Implementation of a Model-Oriented Approach for Supporting Safe Integration of GNSS-Based Virtual Balises in ERTMS/ETCS Level 3

Ouail Himrane, Julie Beugin, Mohamed Ghazel

IEEE Open Journal of Intelligent Transportation Systems

Received XX Month, XXXX; revised XX Month, XXXX; accepted XX Month, XXXX; Date of publication XX Month, XXXX; date of current version XX Month, XXXX.

Digital Object Identifier 10.1109/OJITS.2022.1234567

Implementation of a Model-Oriented Approach for Supporting Safe Integration of GNSS-Based Virtual Balises in ERTMS/ETCS Level 3

OUAIL HIMRANE*, JULIE BEUGIN*, AND MOHAMED GHAZEL*

[1]Univ. Gustave Eiffel, COSYS-ESTAS, F-59650 Villeneuve d'Ascq, France

CORRESPONDING AUTHOR: Julie Beugin (e-mail: julie.beugin@univ-eiffel.fr).

This research has received funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation program under Grant Agreement N. 101015416 (PERFORMINGRAIL). The JU receives support from the European Union's Horizon 2020 research and innovation program and the Shift2Rail JU members other than the Union.

ABSTRACT Moving Block is a railway signaling concept that paves the way for increasing line capacity while reducing maintenance and operating costs. Its implementation relies on autonomous solutions for train localization, mainly based on GNSS technology. However, the introduction of such technological innovations leads to the emergence of new risks. These risks need to be investigated meticulously, and some confidence level needs to be assigned to GNSS-based localization solutions in railways while considering various settings. The contribution of this paper falls within this context by bringing formal approaches into play in order to evaluate performance and safety properties related to the use of GNSS-based virtual balises for train localization. Specifically, the adopted model-based approach consists in translating the relevant behavior of the localization system through configurable timed and probabilistic automata. The elaborated models being parameterizable, various test scenarios, considering a wide range of configurations, can be investigated. Quantitative and qualitative analysis results can be generated on the basis of our models by means of statistical model-checking algorithms implemented in the UPPAAL-SMC modeling and verification tool. A case study is used to illustrate the application of the presented approach, and various numerical analysis results are provided. As the present contribution implements a model-driven approach 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. Such tests are indeed costly and time-consuming, thus jeopardizing the introduction of technical innovations in railways.

INDEX TERMS ERTMS/ETCS L3, Fixed Virtual Block, Formal Model, GNSS-based localization, Moving block, Railway safety, Statistical Model-Checking, Train positioning, Virtual balises

I. INTRODUCTION

IN railway transportation, the localization function plays a critical role in the safe control of train movement and in traffic management. New technologies, such as GNSS-based systems (Global Navigation Satellite Systems), offer promising means to implement this function while allowing for better operational performances. Furthermore, beyond performance improvement, such solutions allow new operational concepts and principles to be implemented, such as the concept of *'virtual balise'* that will be addressed later in this paper.

Introducing virtual objects for the control of train movement was initially envisaged by means of the *'virtual block'* concept which aims at shortening urban train separation distance, and thus increasing metro line capacity [1], [2]. Indeed, virtual block sections subdivide a classical fixed block section[1] into several ones, allowing the presence of more trains throughout the line. Besides, the *'moving block'*

[1]When lines are divided into block sections, a train must not enter a block section until it has been cleared by the train ahead. This allows safe train separation [3].

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

concept is based on virtual blocks and amounts to (theoretically) reducing the length of virtual block sections to zero. In so doing, the moving block notion allows for considering a minimal and dynamical virtual protection zone around the train for ensuring safe and optimal operation [3]. The virtual/moving block notions are today investigated for improving the operation of conventional and high-speed railway lines. They lie today at the center of the highest operational level (L3) of ERTMS (European Rail Traffic Management System), which is the European railway control/command and signaling standard[2]. Virtual/moving block concepts are known under the FVB and FMB principles (respectively Fixed Virtual Block - Full Moving Block) in the framework of ERTMS L3 [5].

However, the monitoring of virtual/moving block occupancy requires to track in a more precise way train position, which is under the responsibility of the localization function. Currently, in ERTMS, this function has another goal: to ensure the control of speed limits on-board train and to guarantee train stop prior to dangerous location. It relies on a number of embedded sensors interacting with trackside equipment, the balises, distributed punctually along the block sections. Virtualization techniques have also been extended to balises by using software applications and databases (geographical data and embedded telegrams), both emulating the role initially fulfilled by trackside equipment. In particular, instead of using the geographical reference position classically provided by the physical balises, GNSS-based localization devices constitute an interesting alternative solution for providing such position references [6]. It is plain that integrating virtual objects in the railway control-command can substantially reduce the installation and maintenance costs of equipment deployed all along the track, i.e. the trackside train detectors installed on the block sections and the physical balises. However, it is less clear whether or not virtual balises can improve directly operational performances. For this purpose, an adjustment between the size of virtual block sections (in FVB operation)/the safety margins added in the moving blocks (in FMB operation), the number of block sections if virtually defined, and the number and the location of balises need to be conjointly investigated for reaching optimized operational performances. Such investigation raises a number of tricky issues, and requires tackling the interaction complexity between the existing physical components and the new virtual items that are part of the railway control-command system.

