat, Federico Barber, Laura Ingolotti, Miguel A Salido, Pilar Tormos, and Antonio Lova (2008). "An assessment of railway capacity". In: *Transportation Research Part E: Logistics and Transportation Review* 44.5, pp. 774–806.

Addad, Boussad, Said Amari, and Jean-Jacques Lesage (2011). "Client-server networked automation systems reactivity: Deterministic and probabilistic analysis". In: *IEEE transactions on automation science and engineering* 8.3, pp. 540–548.

Agha, Gul and Karl Palmskog (2018). "A survey of statistical model checking". In: *ACM Transactions on Modeling and Computer Simulation (TOMACS)* 28.1, pp. 1–39.

Akrouche, Joanna, Mohamed Sallak, Eric Châtelet, Fahed Abdallah, and Hiba Hajj Chehade (2022). "Methodology for the Assessment of Imprecise Multi-State System Availability". In: *Mathematics* 10.1, p. 150.

Aktouche, Sadek Rayan, Mohamed Sallak, Abdelmadjid Bouabdallah, and Walter Schön (2021). "Towards Reconciling Safety and Security Risk Analysis Processes in Railway Remote Driving". In: *2021 5th International Conference on System Reliability and Safety (ICSRS)*. IEEE, pp. 148–154.

Almeida Pereira, Dalay Israel de, Ouail Himrane, Philippe Bon, and Julie Beugin (2021). "From French National Signaling Systems to ERTMS: Considering the Evolution of Track-Side Systems". In: *International Journal of Signal Processing Systems* 9.2, pp11–16.

Alur, Rajeev, Tomás Feder, and Thomas A Henzinger (1996). "The benefits of relaxing punctuality". In: *Journal of the ACM (JACM)* 43.1, pp. 116–146.

Ammour, Rabah and Saïd Amari (2015). "Modelling and temporal performances evaluation of networked control systems using (max,+) algebra". In: *International Journal of Systems Science* 46.1, pp. 18–30.

Arcaini, Paolo, Jan Kofroň, and Pavel Ježek (2020). "Validation of the Hybrid ERTMS/ETCS Level 3 using SPIN". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 265–279.

Avram, Camelia, Karolina Bezerra, Dan Radu, Jose Machado, and Adina Astilean (2018). "A Formal Approach for Railroad Traffic Modelling Using Timed Automata". In: *International Conference on Innovation, Engineering and Entrepreneurship*. Springer, pp. 307–314.

Baccelli, François, Guy Cohen, Geert Jan Olsder, and Jean-Pierre Quadrat (1992). "Synchronization and linearity: an algebra for discrete event systems". In.

Baier, Christel, Boudewijn R Haverkort, Holger Hermanns, and Joost-Pieter Katoen (2005). "Model checking meets performance evaluation". In: *ACM SIGMETRICS Performance Evaluation Review* 32.4, pp. 10–15.

Balbo, Gianfranco (2000). "Introduction to stochastic Petri nets". In: *School organized by the European Educational Forum*. Springer, pp. 84–155.

Banik, Mandira and Sudeep Ghosh (2013). "Railway network modelling using petri nets". In: *International Journal of Science, Engineering and Computer Technology* 3.7, p. 249.

Baouya, Abdelhakim, Otmane Ait Mohamed, Djamal Bennouar, and Samir Ouchani (2019). "Safety analysis of train control system based on model-driven design methodology". In: *Computers in Industry* 105, pp. 1–16.

Barger, Pavol, Walter Schön, and Mohamed Bouali (2009). "A study of railway ERTMS safety with colored Petri nets". In: *Reliability, Risk, and Safety, Three Volume Set*. CRC Press, pp. 1337–1344.

Basile, Davide, Maurice H ter Beek, and Vincenzo Ciancia (2018). "Statistical model checking of a moving block railway signalling scenario with Uppaal SMC". In: *International Symposium on Leveraging Applications of Formal Methods*. Springer, pp. 372–391.

Basile, Davide, Maurice H ter Beek, Alessandro Fantechi, Stefania Gnesi, Franco Mazzanti, Andrea Piattino, Daniele Trentini, and Alessio Ferrari (2018). "On the industrial uptake of formal methods in the railway domain". In: *International Conference on Integrated Formal Methods*. Springer, pp. 20–29.

Basile, Davide, Maurice H ter Beek, Alessio Ferrari, and Axel Legay (2022). "Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods". In: *International Journal on Software Tools for Technology Transfer* 24.3, pp. 351–370.

Basile, Davide, Maurice H ter Beek, and Axel Legay (2020). "Strategy synthesis for autonomous driving in a moving block railway system with Uppaal Stratego". In: *International Conference on Formal Techniques for Distributed Objects, Components, and Systems*. Springer, pp. 3–21.

Basile, Davide, Maurice H ter Beek, Alessio Ferrari, and Axel Legay (2019). "Modelling and analysing ERTMS L3 moving block railway signalling with simulink and Uppaal SMC". In: *International Workshop on Formal Methods for Industrial Critical Systems*. Springer, pp. 1–21.

Bause, Falko and Pieter S Kritzinger (2002). *Stochastic petri nets*. Vol. 1. Citeseer.

Beek, Maurice H ter, Arne Borälv, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi, Christer Löfving, and Franco Mazzanti (2019). "Adopting formal methods in an industrial setting: the railways case". In: *International Symposium on Formal Methods*. Springer, pp. 762–772.

Beek, Maurice H ter, Stefania Gnesi, and Alexander Knapp (2018). "Formal methods for transport systems". In: *International Journal on Software Tools for Technology Transfer* 20.3, pp. 237–241.

Behrmann, Gerd, Alexandre David, and Kim G Larsen (2006). "A tutorial on Uppaal 4.0". In: *Department of computer science, Aalborg university*.

Behrmann, Gerd, Ansgar Fehnker, Thomas Hune, Kim Larsen, Paul Pettersson, and Judi Romijn (2001). "Efficient guiding towards cost-optimality in UPPAAL". In: *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, pp. 174–188.

Behrmann, Gerd, Ansgar Fehnker, Thomas Hune, Kim Larsen, Paul Pettersson, Judi Romijn, and Frits Vaandrager (2001). "Minimum-cost reachability for priced time automata". In: *International workshop on hybrid systems: computation and control*. Springer, pp. 147–161.

Behrmann, Gerd, Kim G Larsen, and Jacob I Rasmussen (2004). "Priced timed automata: Algorithms and applications". In: *International symposium on formal methods for components and objects*. Springer, pp. 162–182.

Bell, Stephanie A (2001). *A beginner's guide to uncertainty of measurement*.

Bertrand, Nathalie, Patricia Bouyer, Thomas Brihaye, and Nicolas Markey (2008). "Quantitative model-checking of one-clock timed automata under probabilistic semantics". In: *2008 Fifth International Conference on Quantitative Evaluation of Systems*. IEEE, pp. 55–64.

Beugin, Julie, Aleš Filip, Juliette Marais, and Marion Berbineau (2010). "Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications". In: *European Transport Research Review* 2.2, pp. 93–102.

Beugin, Julie, Cyril Legrand, Juliette Marais, Marion Berbineau, and El-Miloudi El-Koursi (2018). "Safety appraisal of GNSS-based localization systems used in train spacing control". In: *IEEE Access* 6, pp. 9898–9916.

Beugin, Julie and Juliette Marais (2012). "Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization". In: *Transportation Research Part C: Emerging Technologies* 22, pp. 42–57.

Blanch, Juan, Todd Walter, and Per Enge (2008). "Position error bound calculation for GNSS using measurement residuals". In: *IEEE Transactions on Aerospace and Electronic Systems* 44.3, pp. 977–984.

Blanch, Juan, Todd Walter, and Per Enge (2010). "RAIM with optimal integrity and continuity allocations under multiple failures". In: *IEEE Transactions on Aerospace and Electronic Systems* 46.3, pp. 1235–1247.

Bonacchi, Andrea and Alessandro Fantechi (2014). "On the validation of an interlocking system by model-checking". In: *International Workshop on Formal Methods for Industrial Critical Systems*. Springer, pp. 94–108.

Booch, Grady, James Rumbaugh, and Ivar Jacobson (1999). *The Unified Modeling Language User Guide*.

Boufaied, Amine, Rafika Thabet, and Ouajdi Korbaa (2016). "Dynamic delay risk assessing using cost-based FMEA for transportation systems". In: *2016 IEEE international conference on systems, man, and cybernetics (SMC)*. IEEE, pp. 001057–001062.

Boulanger, Jean-Louis (2014). *Formal methods applied to complex systems: implementation of the B method*. John Wiley & Sons.

Broy, Manfred, Bengt Jonsson, J-P Katoen, Martin Leucker, and Alexander Pretschner (2005). "Model-based testing of reactive systems". In: *Volume 3472 of Springer LNCS*. Springer.

Bulychev, Peter, Alexandre David, Kim G Larsen, Axel Legay, Guangyuan Li, and Danny Bøgsted Poulsen (2012). "Rewrite-based statistical model checking of wmtl". In: *International Conference on Runtime Verification*. Springer, pp. 260–275.

Burch, Jerry R, Edmund M Clarke, Kenneth L McMillan, David L Dill, and Lain-Jinn Hwang (1992). "Symbolic model checking: 1020 states and beyond". In: *Information and computation* 98.2, pp. 142–170.