In this context, the Shift2Rail 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, and PERFORMINGRAIL. Among different innovative topics pertaining to the ERTMS railway standard, these research projects explore the concepts of virtual blocks, moving blocks, and virtual balises, particularly in terms of safety and performance evaluation. They have resulted in the definition of early and high-level specifications for ERTMS L3 that will be improved and detailed in the next European program supported by Europe's Rail, the successor of Shift2Rail [7]. Yet, no detailed specifications that can serve as a stable baseline for the implementation of ERTMS L3 are available nowadays.

In the H2020 European program as well as in previous European research programs, some projects have explicitly focused on GNSS-based on-board systems with the aim of proving the feasibility of using such systems to implement the railway localization function [8]. Projects such as STARS, RHINOS, ERSAT-GGC, ASTRAIL and GATE4RAIL have resulted in multiple innovative solutions, large measurement campaigns and testing platforms 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 on satellite signals 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 heighten safety risks.

Considering the safety-critical aspects 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 to define the safety requirements and to provide a set of safety evidence that allows their certification in accordance with the in force regulations (today the CCS Technical Specification of Interoperability [9]). For this purpose, the safety analysis has to be conducted at railway system level, not only at the localization system level, in order to consider the global risk of the system in operation within a given environment. Nevertheless, it can be observed that, today, safety analyses focus more on the embedded equipment, mainly because the constraints induced by the railway environment on GNSS signals are very difficult to characterize and quantify. Important efforts are also spent on the development of robust architectures and fault detection techniques using fail-safe principles. Besides, performing ad-hoc on-site tests of such architectures proves to be awkward, costly, and very time-consuming. In general terms, the variable impact of the railway environment on GNSS based-systems and its complex interactions with the different control-command parts constitute a considerable obstacle for defining a generic and systematic safety assessment process that can be useful for the deployment and the acceptance of such systems in railway CCS.

It follows that advanced safety and performance analysis techniques need to be elaborated to foster the introduction of GNSS-based solutions in railways and set the stage for innovative, performing and safe railway operational modes.

[2]To go deeper into operation levels and modes of ERTMS, the reader can find a detailed description in [4].

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

The present paper focuses on the most mature GNSS-based solution, which is based on the concept of virtual balise [6] and the developed approach brings into play the model-checking technique. Namely, it is a formal method that offers significant advantages in terms of safety and performance analysis of dynamic systems. Formal methods are based on mathematical and logical foundations that allow for rigorously describing the system behavior and set a basis for automatic verification of a wide range of settings. It is plain that such model-based approaches offer substantial gains in terms of time and cost, particularly when compared to on-site testing. In fact, the underlying idea is to establish parameterizable models that can cope with various operational configurations. Therefore, the analysis of different settings can be performed at the cost of a minimal adaptation effort.

The contribution discussed in this paper aims to apply a comprehensive model-oriented approach that is agnostic from the technical localization solution while considering the main features pertaining to the use of GNSS-based systems, in order to analyze and quantify safety-related properties and operational settings. A particular focus is made on the operating principles dedicated to virtual balise implementation in the context of ERTMS/ETCS L3. Based on formal behavioral models that are adaptable to different systems' features and different operational situations, the approach is aimed to include the parameterization of the model settings. This allows any GNSS-based localization solution to be addressed, considering it as a "Black box" and only requiring the characterization of its safety-related performances. Enabling the models versatility and reusability offers the possibility to fine-tune different operational characteristics while ensuring operational safety. As will be highlighted in Section II, to the best of our knowledge, no such methodology has been proposed to set safe and efficient configuration data, which are of crucial importance for railway safety and signaling engineers. In fact, the present work capitalizes on the preliminary work presented in [10] and [11] while proposing several extensions and useful quantitative results. Namely, [10] is mainly focused on motivating the development of a modular approach, that is based on formal models, towards evaluating safety properties in a railway signaling system that deploys a GNSS-based localization function. The paper also discusses the operational, functional and dysfunctional aspects that need to be considered. Modeling the various GNSS environments is also proposed, and a preliminary rough model of the train movement is also sketched out. Then, [11] is mainly devoted to explaining how safety features can be investigated on the basis of some developed timed automata models, constituents of the detailed approach. Some models emulating the reading of physical balises and GNSS-based virtual balises and train movement are provided. Then, the way safety properties can be formalized by means of watchdogs is explained. The paper also discusses the various parameterizations that can be performed on the models. Now, in the present paper, several amendments have been made to the preliminary models established in [10] and [11], and some new modules have been added to make our evaluation more realistic (as will be discussed in the sequel). Moreover, the evaluation of safety and operational features based on the various developed models is discussed. Besides, as will be detailed later on (cf. Section V), we show how the adopted reasoning can be advantageously re-used to investigate different line layouts while considering the different uncertainties that may impact train localization and, hence, operational safety. For this to be achieved, an ERTMS/ETCS L3 case study is described and analyzed through three settings of parameters used to tune the developed models.

The remainder of this paper is organized as follows. Section II introduces the context and outlines the main related works. The *'virtual balise'* concept is presented in Section III, in which some models to describe the uncertainties related to the train localization based on the use of virtual balise are also established. Section IV discusses the global parametric model, encompassing all the established models, which serves as a basis for our approach. In this section, the various impacting parameters and the properties to be investigated are also presented. In Section V, different simulation scenarios are established accordingly. Then, the simulation results are presented and discussed. Finally, some concluding remarks as well as the perspectives of this work are addressed in Section VI.

II. CONTEXT AND RELATED WORKS

In this section, we first describe how the localization function is involved (among other functions) to ensure safe operation of trains under ETCS. In this context, we specifically focus on the operation under ETCS levels 2 and 3 for which the use of GNSS-based localization solutions proves to be promising. To understand the impact of using GNSS-based localization in railways, we thereafter discuss the various safety aspects related to the use of GNSS as a means for the localization function. Finally, a brief review of the existing works that deal with safety assessment of GNSS-based systems in the railway domain is presented, with a specific focus on the approaches using formal methods.

A. THE LOCALIZATION FUNCTION UNDER ETCS OPERATION

ETCS is broken down into equipment embedded in trains (ETCS On-board) and trackside equipment (ETCS Trackside). In ETCS L2 and L3, the localization function is ensured by ETCS On-board. The latter relies on an embedded localization unit, which has to estimate the train position with some confidence interval. Note that, in the following, the localization function is considered equivalent to the train positioning. Moreover, *'Train positioning'* and *'Train location management'* are different though interrelated functions. Indeed, the latter monitors the presence/absence of trains on

each part of the railway line, i.e. the *'track occupancy'*, and ensures the *'safe train separation'* on a track. As explained below, the track occupancy is determined differently in ETCS L2 and L3; however, the safe train separation relies on the same principle: ETCS Trackside regularly provides each train with an up-to-date target point until which it is allowed to proceed. The distance between the train front-end and its allocated target point, associated with the permitted speed, is called *'Movement Authority'* (MA), while the target point is called *'End of Authority'* (EoA). MA data are sent by the trackside sub-system through a radio communication link.

ETCS L2 uses the traditional train separation method based on dividing the line into fixed block sections. The block sections are delimited by physical devices (e.g., track circuits, axle counters). Based on the block occupancy status reported by the Trackside Train Detection devices (TTD), the ETCS Trackside determines the *'train location'*. With a TTD-based reporting, the system exactly knows the segment (or the segments, when the train is passing from one block to the next block) in which the train lies. This segment includes the train from its front-end (the head) to its rear-end (the tail). However, ETCS Trackside cannot determine the precise *'train position'* (of the train head) in a segment.

In ETCS L3, the train separation function is, instead, based on the *'train position'*. Initially, this information allows ETCS On-board to supervise the train speed and braking curve in order to stay behind the EoA as in the case of ETCS L2. In ETCS L3, it makes also possible the track occupancy to be established in a more precise way. For this purpose, the Train Position Reports (TPR), produced on-board and transmitted by radio to ETCS Trackside, must not only include the train front-end position, but also the train rear-end position. This latter can be estimated using an embedded unit called Train Integrity Monitoring System (TIMS), which is responsible for monitoring the train integrity, i.e., the potential loss of wagons if a mechanical link is broken. Based on TPR with the associated train integrity data, ETCS L3 no longer needs TTD-related physical equipment. Therefore, both the Full Moving Block (FMB) and the Fixed Virtual block (FVB) principles can be applied. In FVB, although the blocks are fixed, they can be used for implementing an FMB-like operation. Indeed, as they are only represented in a logical form in the trackside databases, they can finely discretize a railway line in small fixed sections by adapting the digital track configuration. Nevertheless, under the FMB operation, theoretically EoA can be issued in any point of the railway line, while under the FVB operation, EoA must correspond to some block extremity.

For lines on which a migration towards ETCS L3 is foreseen, a transition phase with mixed traffic (train equipped or not equipped with Moving Block system) is possible by using hybrid implementations. In this case, the ETCS Trackside should be able to manage both physical and logical train separation. Namely, physical separation shall be based on TTD, while logical separation on TPR. Thus, four types of ETCS L3 have been defined: Hybrid FVB, Hybrid FMB, FVB without TTD and, FMB without TTD. The development of ETCS L3 is nowadays carried out according to two related, though complementary, work-streams. The first is led by the Shif2Rail partners and focuses on developing the four MB variants. The second, led by EUG (ERTMS Users' Group) [5], focuses on a specific variant: hybrid FVB, also called hybrid Level 3 [12]. This last variant seems to be the most advanced development phase and actual tests have already been conducted on it such as those led in 2018 in Germany within the DB Living Lab [13], or those led in 2017 on a test track at the ETCS National Integration Facility (ENIF) provided by Network Rail (UK) [14].