Butler, Michael, Philipp Körner, Sebastian Krings, Thierry Lecomte, Michael Leuschel, Luis-Fernando Mejia, and Laurent Voisin (2020). "The first twenty-five years of industrial use of the B-method". In: *International Conference on Formal Methods for Industrial Critical Systems*. Springer, pp. 189–209.

Caillaud, Benoît, Philippe Darondeau, Luciano Lavagno, and Xiaolan Xie (2002). *Synthesis and control of discrete event systems*. Springer Science & Business Media.

Cappart, Quentin, Christophe Limbrée, Pierre Schaus, Jean Quilbeuf, Louis-Marie Traonouez, and Axel Legay (2017). "Verification of interlocking systems using statistical model checking". In: *2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*. IEEE, pp. 61–68.

Cavada, Roberto, Alessandro Cimatti, Charles Arthur Jochim, Gavin Keighren, Emanuele Olivetti, Marco Pistore, Marco Roveri, and Andrei Tchaltsev (2010). "NuSMV 2.6 User Manual". In.

Cavone, Graziana, Mariagrazia Dotoli, and Carla Seatzu (2017). "A survey on Petri net models for freight logistics and transportation systems". In: *IEEE Transactions on Intelligent Transportation Systems* 19.6, pp. 1795–1813.

Chernoff, Herman (1952). "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations". In: *The Annals of Mathematical Statistics*, pp. 493–507.

Ciaffi, Massimiliano, Juliette Marais, Giusy Emmanuele, Omar Garcia Crespillo, Andrea Coluccia, Alessia Vennarini, Salvatore Sabina, Syed Ali Kazim, Daniel Gerbeth, Maria Caamano, et al. (2019). "Classification of Railway tracks for applying enhanced ERTMS/ETCS Solutions Based on GNSS positioning technologies". In: *WCRR 2019, 12th World Congress on Railway Research*, 6p.

Clarke, Edmund, Orna Grumberg, Somesh Jha, Yuan Lu, and Helmut Veith (2001). "Progress on the state explosion problem in model checking". In: *Informatics*. Springer, pp. 176–194.

Clarke, Edmund M and E Allen Emerson (1981). "Design and synthesis of synchronization skeletons using branching time temporal logic". In: *Workshop on Logic of Programs*. Springer, pp. 52–71.

Clarke, Edmund M and Jeannette M Wing (1996). "Formal methods: State of the art and future directions". In: *ACM Computing Surveys (CSUR)* 28.4, pp. 626–643.

Commission, European (2016). *History of ERTMS*. URL: https://ec.europa.eu/transport/modes/rail/ertms/general-information/history_ertms_it (visited on 09/07/2021).

Comptier, Mathieu, David Déharbe, Julien Molinero Perez, Louis Mussat, Thibaut Pierre, and Denis Sabatier (2017). "Safety analysis of a CBTC system: a rigorous approach with Event-B". In: *International Conference on Reliability, Safety and Security of Railway Systems*. Springer, pp. 148–159.

Conference of the Parties, COP (2022). *United Nations Framework Convention on Climate Change (UNFCCC)*. URL: https://unfccc.int/process/bodies/supreme-bodies/conference-of-the-parties-cop (visited on 05/17/2022).

Cost, R Scott, Ye Chen, Tim Finin, Yannis K Labrou, Yun Peng, et al. (1999). "Modeling agent conversations with colored petri nets". In: *Working notes of the Autonomous Agents' 99 Workshop on Specifying and Implementing Conversation Policies*.

Cowie, Jonathan (2009). *The economics of transport: a theoretical and applied perspective*. Routledge.

Craigen, Dan, Susan Gerhart, and Ted Ralston (1993). "An international survey of industrial applications of formal methods". In: *Z User Workshop, London 1992*. Springer, pp. 1–5.

Cunha, Alcino and Nuno Macedo (2020). "Validating the hybrid ERTMS/ETCS level 3 concept with Electrum". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 281–296.

Damy, Sophie (2016). *A novel GNSS-based positioning system to support railway operations*. Imperial College London.

David, Alexandre, Kim G Larsen, Axel Legay, Marius Mikučionis, and Danny Bøgsted Poulsen (2015). "Uppaal SMC tutorial". In: *International Journal on Software Tools for Technology Transfer* 17.4, pp. 397–415.

Dghaym, Dana, Mohammadsadegh Dalvandi, Michael Poppleton, and Colin Snook (2020). "Formalising the Hybrid ERTMS Level 3 specification in iUML-B and Event-B". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 297–313.

DIRECTIVE (EU) 2016/797 (May 11, 2016). *on the interoperability of the rail system within the European Union (recast)*. THE EUROPEAN PARLIAMENT and THE COUNCIL.

Drevelle, Vincent and Philippe Bonnifait (2009). "High integrity GNSS location zone characterization using interval analysis". In: *Proceedings of the 22nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2009)*, pp. 2178–2187.

Duflot, Marie, Laurent Fribourg, Thomas Herault, Richard Lassaigne, Frédéric Magniette, Stéphane Messika, Sylvain Peyronnet, and Claudine Picaronny (2005). "Probabilistic model checking of the CSMA/CD protocol using PRISM and APMC". In: *Electronic Notes in Theoretical Computer Science* 128.6, pp. 195–214.

Durazo-Cardenas, I, A Starr, Antonios Tsourdos, Maurizio Bevilacqua, and Julien Morineau (2014). "Precise vehicle location as a fundamental parameter for intelligent self-aware railtrack maintenance systems". In: *Procedia CIRP* 22, pp. 219–224.

Ehrig, Hartmut, Arend Rensink, Grzegorz Rozenberg, and Andy Schürr (2010). *Graph Transformations: 5th International Conference, ICGT 2010, Twente, The Netherlands, September 27–October 2, 2010, Proceedings*. Vol. 6372. Springer.

EN 50126 : (Oct. 2017). *Railway Applications - The Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*. Std. European Committee for Electrotechnical Standardisation (CENELEC).

EN 50128 : (Oct. 2011). *Railway Applications - Communication, signalling and processing systems - Software for railway control and protection systems*. Std. European Committee for Electrotechnical Standardisation (CENELEC).

EN 50129: (Nov. 2018). *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. Std. European Committee for Electrotechnical Standardisation (CENELEC).

EN 61882: (Oct. 2016). *Hazard and operability studies (HAZOP studies) - Application guide*. Std. European Committee for Electrotechnical Standardisation (CENELEC).

ERA, European Railway Agency (Jan. 2009). *Guide for the application of the CSM Regulation*. Guide. The European Commission.

Eschbach, Robert (2021). "Formalizing and Analyzing System Requirements of Automatic Train Operation over ETCS Using Event-B". In: *International Conference on Rigorous State-Based Methods*. Springer, pp. 137–142.

EU Agency for Railways (2021). *Common Safety Methods*. URL: https://www.era.europa.eu/activities/common-safety-methods_en (visited on 09/15/2021).

European Environment Agency, EEA (Feb. 25, 2021). *Transport and Environment Report 2020 (TERM)*.

— (2022). *Motorised transport: train, plane, road or boat — which is greenest?* URL: https://www.eea.europa.eu/highlights/motorised-transport-train-plane-road (visited on 05/17/2022).

Fantechi, Alessandro (2013). "Twenty-five years of formal methods and railways: what next?" In: *International Conference on Software Engineering and Formal Methods*. Springer, pp. 167–183.

Fantechi, Alessandro, Alessio Ferrari, and Stefania Gnesi (2016). "Formal methods and safety certification: challenges in the railways domain". In: *International Symposium on Leveraging Applications of Formal Methods*. Springer, pp. 261–265.

Federal Radionavigation Plan. (2010). *DOT-VNTSC-RITA-08-02/DoD-4650.05*. Std. United States Department of Defense, United States Department of Homeland Security, and Department of Transportation.

Ferrari, Alessio and Maurice H ter Beek (2021). "Formal Methods in Railways: a Systematic Mapping Study". In: *arXiv preprint arXiv:2107.05413*.

Ferrari, Alessio, Maurice H ter Beek, Franco Mazzanti, Davide Basile, Alessandro Fantechi, Stefania Gnesi, Andrea Piattino, and Daniele Trentini (2019). "Survey on formal methods and tools in railways: the ASTRail approach". In: *International Conference on Reliability, Safety, and Security of Railway Systems*. Springer, pp. 226–241.

Ferrari, Alessio, Alessandro Fantechi, Stefania Gnesi, and Gianluca Magnani (2013). "Model-based development and formal methods in the railway industry". In: *IEEE software* 30.3, pp. 28–34.

Ferrari, Alessio, Franco Mazzanti, Davide Basile, Maurice H ter Beek, and Alessandro Fantechi (2020). "Comparing formal tools for system design: a judgment study". In: *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)*. IEEE, pp. 62–74.

Filip, Aleš, Julie Beugin, Juliette Marais, and Hynec Mocek (2008). "Interpretation of the Galileo safety-of-life service by means of railway RAMS terminology". In: *Transactions on Transport Sciences* 1.2, pp. 61–68.

Filip, Aleš, Francesco Rispoli, and Roberto Capua (2020). "A safety regulatory framework for certification and authorization process of self-driving cars: experience from European railways". In: *Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*. Research Publishing Services.

Filip, Aleš, Salvatore Sabina, and Francesco Rispoli (2018). "A framework for certification of train location determination system based on GNSS for ERTMS/ETCS". In: *International Journal of Transport Development and Integration* 2.3, pp. 284–297.