Safety specification for ETCS sub-systems [9], [15] imposes very high safety requirements. The train localization function has then to meet a Tolerable Hazard Rate (THR) of 10^{-9} per operating hour. This constraint has been resolved in a satisfactory manner by a combination of balises[3] and odometry systems. These interoperable components are today used in ETCS L2 and will surely be used in ETCS L3, as most railway actors still request them, especially due to the absolute position references provided by the balises. Nevertheless, deploying *'physical balises'* (PB) on the track is substantially costly. Therefore, GNSS-based *'virtual balise'* (VB) systems are envisaged in ETCS L2 and L3 (their principles will be explained in Section III).

The underlying idea behind using VB is to emulate the behavior produced by PB without resorting to physical devices (balises). In general, balises can be placed to coincide with blocks' limits. Hence, by using VB, it becomes possible to virtually split the line into shorter sections without using additional physical devices (cf. Figure 1). However, choosing the location of the balises is an engineering matter since no rule in the specifications addresses this aspect. Besides, when upgrading existing lines toward ETCS L3 with the possible use of VB, the presence of some existing PB and new VB has also to be considered. The question of the gradual migration of an existing line by using new artifacts, such as VB, is of paramount importance. Indeed, the components which are already implemented on the line have to coexist with those to be deployed during the migration. This would not have been the case if a completely new line is built. However, in most cases, new constructions are avoided because they induce unaffordable infrastructure costs and can even be technically impossible due to geographical 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 paper will consider the presence of both types of balises along a

[3]Balises are passive electronic components that can be activated by an electromagnetic field continuously emitted by the train. Once activated, the balise sends a telegram containing information on its geographical position to the ETCS On-board module.

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

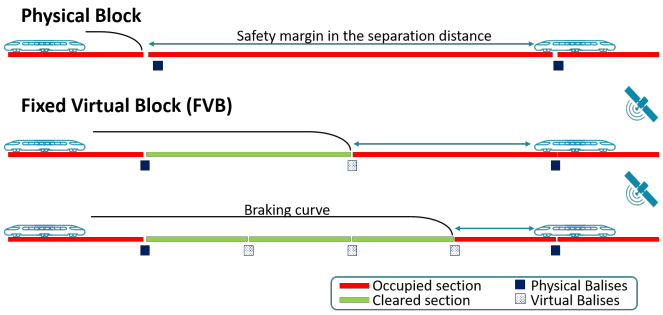


FIGURE 1. Example of balise implantation in ETCS Trackside.

line. Such a process can advantageously serve as a guide for railway signaling engineers to set a safe configuration of virtual balises on a given railway track.

B. GNSS-RELATED SAFETY FACTORS

A GNSS system (such as Galileo or GPS) includes a constellation of satellites in orbit, ground monitoring installations and user receivers. The satellites transmit signals that allow a receiver to estimate its position. This estimation is calculated by triangulation based on the signal propagation delay from the transmitters to the receiver. In the railway operation environment, the presence of obstacles, such as vegetation and buildings, can lead to signal perturbations that affect the position calculation process. Moreover, another issue is pertaining to the availability of the GNSS signals such as for instance when train enters tunnels or in harsh environments. In most cases, GNSS receivers are implemented in combined architectures in such a way that GNSS technology is integrated with additional sensors/digital means, which can compensate GNSS perturbations. Such a combined architecture offers several advantages as discussed in [16]. Therefore, safety and performance features have to be associated with the calculated position, especially in safety-critical applications [17]. Namely, "a measure of the trust that can be placed in the correctness of the information supplied by the navigation system" is defined as the *'Integrity Risk'* (IR). It refers to the probability of providing localization information out of some tolerance margin without warning the user within a given period of time [18]. The estimation of *IR* is based on a set of parameters that are dependent on the target application.

- The *'Position Error'* (PE), which is the difference between the estimated position and the actual position.
- The *'Alert Limit'* (AL), which represents the largest position error that allows for safe operation. The *AL* defines the error tolerance that cannot be exceeded without issuing a warning. Therefore, it is generally defined as an application-dependent safety requirement.

However, since it is not possible to know the actual position error in real time during the operation, a statistical bound to the position error, called *'Protection Level'* (PL), needs to be computed in order to measure the risk that the alert limit has been exceeded. As the train position is constrained by the track coordinates, only the one-dimensional component of the *PL*, called *'Along Track Protection Level'* (ATPL), can also be determined on the basis of the track description information.

The expected nominal operation mode implies to have a *PE* smaller than the calculated *PL* and a *PL* smaller than the *AL* (cf. Figure 2, case 1). Therefore, to allow the use of GNSS-based systems for train localization, it has to be proved that the delivered position information is never (or sufficiently rarely, *i.e.*, with a small acceptable probability) declared reliable and available when the actual *PE* exceeds *AL* while the estimated *PL* is smaller than *AL* (cf. Figure 2, case 2). In aeronautics, the authorities have already certified that an aircraft can realize a safety-critical APV (Approach with Vertical Guidance) with GNSS, especially with the EGNOS augmentation system [6]. An analogous certification process is needed in railways to ensure the required confidence level in terms of safety.

C. RELATED WORKS

In this section, we give a brief overview of the existing works that tackle the safety issues related to the use of GNSS-based localization systems in railways. With the localization function being safety-critical, such systems must go through a certification process to be adopted in railway CCS systems, such as ERTMS. In Europe, such a process is controlled by the ERA (European Union Agency for Railways[4]) and national railway safety authorities (e.g., EPSF in France, EBA in Germany). It results in an authorization for placing in service or on the market.

In fact, most of the certification effort focuses on providing a safety and quality set of evidences, which endeavors to prove that the system fulfills the relevant safety requirements. Therefore, on the one hand, some existing works have intended to define safety requirements and allocate quantitative safety targets to the functional parts of satellite-based localization systems [20], [21], especially in the case of the Virtual Balise Transmission System [22]. On the other hand, some studies have proposed means to demonstrate safety performances of different technical architectures [23], [24] and to qualify hazardous positioning errors w.r.t railway safety criteria [25], [26]. Furthermore, we can also find some contributions that establish links between aeronautical and railway safety criteria [27], [28]. In order to assess these criteria, on-site testing approaches have been used in the aforementioned works, benefiting from their great power of persuasion. However, the implementation of testing approaches is both expensive and time-consuming. Moreover, the obtained results are strongly dependent on the environmental testing conditions. Consequently, complementary *'zero on-site testing'* approaches, based on models and simulation, are needed to investigate different configurations and environments at a much lower cost. In this context and

[4] https://www.era.europa.eu/

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

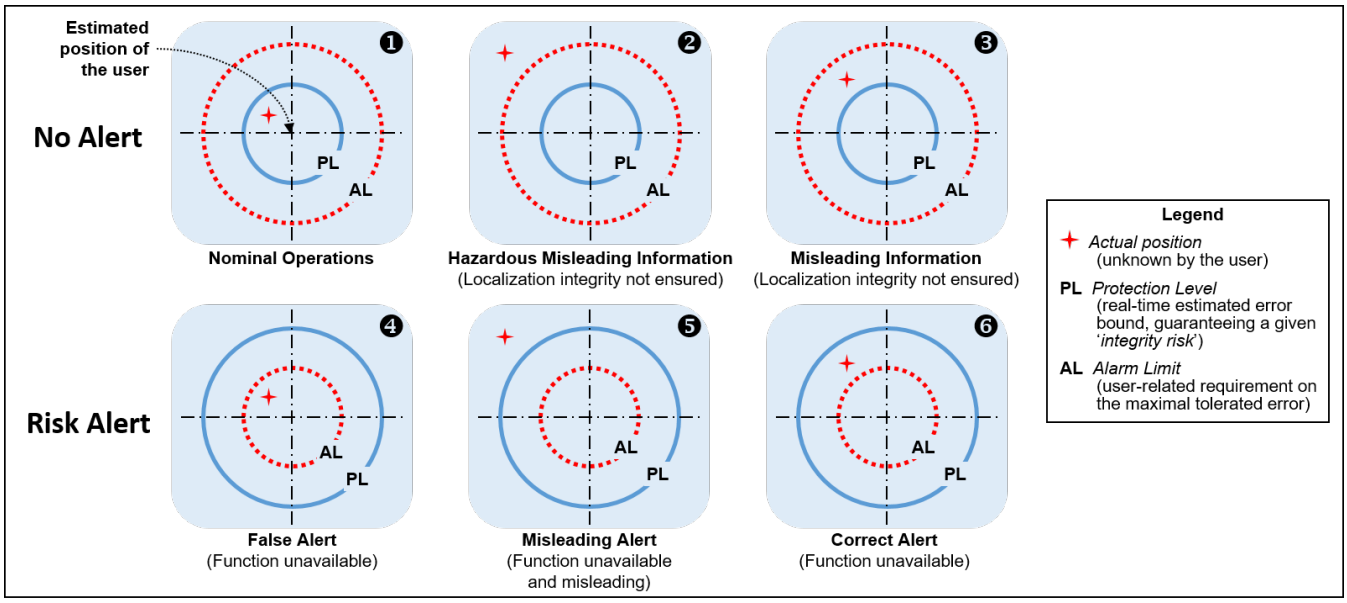


FIGURE 2. Illustration of the concepts related to the localization integrity risk using a 2-dimensional space [19].

in light of the strict safety requirements in the railway sector, a long-standing effort considers the use of formal methods and tools for the analysis of railway signaling systems [29]–[40]. Specifically, the recent works in [41] and [42] have presented a survey and a mapping study on various formal methods and tools used in railways. It should be noted here that a number of studies have addressed the assessment of railway safety properties, while tackling different use cases. In [43] and [44], the reliability of railway interlocking systems is considered, while [45] deals with the analysis of railway timetables. In [46], a moving block signaling system endowed with autonomous driving is modeled and analyzed, while considering various driving strategies. In [47]–[49], 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 coming from balises or GNSS. In [50], the occupancy of virtual tramway track sections at a simple junction was modeled and analyzed, considering random intervals around tram location continuously provided by means of a GNSS-based system. However, to the best of our knowledge, no study has provided comprehensive formal models that allow for quantitative assessment of safety properties pertaining to the use of GNSS-based localization systems in the railway domain, in particular with the operating principles specific to Virtual Balises.