Furness, Nicola, Henri Van Houten, Laura Arenas, and Maarten Bartholomeus (Apr. 2017). "ERTMS Level 3: the Game-Changer". In: *IRSE - Institute of Railway Signal Engineers*, p. 8.

Ghazel, Mohamed (2009). "Using stochastic Petri nets for level-crossing collision risk assessment". In: *IEEE transactions on intelligent transportation systems* 10.4, pp. 668–677.

— (2017). "A control scheme for automatic level crossings under the ERTMS/ETCS level 2/3 operation". In: *IEEE Transactions on Intelligent Transportation Systems* 18.10, pp. 2667–2680.

Ghazel, Mohamed and El-Miloudi El-Koursi (2014). "Two-half-barrier level crossings versus four-half-barrier level crossings: A comparative risk analysis study". In: *IEEE Transactions on Intelligent Transportation Systems* 15.3, pp. 1123–1133.

Gleirscher, Mario, Simon Foster, and Jim Woodcock (2019). "New opportunities for integrated formal methods". In: *ACM Computing Surveys (CSUR)* 52.6, pp. 1–36.

Gnesi, Stefania and Tiziana Margaria (2012). *Formal methods for industrial critical systems: A survey of applications*. John Wiley & Sons.

Goya, Jon, Gorka De Miguel, Saioa Arrizabalaga, Leticia Zamora-Cadenas, Iñigo Adin, and Jaizki Mendizabal (2018). "Methodology and key performance indicators (KPIs) for railway on-board positioning systems". In: *IEEE Transactions on Intelligent Transportation Systems* 19.12, pp. 4035–4042.

Guck, Dennis (2017). "Reliable systems: fault tree analysis via Markov reward automata". In.

Hall, Anthony (2007). "Realising the Benefits of Formal Methods." In: *J. Univers. Comput. Sci.* 13.5, pp. 669–678.

Hamid, HA, GL Nicholson, and C Roberts (2018). "Investigation into the Positioning Accuracy Required for Traffic". In: *IET Conference Proceedings*. The Institution of Engineering & Technology.

Hamid, Hassan Abdulsalam (2020). "Using information engineering to understand the impact of train positioning uncertainties on railway subsystems". PhD thesis. University of Birmingham.

Hansen, Dominik, Michael Leuschel, Körner Philipp, Sebastian Krings, Thomas Naulin, Nayeri Nader, David Schneider, and Frank Skowron (2020). "Validation and real-life demonstration of ETCS hybrid level 3 principles using a formal B model". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 315–332.

Hartonas-Garmhausen, Vicky, Sergio Campos, Alessandro Cimatti, Edmund Clarke, and Fausto Giunchiglia (2000). "Verification of a safety-critical railway interlocking system with real-time constraints". In: *Science of Computer Programming* 36.1, pp. 53–64.

Haxthausen, Anne E and Kristian Hede (2019). "Formal verification of railway timetables-using the UPPAAL model checker". In: *From Software Engineering to Formal Methods and Tools, and Back*. Springer, pp. 433–448.

Henzinger, Thomas A and Pei-Hsin Ho (1995). "Algorithmic analysis of nonlinear hybrid systems". In: *International Conference on Computer Aided Verification*. Springer, pp. 225–238.

Hérault, Thomas, Richard Lassaigne, Frédéric Magniette, and Sylvain Peyronnet (2004). "Approximate probabilistic model checking". In: *International Workshop on Verification, Model Checking, and Abstract Interpretation*. Springer, pp. 73–84.

Himrane, Ouail, Julie Beugin, and Mohamed Ghazel (2020a). "Proposition d'une approche orientée modèles pour évaluer la sécurité des systèmes de signalisation ferroviaire utilisant les GNSS". In: *Lambda Mu 22, 22e Congrès de maîtrise des risques et de sûreté de fonctionnement. Les risques au coeur des transitions (e-congrès)*, pp687–696.

— (2020b). "Towards a Model-Based Safety Assessment of Railway Operation Using GNSS Localization". In: *ESREL 2020 PSAM 15, 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, 8p.

— (2021). "Toward Formal Safety and Performance Evaluation of GNSS-based Railway Localisation Function". In: *IFAC-PapersOnLine* 54.2, pp. 159–166.

Himrane, Ouail, Alain Ourghanlian, and Saïd Amari (2022). "Response time evaluation of industrial-scale distributed control systems by discrete event systems formalisms". In: *International Journal of Control* 95.2, pp. 419–431.

Hirel, Christophe, Bruno Tuffin, and Kishor S Trivedi (2000). "Spnp: Stochastic petri nets. version 6.0". In: *International Conference on Modelling Techniques and Tools for Computer Performance Evaluation*. Springer, pp. 354–357.

Hirwa, Serge (2013). "Line of sight stabilization using advanced control techniques." PhD thesis. Supélec.

Hoeffding, Wassily (1994). "Probability inequalities for sums of bounded random variables". In: *The collected works of Wassily Hoeffding*. Springer, pp. 409–426.

Hofmann-Wellenhof, Bernhard, Klaus Legat, and Manfred Wieser (2003). *Navigation: Principles of Positioning and Guidance*. Springer Science & Business Media.

Hörste, M zu, Hardi Hungar, and Eckehard Schnieder (2013). "Modelling functionality of train control systems using petri nets". In: *Towards a Formal Methods Body of Knowledge for Railway Control and Safety Systems*, p. 46.

Huang, Yi-Sheng, Yi-Shun Weng, and MengChu Zhou (2010). "Critical scenarios and their identification in parallel railroad level crossing traffic control systems". In: *IEEE transactions on intelligent transportation systems* 11.4, pp. 968–977.

ICAO, International Civil Aviation Organization (July 2018). *International Standards and Recommended Practices. Annex 10 to the Convention on International Civil Aviation: Aeronautical Telecommunications*. Vol. 1 Radio Navigation Aids, Seventh Edition.

IEC 60050-192: (Feb. 2015). *International electrotechnical vocabulary - Part 192 : dependability*. Std. International Electrotechnical Commission (IEC).

IEC 60812: (Oct. 2018). *Failure Modes and Effects analysis (FMEA and FMECA)*. Std. International Electrotechnical Commission (IEC).

IEC 61025: (Dec. 2006). *Fault tree analysis (FTA)*. Std. International Electrotechnical Commission (IEC).

IEC 61508 : (2011). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Std. IEC-International Electrotechnical Commission.

IEC 61508-1: (Apr. 2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1 : general requirements*. Std. International Electrotechnical Commission (IEC).

IEC 61508-4: (Apr. 2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4 : definitions and abbreviations*. Std. International Electrotechnical Commission (IEC).

IEC 62502: (Oct. 2010). *Analysis techniques for dependability - Event tree analysis (ETA)*. Std. International Electrotechnical Commission (IEC).

Intergovernmental Panel on Climate Change, IPCC (2022). *The IPCC Assessment Reports about knowledge on climate change, its causes, potential impacts and response options*. URL: https://www.ipcc.ch/reports/ (visited on 05/17/2022).

International union of railways, UIC (Nov. 12, 2015). *Rail transport and environment: facts and figures*.

James, Phillip, Faron Moller, Hoang Nga Nguyen, Markus Roggenbach, Steve Schneider, and Helen Treharne (2014). "Techniques for modelling and verifying railway interlockings". In: *International Journal on Software Tools for Technology Transfer* 16.6, pp. 685–711.

Jeffrey, Charles (2010). *An introduction to GNSS: GPS, GLONASS, Galileo and other global navigation satellite systems*. NovAtel.

Jensen, Kurt (1997). "A brief introduction to coloured petri nets". In: *International Workshop on Tools and Algorithms for the Construction and Analysis of Systems*. Springer, pp. 203–208.

— (2013). *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical Use. Volume 1*. Springer Science & Business Media.

Jensen, Kurt and Lars M Kristensen (2015). "Colored Petri nets: a graphical language for formal modeling and validation of concurrent systems". In: *Communications of the ACM* 58.6, pp. 61–70.

Jiang, Ziyi (2011). "Digital route model aided integrated satellite navigation and low-cost inertial sensors for high-performance positioning on the railways". PhD thesis. UCL (University College London).

Kalajdzic, Kenan, Cyrille Jégourel, Anna Lukina, Ezio Bartocci, Axel Legay, Scott A Smolka, and Radu Grosu (2016). "Feedback control for statistical model checking of cyber-physical systems". In: *International Symposium on Leveraging Applications of Formal Methods*. Springer, pp. 46–61.

Kamdem Simo, F, Dominique Ernadote, Dominique Lenne, and Mohamed Sallak (2021). "Principles for coping with the modelling activity of engineered systems". In: *Research in Engineering Design* 32.1, pp. 3–30.

Kaplan, Elliott D and Christopher Hegarty (2017). *Understanding GPS/GNSS: Principles and applications*. Artech house.

Kazim, Syed Ali, Nourdine Aït Tmazirte, and Juliette Marais (2020). "Realistic position error models for GNSS simulation in railway environments". In: *2020 European Navigation Conference (ENC)*. IEEE, pp. 1–9.

Konnov, Igor (2019). *Edmund M. Clarke, Thomas A. Henzinger, Helmut Veith, and Roderick Bloem (eds): Handbook of model checking*.

Koymans, Ron (1990). "Specifying real-time properties with metric temporal logic". In: *Real-time systems* 2.4, pp. 255–299.

Kozol, BA and DF Thurston (2010). "Axle counters Vs track circuits-safety in track vacancy detection and broken rail detection". In: *Proceedings of the American Railway and Maintenance-of-Way Association AREMA 2010 annual conference & exposition. Orlando, FLAug*.