In the following sections, we focus on the investigation of the train localization process with VB while considering the localization errors that such balises can introduce. In particular, we seek to finely and rigorously investigate the localization uncertainties induced by the use of VB in railway CCS, with the help of formal models. Such models are built while making particular effort to ensure reusability, modularity, and parametrization as detailed in [10], and models in [11] serve as a preliminary basis to the models established in the present work, while showing various extensions and some additional details. Namely, the parameterization aspects intervene in these models at several places, for instance when the mentioned uncertainties related to the operational environment are characterized depending on various distribution settings. Another aspect that will be shown is related to the reusability of the elaborated models to cope with different operational configurations. Having these features associated with the formal models, we can assess how well (in a probabilistic way) the safety requirements are fulfilled for different railway operational context where VB are employed for train localization.

III. BEHAVIORAL MODELS FOR THE VB-BASED LOCALIZATION SYSTEM

A. THE LOCALIZATION PROCESS WITH VB

As explained in Section II, railway localization is fundamental for performing the safe control of train movement. Traditionally, trains use on-board odometry to continuously estimate their position. Concretely, the odometer calculates the *'traveled distance'* from a *'reference position'* by monitoring the number of wheels revolutions. The reference position is acquired by means of physical balises installed along the track (set in groups). These balises allow odometry errors to be corrected punctually. Such errors are due to wheel jamming and slipping phenomena and are accumulated as the traveled distance increases until the next balise group is met. In between two successive groups of balises, the localization process involves a *'confidence interval'* (cf. Figure 3.a)) that is centered on the estimated train head position and whose