Kumar, Rajesh (2018). "Truth or dare: quantitative security risk analysis via attack trees". PhD thesis. University of Twente.

Kwiatkowska, Marta, Gethin Norman, and David Parker (2011). "PRISM 4.0: Verification of probabilistic real-time systems". In: *International conference on computer aided verification*. Springer, pp. 585–591.

Lajimi, Chokri, Amine Boufaied, Elyes Lamine, and Ouajdi Korbaa (2016). "Dynamic delay risk assessing in supply chains". In: *IET Intelligent Transport Systems* 10.10, pp. 666–673.

Landex, Alex (2008). *Methods to estimate railway capacity and passenger delays*. Technical University of Denmark.

Larsen, Kim, Gerd Behrmann, Ed Brinksma, Ansgar Fehnker, Thomas Hune, Paul Pettersson, and Judi Romijn (2001). "As cheap as possible: effcient cost-optimal reachability for priced timed automata". In: *International Conference on Computer Aided Verification*. Springer, pp. 493–505.

Laursen, Per Lange, Van Anh Thi Trinh, and Anne E Haxthausen (2020). "Formal modelling and verification of a distributed railway interlocking system using uppaal". In: *International Symposium on Leveraging Applications of Formal Methods*. Springer, pp. 415–433.

Legrand, Cyril (2016). "Contribution to the safety evaluation of railway localisation systems based on GNSS by formalising extended integrity concepts". PhD thesis. Université de Lille 1.

Li, Kaicheng, Xiaofei Yao, Dewang Chen, Lei Yuan, and Datian Zhou (Feb. 2015). "HAZOP Study on the CTCS-3 Onboard System". In: *IEEE Transactions on Intelligent Transportation Systems* 16.1, pp. 162–171. ISSN: 1558-0016. DOI: 10.1109/TITS.2014.2329692.

Limbrée, Christophe and Charles Pecheur (2019). "A Framework for the Formal Verification of Networks of Railway Interlockings-Application to the Belgian Railway". In: *Electronic Communications of the EASST* 76.

Liu, Dongsheng, Jianmin Wang, Stephen CF Chan, Jiaguang Sun, and Li Zhang (2002). "Modeling workflow processes with colored Petri nets". In: *computers in industry* 49.3, pp. 267–281.

LML Specification (2022). *Lifecycle Modeling Language Specification (Version 1.3)*.

Lu, Debiao (2014). "Gnss for train localisation performance evaluation and verification". PhD thesis. Technische Universität Carolo-Wilhelmina zu Braunschweig.

Lu, Debiao and Eckehard Schnieder (2014). "Performance evaluation of GNSS for train localization". In: *IEEE transactions on intelligent transportation systems* 16.2, pp. 1054–1059.

Lu, Debiao, Dezhang Tang, and Dirk Spiegel (2020). "Hazard Rate Estimation for GNSS-Based Train Localization Using Model-Based Approach". In: *Chinese Journal of Electronics* 29.1, pp. 49–56.

Mammar, Amel, Marc Frappier, Steve Jeffrey Tueno Fotso, and Régine Laleau (2018). "An Event-B model of the hybrid ERTMS/ETCS level 3 standard". In: *International Conference on Abstract State Machines, Alloy, B, TLA, VDM, and Z*. Springer, pp. 353–366.

— (2020). "A formal refinement-based analysis of the hybrid ERTMS/ETCS level 3 standard". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 333–347.

Marais, Juliette, Julie Beugin, and Marion Berbineau (2017). "A survey of GNSS-based research and developments for the European railway signaling". In: *IEEE Transactions on Intelligent Transportation Systems* 18.10, pp. 2602–2618.

Marsan, M Ajmone, Gianfranco Balbo, Gianni Conte, Susanna Donatelli, and Giuliana Franceschinis (1998). "Modelling with generalized stochastic Petri nets". In: *ACM SIGMETRICS performance evaluation review* 26.2, p. 2.

Martinez, Felipe Aguirre, Mohamed Sallak, and Walter Schön (2015). "An efficient method for reliability analysis of systems under epistemic uncertainty using belief function theory". In: *IEEE Transactions on Reliability* 64.3, pp. 893–909.

Mazzanti, Franco and Alessio Ferrari (2018). "Ten diverse formal models for a CBTC automatic train supervision system". In: *arXiv preprint arXiv:1803.10324*.

Mazzanti, Franco, Alessio Ferrari, and Giorgio O Spagnolo (2018). "Towards formal methods diversity in railways: an experience report with seven frameworks". In: *International Journal on Software Tools for Technology Transfer* 20.3, pp. 263–288.

Mekki, Ahmed, Mohamed Ghazel, and Armand Toguyeni (2012). "Validation of a new functional design of automatic protection systems at level crossings with model-checking techniques". In: *IEEE Transactions on Intelligent Transportation Systems* 13.2, pp. 714–723.

Merriam-Webster (2022). *"Navigation." Merriam-Webster.com Dictionary*. URL: https://www.merriam-webster.com/dictionary/navigation (visited on 07/12/2022).

Molloy, Michael K. (1982). "Performance analysis using stochastic Petri nets". In: *IEEE Transactions on computers* 31.09, pp. 913–917.

El-Mowafy, Ahmed and Nobuaki Kubo (2017). "Integrity monitoring of vehicle positioning in urban environment using RTK-GNSS, IMU and speedometer". In: *Measurement Science and Technology* 28.5, p. 055102.

Nawaz, M Saqib, Moin Malik, Yi Li, Meng Sun, and M Lali (2019). "A survey on theorem provers in formal methods". In: *arXiv preprint arXiv:1912.03028*.

Nguyen, TP Khanh, Julie Beugin, and Juliette Marais (2015). "Method for evaluating an extended Fault Tree to analyse the dependability of complex systems: Application to a satellite-based railway system". In: *Reliability Engineering & System Safety* 133, pp. 300–313.

Pachl, Jörn (2020). "Railway Signalling Principles". In: *Braunschweig, Jun*.

Peng, Zhaoguang, Yu Lu, Alice Miller, Tingdi Zhao, and Chris Johnson (2016). "Formal specification and quantitative analysis of a constellation of navigation satellites". In: *Quality and Reliability Engineering International* 32.2, pp. 345–361.

Peterson, James L et al. (1980). "A note on colored Petri nets". In: *Inf. Process. Lett.* 11.1, pp. 40–43.

Petri, Carl Adam (1962). "Kommunikation mit Automaten (Communication through automatons)". PhD thesis. The Rhenish Friedrich Wilhelm University of Bonn.

Pouryousef, Hamed, Pasi Lautala, and Thomas White (2015). "Railroad capacity tools and methodologies in the US and Europe". In: *Journal of Modern Transportation* 23.1, pp. 30–42.

PR NF ISO 5725-1: (June 2022). *Accuracy (trueness and precision) of measurement methods and results - Part 1 : general principles and definitions*. Std.

Presti, Letizia Lo and Salvatore Sabina (2018). "GNSS for Rail Transportation". In: *Switzerland: Springer*.

Qiu, Siqi, Mohamed Sallak, Walter Schön, and Zohra Cherfi-Boulanger (2014a). "Availability assessment of railway signalling systems with uncertainty analysis using Statecharts". In: *Simulation Modelling Practice and Theory* 47, pp. 1–18.

— (2014b). "Modeling of ERTMS level 2 as an SoS and evaluation of its dependability parameters using statecharts". In: *IEEE Systems Journal* 8.4, pp. 1169–1181.

Queille, Jean-Pierre and Joseph Sifakis (1982). "Specification and verification of concurrent systems in CESAR". In: *International Symposium on programming*. Springer, pp. 337–351.

Ramchandani, Chander (1973). "Analysis of asynchronous concurrent systems by timed petri nets." PhD thesis. Massachusetts Institute of technology.

Rangra, S, M Sallak, W Schön, and F Belmonte (2018). "Risk and safety analysis of main line autonomous train operation: Context, challenges and solutions". In: *Conference: Congrès Lambda Mu 21 de Maîtrise des Risques et de Sûreté de Fonctionnement*.

Ranjbar, Vahid and Nils OE Olsson (2020). "Towards Mobile and Intelligent Railway Transport: A Review of Recent ERTMS Related Research". In: *Computers in Railways XVII: Railway Engineering Design and Operation* 199, p. 65.

Regulation TSI CCS (EU) 2016/919 (May 27, 2016). *Technical Specification for Interoperability relating to the 'Control-Command and Signalling' subsystems of the rail system in the European Union*. European Commission regulation.

Rehman, Aniqa, Saba Latif, and Nazir Ahmad Zafar (2019). "Automata based railway gate control system at level crossing". In: *2019 International Conference on Communication Technologies (ComTech)*. IEEE, pp. 30–35.

Robinson, Alan JA and Andrei Voronkov (2001). *Handbook of automated reasoning*. Vol. 1. Elsevier.

Sallak, Mohamed (2007). "Évaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception: application aux Systèmes Instrumentés de Sécurité". PhD thesis. Institut National Polytechnique de Lorraine.

Sallak, Mohamed, Walter Schön, and Felipe Aguirre (2013). "Reliability assessment for multi-state systems under uncertainties based on the Dempster–Shafer theory". In: *IIE Transactions* 45.9, pp. 995–1007.

Shif2Rail (2022). *Shif2Rail IP2 projects (Innovation Programme):* URL: https://shift2rail.org/research-development/ip2 (visited on 05/17/2022).

Shift2Rail X2Rail1 (Sept. 1, 2016). *Deliverable D5.2: Moving Block Operational and Engineering Rules*.

Shift2Rail X2Rail2 (May 16, 2018). *Deliverable D5.1: Formal Methods (taxonomy and survey), Proposed methods and Applications*.

Stok, Roberto (2008). *Estimation of railway capacity consumption using stochastic differential equations.* Universita degli studi di Trieste.

Subset 026: (June 13, 2016). *System Requirements Specification v3.6.0*. ERA UNISIG ERTMS Users Group.

Subset 035: (Dec. 16, 2015). *Subset-35 Specific Transmission Module FFFIS*. ERA UNISIG EEIG ERTMS Users Group, p. 99.

Subset 041: (Dec. 17, 2015). *Subset-41 Performance Requirements for Interoperability*. ERA UNISIG EEIG ERTMS Users Group, p. 16.

Subset- 023: (May 12, 2014). *Subset-023 Glossary of Terms and Abbreviation*. ERA UNISIG EEIG ERTMS Users Group, p. 27.

Sun, Rui, Junhui Wang, Qi Cheng, Yi Mao, and Washington Yotto Ochieng (2021). "A new IMU-aided multiple GNSS fault detection and exclusion algorithm for integrated navigation in urban environments". In: *GPS Solutions* 25.4, pp. 1–17.

SysML Specification, OMG (2019). *OMG Systems Modeling Language (OMG SysML™), V1.6, SysML Open Source Specification Project*.

Tamssaouet, Ferhat and Saïd Amari (2018). "Modelling and temporal evaluation of networked control systems using timed automata with guards and (max,+) algebra". In: *International Journal of Systems Science* 49.10, pp. 2073–2088.

Tang, Shengjie, Haifeng Wang, Bin Ning, Geer Han, and Ming Chai (2018). "Positive Safety Modeling of CTCS-3 Train Control System for High-speed railway". In: *2018 International Conference on Intelligent Rail Transportation (ICIRT)*. IEEE, pp. 1–5.

Thabet, Rafika, Dominik Bork, Amine Boufaied, Elyes Lamine, Ouajdi Korbaa, and Hervé Pingaud (2021). "Risk-aware business process management using multi-view modeling: method and tool". In: *Requirements Engineering* 26.3, pp. 371–397.

Thabet, Rafika, Elyes Lamine, Amine Boufaied, Dominik Bork, Ouajdi Korbaa, and Herve Pingaud (2020). "Formal specification, implementation, and evaluation of the AdoBPRIM approach". In.

Tijero, E Domínguez, E Carbonell Pons, JD Calle, L Martínez Fernández, PF Madrid, C Moriana Varo, and M Azaola Sáenz (2017). "Advanced GNSS Algorithms for Safe Autonomous Vehicles". In: *Proceedings of the 30th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2017)*, pp. 655–664.

Tmazirte, Nourdine Ait, Syed Ali Kazim, and Juliette Marais (2020). "Towards a new GNSS observation weighting strategy for terrestrial applications". In: *2020 European Navigation Conference (ENC)*. IEEE, pp. 1–10.

Tmazirte, Nourdine Aït, Maan E El Najjar, Joelle Al Hage, Cherif Smaili, and Denis Pomorski (2014). "Fast multi fault detection & exclusion approach for GNSS integrity monitoring". In: *17th International Conference on Information Fusion (FUSION)*. IEEE, pp. 1–6.

Tossaint, M, Jaron Samson, Felix Toran, Javier Ventura-Traveset, J Sanz, Manuel Hernandez-Pajares, and JM Juan (2006). "The stanford-ESA integrity diagram: focusing on SBAS integrity". In: *Proceedings of the 19th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2006)*, pp. 894–905.

Trouillet, Benot, Ouajdi Korbaa, and Jean-Claude Gentina (2006). "Formal approach of FMS cyclic scheduling". In: *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 37.1, pp. 126–137.

Tueno Fotso, Steve Jeffrey, Marc Frappier, Régine Laleau, and Amel Mammar (2020). "Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach". In: *International Journal on Software Tools for Technology Transfer* 22.3, pp. 349–363.

Van Diggelen, Frank Stephen Tromp (2009). *A-gps: Assisted gps, gnss, and sbas*. Artech house.

Vanicek, P and EJ Krakiwsky (2015). *Geodesy: the concepts*. Elsevier Science BV 1986 Elsevier.

Vanit-Anunchai, Somsak (2018). "Modelling and simulating a Thai railway signalling system using Coloured Petri Nets". In: *International Journal on Software Tools for Technology Transfer* 20.3, pp. 243–262.

Vu, Linh H, Anne E Haxthausen, and Jan Peleska (2017). "A domain-specific language for generic interlocking models and their properties". In: *International Conference on Reliability, Safety and Security of Railway Systems*. Springer, pp. 99–115.

Vu, Linh Hong, Anne E Haxthausen, and Jan Peleska (2017). "Formal modelling and verification of interlocking systems featuring sequential release". In: *Science of Computer Programming* 133, pp. 91–115.

Wang, Jiacun (2012). *Timed Petri nets: Theory and application*. Vol. 9. Springer Science & Business Media.

Wang, Jinling and Pieter B Ober (2009). "On the availability of fault detection and exclusion in GNSS receiver autonomous integrity monitoring". In: *the Journal of Navigation* 62.2, pp. 251–261.

Wang, Shizhuang, Xingqun Zhan, Yawei Zhai, and Baoyu Liu (2020). "Fault detection and exclusion for tightly coupled GNSS/INS system considering fault in state prediction". In: *Sensors* 20.3, p. 590.

Wang, Tuo, Jidong Lv, Baiquan Wei, Tao Tang, and Wei Shangguan (2018). "Test Suite Generation for CTCS-3 Train Control System Based On TAIO and Mutation Theory". In: *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pp. 1950–1955. DOI: 10.1109/ITSC.2018.8569768.

Wells, DE, N Beck, D Delikaraoglou, A Kleusberg, EJ Krakiwsky, G Lachapelle, RB Langley, M Nakiboglu, KP Schwarz, JM Tranquilla, et al. (1986). *Guide to GPS Positioning. Canadian GPS Associates, Fredericton*.

Weyns, Danny, M Usman Iftikhar, Didac Gil De La Iglesia, and Tanvir Ahmad (2012). "A survey of formal methods in self-adaptive systems". In: *Proceedings of the fifth international c* conference on computer science and software engineering*, pp. 67–79.

Winter, Kirsten (2002). "Model checking railway interlocking systems". In: *Australian Computer Science Communications* 24.1, pp. 303–310.

Woodcock, Jim, Peter Gorm Larsen, Juan Bicarregui, and John Fitzgerald (2009). "Formal methods: Practice and experience". In: *ACM computing surveys (CSUR)* 41.4, pp. 1–36.

Wu, Daohua and Eckehard Schnieder (2016). "Scenario-based modeling of the on-board of a satellite-based train control system with colored petri nets". In: *IEEE Transactions on Intelligent Transportation Systems* 17.11, pp. 3045–3061.

Wullems, Christian, Francesco Sperandio, Marzia Basso, Silvia Sturaro, and Salvatore Sabina (2018). "A preliminary apportionment of safety targets for virtual Balise detection using GNSS in future evolutions of ERTMS". In: *2018 16th International Conference on Intelligent Transportation Systems Telecommunications (ITST)*. IEEE, pp. 1–8.

Yang, Ling, Yong Li, Youlong Wu, and Chris Rizos (2014). "An enhanced MEMS-INS/GNSS integrated system with fault detection and exclusion capability for land vehicle navigation in urban areas". In: *Gps Solutions* 18.4, pp. 593–603.

Yin, Jiateng, Tao Tang, Lixing Yang, Jing Xun, Yeran Huang, and Ziyou Gao (2017). "Research and development of automatic train operation for railway transportation systems: A survey". In: *Transportation Research Part C: Emerging Technologies* 85, pp. 548–572.

Younes, Hakan Lorens Samir (2004). *Verification and planning for stochastic processes with asynchronous events*. Carnegie Mellon University.

Zabalegui, Paul, Gorka De Miguel, Alejandro Pérez, Jaizki Mendizabal, Jon Goya, and Iñigo Adin (2020). "A review of the evolution of the integrity methods applied in GNSS". In: *IEEE Access* 8, pp. 45813–45824.

Zafar, Nazir Ahmad, Sher Afzal Khan, and Keijiro Araki (2012). "Towards the safety properties of moving block railway interlocking system". In: *Int. J. Innovative Comput., Info & Control* 8.7, pp. 5677–5690.

Zhang, Yong, Haifeng Wang, Tommy Yuan, Jidong Lv, and Tianhua Xu (2019). "Hybrid online safety observer for CTCS-3 train control system on-board equipment". In: *IEEE Transactions on Intelligent Transportation Systems* 20.3, pp. 925–934. ISSN: 1524-9050. DOI: 10.1109/TITS.2018.2836459.

Zhou, Yonghua and Chao Mi (2012). "Modeling train movement for moving-block railway network using cellular automata". In: *Computer Modeling in Engineering & Sciences(CMES)* 83.1, pp. 1–21.

Zhu, Ni, David Betaille, Juliette Marais, and Marion Berbineau (2018). "GNSS integrity enhancement for urban transport applications by error characterization and fault detection and exclusion (FDE)". In: *Géolocalisation et Navigation dans l'Espace et le Temps, Journées Scientifiques 2018 de l'URSI*, 11p.