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

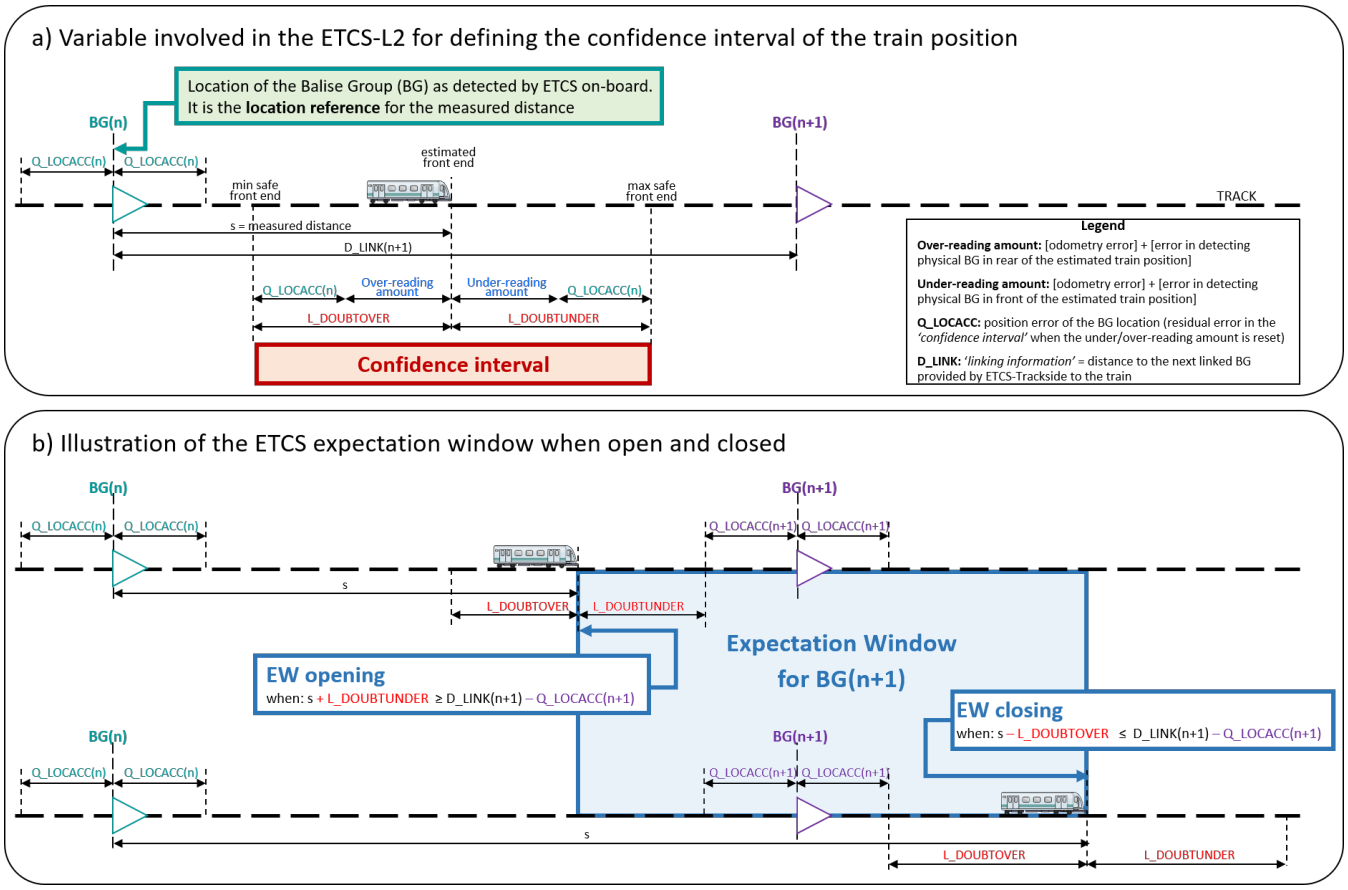


FIGURE 3. **'Confidence interval' and 'expectation window' concepts in ETCS.**

calculation process must be designed to include the actual train position with a minimal margin.

According to ERTMS specifications [51], the *'distance measured on-board'* can have an error that must not exceed $\pm(5 + 5\% \cdot s)$ meters, s being the estimated traveled distance. Hence, if the actual train position is in front (resp. in rear) of the estimated position, this latter is underestimated (resp. over-estimated). Consequently, the mentioned requirement can be expressed as follows: the *'under-reading amount'* (resp. the *'over-reading amount'*) shall be at most $5 + 5\% \cdot s$ meters. This threshold is a maximal value for the *'under/over-reading amount'* (illustrated in Figure 3.a)). Note that this requirement specifically refers to on-board localization errors, including odometry errors and *'balise detection'* related errors [52].

As mentioned above, the traveled distance is calculated w.r.t some reference position. Today, in ETCS L2, this reference position is provided by *physical balises (PB)* installed on the track and is updated to the location of the last activated balise. Moreover, by readjusting the estimated train position with the balise position, the *'over/under-reading amount'* is reset. Yet, a *'residual error'* still remains, corresponding to the uncertainty related to the balise location itself. In ERTMS specifications, this error is referred to as the Q_LOCACC parameter, which is a fixed value (cf. Figure 3.a)).

As mentioned earlier in the paper, some ongoing research projects are investigating the possibility of replacing the physical balises with virtual balises [6]. Concretely, each of these VB corresponds to a reference position stored in the ETCS On-board module. By means of the GNSS-based localization unit, the on-board module launches the calculation of the train position in every interval where it expects to encounter a virtual balise; such interval is called *'expectation window'* in ERTMS specifications (cf. Figure 3.b)). Namely, when the traveled distance estimated on-board (including associated uncertainties) reaches the expectation interval, the ETCS on-board module continuously monitors whether the GNSS-based position matches the position of the VB. As soon as this matching occurs, the VB is *activated* (emulating the activation of a PB), and its position is used as a new reference position. Accordingly, a protection level (PL) (cf. Subsection C) is associated with the GNSS-based position at the time of the VB activation, and this PL serves as a *'residual error'* related to the location of VB.

It should be noticed that the value of the residual error in the case of PB is fixed and bounded by 5 meters, as required in the ERTMS specifications. In contrast, the residual error value related to VB activation is unknown and bounded by the PL, which may exceed 5 meters. Moreover, the PL may vary from one balise to another, and from one passage to

another, depending on several parameters mainly related to the operating environment. Consequently, as it is not possible to predict with certainty the PL value that shall be used for readjusting the train position estimated on-board, a new uncertainty factor arises. Therefore, a new variable must be accounted for when studying balise arrangements during the design phase of a railway line.

For the safe configuration of balises, the process proposed in the present paper allows for analyzing, globally on a line, how likely the train position error *'bound'* may exceed some predetermined threshold. In the following section, we will discuss the developed models involved in the performance/safety analysis.

B. DEVELOPMENT OF THE FORMAL MODELS

B.1) Behavioral models

Our aim through this modeling phase is to set rigorous models to describe the behavior of the localization function presented previously. In fact, we do not seek to model the position error at each time step. Instead, we focus our modeling process on the maximum tolerated interval that has to include the actual and estimated positions. This allows us to adopt a safety-oriented point of view. It is worth mentioning that this *'global uncertainty on the train position'* will be determined while considering the various sources of uncertainties.

These models will serve to check a number of properties on this function while considering various configurations. In this respect, our modeling process ensures modularity and parameterization so as the generated models can be updated to various settings. 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 actual behavior faithfully [53]. Hence, the modeling activity remains a crucial phase in these approaches and highly relies on the user expertise, both in terms of modeling and system comprehension [54], [55].

In our work, we mainly focus on the following features:

1) modelling the train dynamics as it moves. This allows the travelled distance to be updated according to a set of parameters.
2) modelling the evolution of the train position error bound, i.e., the continuous evolution of the maximal position error permitted according to the measured travelled distance.
3) modelling the activation of physical and virtual balises.
4) updating the error bound when a PB or a VB is encountered. Concretely, this induces a punctual down jump, in nominal conditions, of the error bound due to the resetting function, while the corresponding residual error is kept.