Zimmermann, Armin and Günter Hommel (2003). "A train control system case study in model-based real time system design". In: *Proceedings International Parallel and Distributed Processing Symposium*. IEEE, 8–pp.

— (2005). "Towards modeling and evaluation of ETCS real-time communication and operation". In: *Journal of Systems and Software* 77.1, pp. 47–54.

Annex A: ERTMS/ETCS Level 1 and 2

The present appendix is complementary to chapter 2 of this manuscript. In particular, a graphical representation of ERTMS/ETCS levels 1 and 2, as introduced in Subset 026 , is shown hereafter:

ERTMS/ETCS Level 1

The ERTMS/ETCS Level 1 (see figure 6.1) is a spot-transmission-based train control system overlaid onto conventional lineside signaling. In level 1, the trackside generates movement authorities relying on conventional means to determine train position and integrity. The MA is then transmitted to the train via trackside equipment (e.g., Switchable Eurobalises, Euroloop, Radio Infill).

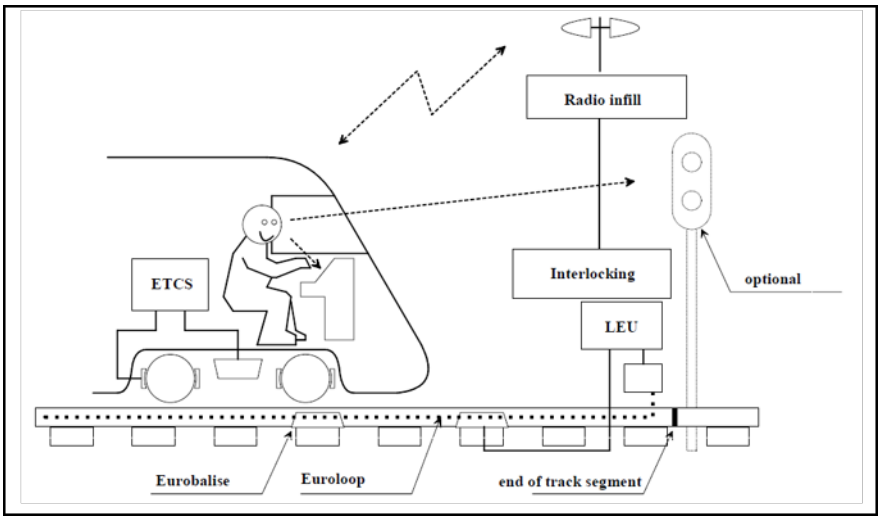


Figure 6.1: ERTMS/ETCS Application Level 1 with infill function by Euroloop or Radio infill

ERTMS/ETCS Level 2

The ERTMS/ETCS Level 2 (see figure 6.2) is a radio-based train control system where the lineside signals can be suppressed. Concretely, GSM-R is used for bi-directional communication between the track and the train and transmitting movement authorities to the train. The MA calculated

by the trackside relies on conventional trackside means to determine train position and integrity. Fixed Eurobalises are used for location referencing.

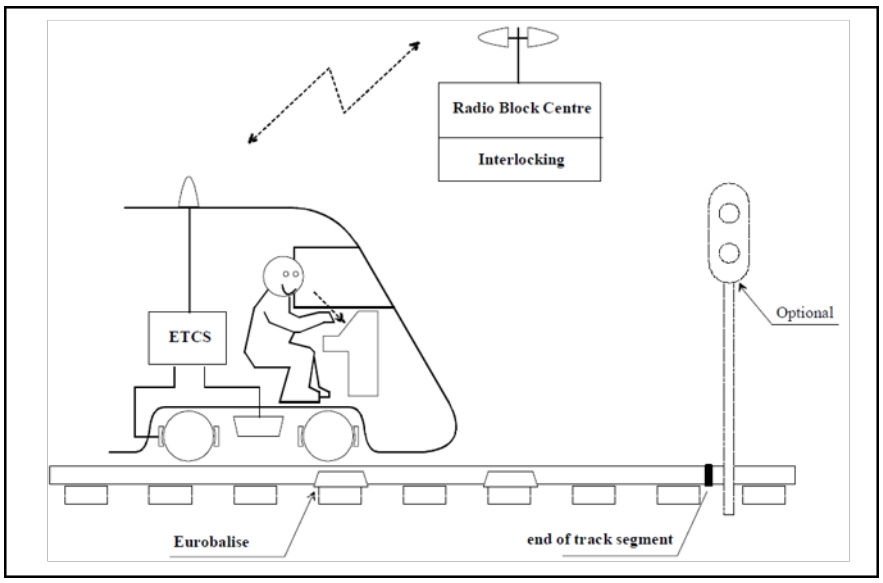


Figure 6.2: ERTMS/ETCS Application Level 2

In ERTMS/ETCS Level 2, the Eurobalises position on the track is defined during the design phase of the signaling system. Such a positioning depends on the specific signaling rules to be applied.

For instance, balises may be located at:

1. a point where a change of the speed limit must be communicated to the train
2. entrance of a station
3. before a track switching point
4. close to a signal in order to repeat its status (e.g., red) to the on-board equipment (i.e., the on-board automatically stops the train when reads this information).

Annex B: The existing constellations of Global Navigation Satellite Systems

GNSS is a comprehensive term that refers to Global Navigation Satellite System. If the GPS system is certainly the most famous satellite localization system, it is nevertheless not the only system currently available. In fact, the GNSS concept encompasses four distinct systems (see figure 6.3). Namely:

- the American GPS
- the Russian GLONASS
- the European GALILEO
- the Chinese BeiDou

Each of the aforementioned systems employs a number of orbital satellites, called constellations.

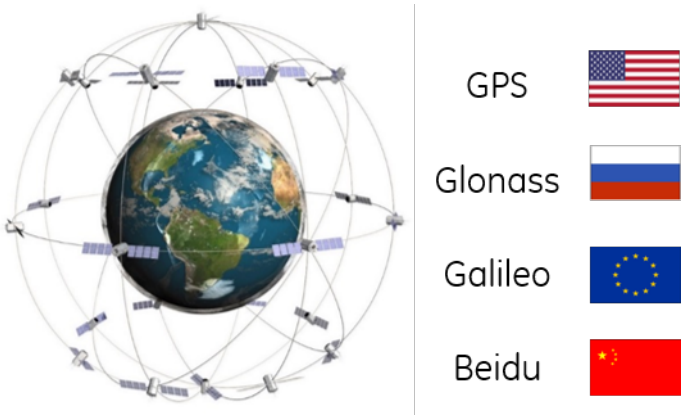


Figure 6.3: The currently existing GNSS constellations.

In particular, an overview of these constellations composition and development history are briefly presented hereafter.

The Global Positioning System (GPS)

The *Global Positioning System (GPS)* developed in the United States by the Department of Defense (DoD) is the first Global Navigation Satellite Systems (GNSS).

From a historical point of view, the first GPS satellite was launched in 1979. Although the constellation only became complete and fully operational in 1995.

It is noted that the GPS was originally designed as a navigation system for U.S. military users (in particular for ballistic missile tracking). Providing an unequaled accuracy compared to the positioning systems of that time, the satellite system became a necessity from a military point of view. Later on, GPS was gradually opened for civil applications (particularly in the aeronautical field). Currently, the GPS is a dual-use system for both military and civilian users.

The baseline GPS constellation contains 24 Medium Earth Orbit (MEO) satellites disposed in six Earth-centered orbital planes. Each plane hosts four satellites and has a radius of 26,560 km (i.e., about 20,163 km above the Earth). To ensure this requirement, the Air Force has been flying 31 operational GPS satellites (24 active + 7 spares).

In the context of the Cold War, the GPS equivalent system GLONASS was developed.

GLONASS (Global'naya Navigatsionnaya Sputnikovaya Sistema)

GLONASS (Global'naya Navigatsionnaya Sputnikovaya Sistema) is the Russian counterpart system to GPS. The GLONASS, initially developed for military use by the former Soviet Union, was declared fully operational in 1996.

Its nominal constellation comprises 24 active MEO satellites (21 active satellites + 3 active spares) in three orbital planes separated by 120 degrees. The satellites operate in circular 19,100-km orbits at an inclination of 64.8 degrees to the Earth's surface.

However, the system fell rapidly in the following five years without sufficient maintenance due to financial problems. By the end of 2001, it operated with only eight satellites.

In 2011, the Russian government restored the 24 satellite constellation, which is currently operated as a dual-use system for both civil and military users.

In the 21st century, both European Union (EU) and China are launching navigation satellites for their Galileo and BeiDou Navigation Satellite System (BDS) to provide similar functions and performances like GPS and GLONASS.

GALILEO

Unlike GPS and GLONASS, the Galileo system is a European GNSS specifically designed for civilian use. *Galileo* is an independent system initially built by the European Union and European Space Agency.

The idea of Galileo began in the early 1990s, and the different concepts for Galileo were unified by the agreement of four EU countries (the United Kingdom, Germany, Italy, and France) at the end of 1999. In 2000, the feasibility and definition phases of the Galileo system were finally completed.

The Galileo constellation consists of 30 MEO satellites, divided within three operational orbital planes at an altitude of 23,616 km above the Earth's surface and with an inclination of 56 degrees. Each orbital plane hosts nine operational satellites and one active spare satellite.

BeiDou navigation satellite system (BDS)

Compass Navigation Satellite System (CNSS) is the Chinese-developed GNSS. This system is commonly known as the BeiDou navigation satellite system (BDS).

On its first test stage, called BeiDou-1, the navigation system was only available for local operation. BeiDou-1 became fully operational in 2004 and provided services to users over China and surrounding areas as a regional satellite navigation system.

Later on, the China National Space Administration decided to upgrade the BeiDou-1 system in order to cover the whole world. Therefore, this extended system known as the BeiDou-2 became the fourth GNSS in the world.

The design for the Beidou-2 system consists of a constellation of 27 MEO satellites (3 Inclined Geosynchronous (IGSO) satellites + 5 five Geostationary (GEO) satellites). The MEO satellites are equally split into six orbital planes at an altitude of about 21,500 km above the Earth's surface and with an inclination of 55 degrees.

Finally, the BeiDou-2 system provides both civilian and military service.

Annex C: Definitions of key safety-related terms

To help the reader unfamiliar with safety terminology, but also to avoid any ambiguities, we provide definitions of key safety concepts below. These definitions are derived from (IEC 61508-4: 2010; EN 50126 : 2017)

1. Risk / Harm / Hazard.
   (a) **Risk** is the probable rate of occurrence of a hazard causing harm and the degree of severity of the harm. The characteristic of risk can be estimated as:

   $$Risk = probability\ rate\ of\ occurrence\ of\ harm \times severity\ of\ harm.$$

   (b) **Harm** represents the physical injury or damage to the health of people or damage to property or the environment.
   (c) **Hazard** is defined as the potential source of harm and includes danger to persons arising within a short time scale (e.g., fire and explosion) in addition to those that have long-term effect on the health.
2. Constraints (Fault/ Error/ Failure):
   (a) **Fault**: abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.
   (b) **Error**: discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.
   (c) **Failure**: termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required.
3. Means
   (a) **Fault avoidance** : use of techniques and procedures that aim to avoid the introduction of faults during any phase of the safety lifecyle of the safety-related system.
   (b) **Fault tolerance** : ability of a functional unit to continue to perform a required function in the presence of faults or errors.
   (c) **Fault elimination** : is the reduction of the presence of faults in terms of number and severity.
   (d) **Fault prevision**: is the prediction of the presence of faults, the conditions of their occurrence and their consequences.

Annex D: Estimation of RAMS performances of repairable systems

The present appendix is complementary to Chapter 3 of this manuscript and introduces key time indicators that can be employed to represent the RAMS performances of repairable systems.

Key time indicators related to systems dependability

In the industry, average time indicators are often used to represent the different temporal phases of repairable systems (cf. figure 6.4).

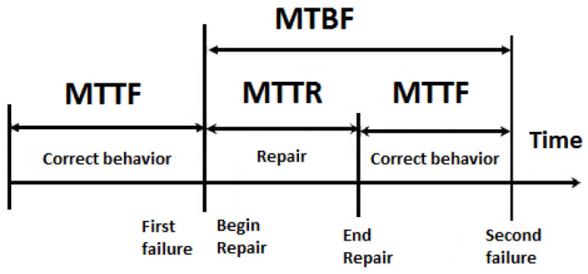


Figure 6.4: Dependability mean-time indicators

In particular, the Mean time between failures (MTBF) and Mean Mean Time to Repair (MTTR) can be defined as follows:

1. **Mean time between failures (MTBF)** is the average time between system breakdowns. MTBF is a crucial metric to measure performance, safety, and determine the reliability.
2. **Mean Mean Time to Repair (MTTR)** is the expected time to achieve restoration. MTTR encompasses:
   (a) the time to detect the failure.
   (b) the time spent before starting the repair.
   (c) the effective time to repair.
   (d) the time before the component is put back into operation.

The other relevant time indicators are listed in the following table:

MTTF	Mean Time to Failure
MTBF	Mean Time Between Failure
MTTR	Mean Mean Time to Repair (Restoration)
MUT	Mean Up Time
MDT	Mean Down Time

Table 6.1: Dependability time indicators

Here, it is noted that such time indicators can be further employed to quantitatively represent the RAMS parameters of repairable systems.

Reliability calculation

Reliability is a probabilistic value commonly represented by $R(t)$ or by its compliment represented by $F(t)$, where $F(t) = 1 - R(t)$. On the other side, the reliability is related to the so called *failure rate* represented by $\lambda(t)$. If the failure rate is constant, it is then noted λ and the reliability can be calculated as:

$$R(t) = e^{-\lambda . t} \tag{6.1}$$

Employing the time indicators, reliability can also be expressed in terms of Mean Time to Failure (MTTF) as:

$$MTTF = \int_0^\infty R(t).dt = \frac{1}{\lambda} \tag{6.2}$$

It is also noted that MDT is very small compared to MUT for many systems. Therefore, it can be assumed that $MTTF \simeq MTBF$. Thus:

$$MTBF = \frac{1}{\lambda} \tag{6.3}$$

Availability calculation

For availability calculation, the average availability defined by the ratio between the up-time and the total time is commonly used. Under certain conditions such as constant failure and repair rate, the mean availability is expressed in its simplest representation using the following equation:

$$A = \frac{MUT}{MUT + MDT} \leq 1 \tag{6.4}$$

Considering that the time interval between the failure occurrence and its detection is included in the MTTR, and in the case of no planned preventive maintenance is applied, one can conclude that: $MDT = MTTR$. Hence, another equation to calculate the availability (A) is

$$A = \frac{MTTF}{MTTF + MTTR} \tag{6.5}$$

Maintainability calculation

The maintainability attribute calculation supposes that the system is repairable. In that case, the Mean Time To Repair (MTTR) is typically used to express the maintainability performance. Concretely:

$$MTTR = \frac{1}{\mu} \tag{6.6}$$

in which μ represents the *reparability rate*.

Safety estimation

The safety integrity can be associated with different *safety integrity levels (SIL)*. These discrete levels (one out of possible four) correspond to a range of safety integrity values, where safety integrity level 4 represents the highest level of safety integrity while level 1 is the lowest. The target failure measures associated with the SIL levels in the case of a safety function operating in a high-demand mode of operation or continuous mode of operation (e.g., train localization) are presented in the following tab 6.2 (EN 50129: 2018 adapted from IEC 61508-1: 2010).

Safety integrity level (SIL)	Tolerable Hazard Rate (THR) per hour and per function
4	$\geq 10^{-9}$ *to* $< 10^{-8}$
3	$\geq 10^{-8}$ *to* $< 10^{-7}$
2	$\geq 10^{-7}$ *to* $< 10^{-6}$
1	$\geq 10^{-6}$ *to* $< 10^{-5}$

Table 6.2: Safety integrity levels

Note: we note that the concept of *safety* should not be confused with the *Security* which represents the robustness against intentional hostile action.

Links between RAMS properties and their characteristics

The links between all RAMS attributes previously introduced in this subsection and the parameters allowing to quantify them can be summarized in the figure 6.5 (from Lu 2014):

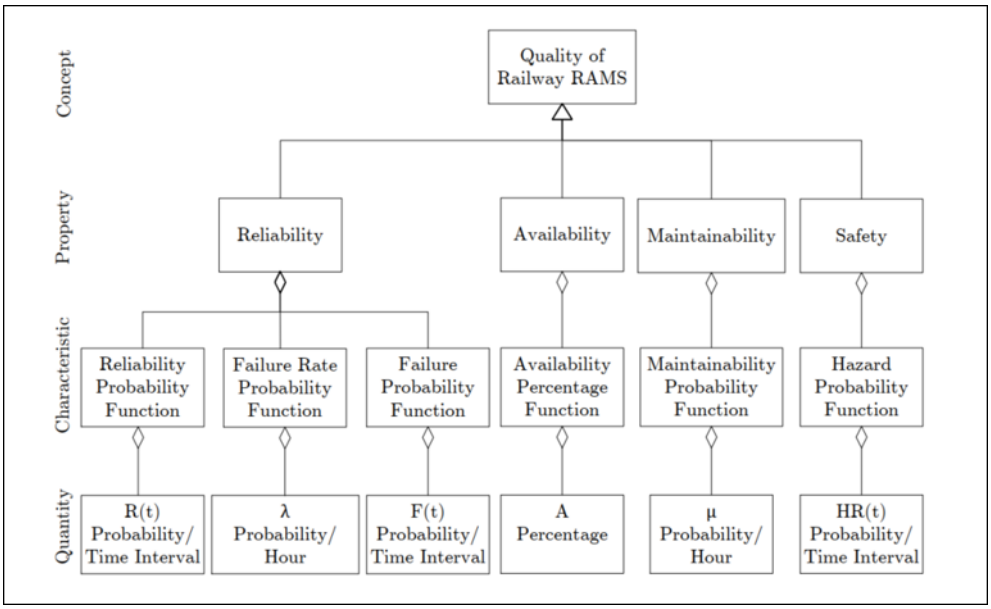


Figure 6.5: RAMS attributes used for Railway systems

Annex E: Stanford diagram

In this appendix section, we provide a synthesized representation of the GNSS integrity-related concepts employed in this manuscript. Concretely, the relation linking those parameters can be illustrated through the commonly used Stanford diagram (or Stanford plot) (Tossaint et al. 2006).

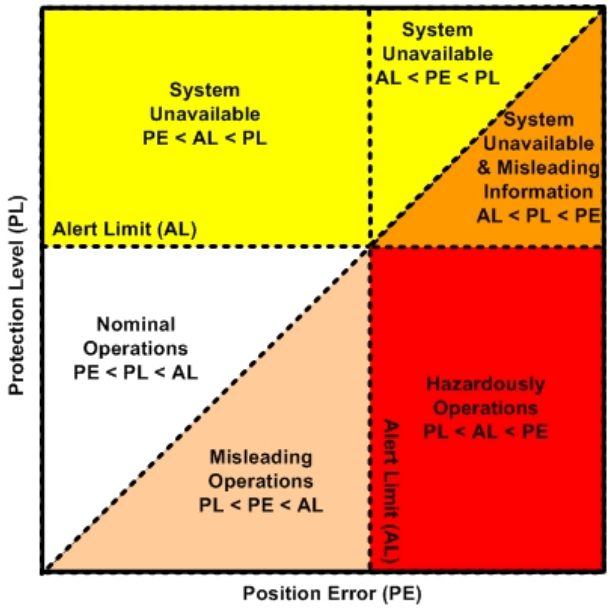


Figure 6.6: The Stanford diagram

Moreover, it is noted that the Stanford diagram tool specifically allows to distinguish between two types of integrity events (see Figure 6.6):

1. Misleading Information (MI) events.

2. Hazardously Misleading Information (or HMI) events

In particular, a *misleading information event* occurs when, being the system declared available (i.e., $PL < AL$), the position error exceeds the protection level but not the alert limit.

$$PL < PE < AL \tag{6.7}$$

In contrast, a *hazardously misleading information event* occurs when, being the system declared available (i.e., $PL < AL$), the position error exceeds the alert limit.

$$PL < AL < PE \tag{6.8}$$

Contents

Contribution to Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach.

Abstract

Transportation systems are safety-critical systems whose failures may result in considerable losses. In railway transportation, this may involve damage to equipment and environment, serious injury to people or even the loss of human lives. In order to avoid train collision or derailment, safety-related functions (e.g., management of routes allocation, safe distance separation between trains, and over-speed prevention) are implemented. These functions are at the core of railway control-command and signaling systems (CCS) which provide the driver with the relevant information and warnings to adapt the speed of the train or brake when necessary.

Historically, European rail CCS systems were developed on a national basis. Hence, the absence of common technical and operational standards has considerably limited the railway interoperability between countries. That is why the European Rail Traffic Management System (ERTMS) standard was defined with the aim of harmonizing the railway systems throughout Europe. More specifically, European Train Control System (ETCS) is the CCS component of the ERTMS. This system is essential to guarantee the safe and interoperable operation of trains. To enhance the competitiveness of rail transport services, the introduction of innovative solutions is under study in view of the evolution of ETCS. In this context, the adoption of Global Navigation Satellite System (GNSS) for train localization is investigated as a technology which can ensure an undeniable added value for railways. In particular, the adoption of such satellite-based solution should permit the train to autonomously and continuously determine its location. Hence, implementing more flexible operating principles (i.e., Moving Block) that pave the way for increasing line capacity while reducing maintenance and operating costs shall be possible.

However, the introduction of such technological innovations leads to the emergence of new risks that need to be investigated meticulously. Accordingly, a main challenge is to provide safety evidence permitting the certification of these new systems. In particular, classical safety analysis approaches (e.g., FMECA, HAZOP, FTA) show limitations in dealing with the complexity of such systems. Therefore, more adapted safety and performance analysis techniques need to be elaborated.

The contribution of this thesis falls within this context by proposing a model-based approach to evaluate performance and safety properties related to the use of GNSS-based localization systems in railway. Specifically, the investigated method consists in translating the relevant behavior of the train localization system through a modular and configurable representation.

Considering the safety-critical aspect of the localization function in railways, formal methods which are based on rigorous mathematical foundations are adopted in the present work. Namely, probabilistic timed automata formalisms are employed. Concretely, such notations allow for considering stochastic and dynamic aspects, so as to reflect the GNSS-related uncertainties in a trustworthy way.

The elaborated models being parameterizable, various operational scenarios, considering a wide range of configurations, can be investigated. Such a feature is particularly relevant considering the impact of the environmental conditions on the GNSS performances.

Then, the safety and performance properties to be checked can be formulated by means of temporal logics. Accordingly, the analysis of such features can be achieved by means of model-checking and simulation techniques. This evaluation phase yields both qualitative and quantitative results and allows for assessing the impact of various parameters and functional choices on both safety and performance. In this thesis, UPPAAL-SMC is used to set the tooling chain of our approach, and to provide illustrative numerical analysis results considering various operational cases study.

Finally, as the present contribution implements a model-driven technique to perform safety analysis in railways, it is fully in line with the increasing willingness to reduce recourse to on-site tests in the sector (as such costly and time-consuming tests jeopardize the introduction of technical innovations in railways).

Keywords: railway system safety; model-based approach; gnss-based train positioning; formal methods; ERTMS/ETCS; intelligent transportation systems

Résumé

Les systèmes de transport collectifs sont des systèmes critiques dont les défaillances peuvent entraîner des pertes considérables. Dans le cas du transport ferroviaire, ces défaillances peuvent mener à des dommages matériels ou environnementaux, des blessures graves ou des décès de personnes. Afin d'éviter les collisions et les déraillements de trains, des fonctions liées à la sécurité telles que la gestion des itinéraires, la séparation entre les trains et la prévention de survitesses, sont mises en œuvre. Ces fonctions sont au cœur des systèmes de Contrôle-Commande et de Signalisation ferroviaire (CCS) et fournissent au conducteur les informations et les avertissements nécessaires leur permettant d'ajuster la vitesse du train ou de freiner si nécessaire.

Historiquement, les systèmes CCS ferroviaires européens ont été développés sur la base de principes nationaux. De ce fait, l'absence de normes communes a considérablement limité l'interopérabilité ferroviaire entre les pays. C'est pourquoi, le système européen ERTMS (European Rail Traffic Management System) a été défini dans le but d'harmoniser les systèmes ferroviaires à travers l'Europe. Plus précisément, le système européen de contrôle des trains ETCS (European Train Control System) est la composante CCS de l'ERTMS. L'utilisation de ce système est requise pour garantir l'exploitation sûre et interopérable des trains. Afin de répondre à la demande croissante et renforcer la compétitivité des services de transport ferroviaire, l'introduction de solutions innovantes est actuellement à l'étude en vue de l'évolution de l'ETCS. Dans ce contexte, les technologies de rupture comme celles s'appuyant sur les GNSS (systèmes globaux de navigation par satellite) sont explorées pour améliorer la localisation des trains. En effet, l'adoption de solutions satellitaires permettra à un train de déterminer sa position de manière autonome et continue. Ainsi, il sera possible d'implémenter des principes d'exploitation plus flexibles (tels ceux liés aux cantons mobiles) permettant d'augmenter la capacité des lignes tout en réduisant les coûts de maintenance et d'exploitation.

Toutefois, l'introduction de ces innovations technologiques entraîne l'apparition de nouveaux risques qui doivent être analysés méticuleusement. En conséquence, l'un des principaux défis consiste à fournir des preuves de sécurité permettant la certification de ces nouveaux systèmes. En outre, les approches classiques d'analyse de la sécurité (par exemple, AMDEC, HAZOP, FTA) montrent des limites face à la complexité de ces systèmes. Ainsi, des techniques d'analyse de sécurité et de performance plus adaptées doivent être élaborées.

Ces travaux de thèse s'inscrivent dans ce contexte en proposant une approche orientée modèles afin d'évaluer des propriétés de sécurité et de performance liées à l'utilisation de systèmes de localisation intégrant les GNSS pour l'exploitation ferroviaire. Compte tenu de l'aspect critique de la sécurité liée à la fonction de localisation, les méthodes formelles qui reposent sur des fondements mathématiques et logiques rigoureux sont mises à profit. En particulier, les formalismes d'automates temporisés probabilistes sont employés. Concrètement, ces notations permettent de prendre en compte les aspects temporels et aléatoires dans le comportement de la fonction de localisation, de manière à refléter les incertitudes liées au GNSS d'une manière fiable. Les modèles élaborés étant paramétrables, divers scénarios opérationnels, considérant une large variété de configurations, peuvent ainsi être étudiés. Cette possibilité est particulièrement pertinente compte tenu de l'impact des conditions environnementales sur les performances du GNSS. Sur la base des modèles développés, des propriétés de sécurité et de performance à vérifier peuvent être formulées au moyen de logiques temporelles. En conséquence, l'analyse de ces caractéristiques peut être réalisée à l'aide de techniques de vérification analytique et de simulation. Cette phase d'évaluation permet d'obtenir des résultats qualitatifs et quantitatifs et offre la capacité d'anticiper l'impact de différents paramètres et choix fonctionnels sur la sécurité et les performances. Dans cette thèse, l'outil UPPAAL-SMC est utilisé comme support à notre approche et nous permet d'obtenir des résultats d'analyse numérique illustratifs, en considérant divers cas d'étude opérationnels. La contribution proposée adoptant des techniques fondées sur des modèles répond avantageusement à la volonté croissante de réduire le recours aux essais sur site ferroviaire pour vérifier des conditions ou propriétés de sécurité. Ces essais étant coûteux et chronophages, ils compromettent l'introduction d'innovations techniques dans le secteur ferroviaire.

Mots clés : sécurité des systèmes ferroviaires ; approche fondée sur les modèles ; positionnement des trains par gnss ; méthodes formelles ; ERTMS/ETCS ; systèmes de transport intelligents