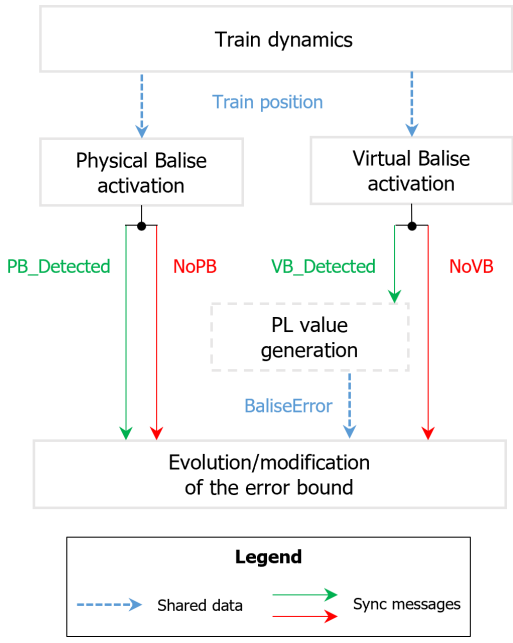


FIGURE 4. High-level view of the global model.

To meet the requirements of our modeling process as discussed above, we chose the *UPPAAL* model-checking[5] tool employed in several works mentioned in Subsection C. *UPPAAL* [56] allows for handling a network of parameterizable timed and probabilistic automata, hence making it possible to establish modular and configurable models. First, the behavioral *modules* in UPPAAL have to be established as a number of parameterizable timed automaton templates. Then, the actual behavioral model is generated as a product of timed automaton models instantiated from these template models. Moreover, the tool includes a number of model-checking algorithms that allow the evaluation of various types of properties expressed as temporal logic assertions. If some property is not satisfied on the model, a counter-example is generated showing a trace that violates the property, which offers a valuable feature for debugging. Finally, it is worth noting that UPPAAL also offers simulation facilities that can be advantageously used for both modeling and verification phases.

Figure 4 and Figure 5 show the main modules that have been developed to describe the behavior of the localization function. Besides these five modules, a module allowing the initialization of PB and VB location on the track, and another allowing the time to be elapsed have been developed. Figure 4 exhibits a high-level view of the global model with the shared data and the synchronization messages among the interacting modules, while Figure 5 exhibits four detailed automata along with the module variables and their role. The PL (Protection Level) module is not represented here as it

[5]Model-checking is a formal method that allows for automatically checking properties expressed as temporal logic formulas on state-transition models.

is related to random variable generation according to some stochastical distributions that depend on the surrounding environment encountered by the train (cf. Subsection IV.3), and due to the consideration of different classes of environment as explained in [10]. The main features of the four modules are described below; for a deeper insight into the modules, all the behavioral models are made available in a public GitHub repository with many technical details[6].

In the first module dedicated to translating the train dynamics, a variable is set to represent the value of the train acceleration. This variable allows us to represent the variation of the train speed due to acceleration and braking. From the acceleration, the instantaneous speed of the train can be easily deduced using the integral function. Likewise, the distance traveled by the train can be calculated from the velocity. This module is built in such a way as to be able to vary the speed according to the characteristics of the different track areas, and according to the maximum speed of the trains. The latter depends on the category of the trains to be considered and their load.

The distance variable in the first module serves as an input of the second module dedicated to the determination of the localization error bound. Namely, the value of this variable is used to model the acceptable error bound on the traveled distance. For that to happen, we consider the *OdoError_dyn* variable in the second module to model the odometry accumulated uncertainty. At each time step, the value of *OdoError_dyn* is incremented according to the traveled distance (while considering a rate of 5%) to represent the maximal odometry error bound as stated in the ERTMS specifications. In parallel to *OdoError_dyn*, the maximal residual error linked to the current reference position (i.e., the *balise activation uncertainty*) is also considered in our model and noted *BaliseError*. Hence, the global uncertainty on the *train position* can be represented as follows:

> *Global uncertainty on the train position* = *balise activation uncertainty* + 5% $\times$ *distance from the last reference position*

Using the model variables, it leads to: *PositionError* = *BaliseError* + *OdoError_dyn*.

In the third and fourth modules, we model the balise activation. In these modules, the actual relative train position, i.e., the real traveled distance modeled with variable P_int is taken as an input. This variable is only accessible because the train dynamics is modeled. In reality, the on-board system waits for the electromagnetic activation of PB or verifies if the GNSS-based estimated position (in distance) matches the VB position stored on-board. In the model, P_int is compared to the location of the next expected balise. When both values match, the position of the balise is retained as the new reference position. Thus, the value of uncertainty on the position is recalculated, keeping only the value related to the uncertainty at the detection time of the balise (max. 5 meters for PB and *PL* meters for VB).

B.2) Correctness and trustworthiness of the models

In order to ensure the model correctness and trustworthiness, various aspects have been considered all along the model development activities. For the sake of brevity, those aspects are outlined hereunder according to three global considerations, without discussing the technical details (formal properties, etc.), in order to keep the content of this part condensed. Yet, the reader can refer to our public Github repository where all the models are made available with relevant explanations:

Model construction process: A thorough analysis of the mechanisms related to the introduction and activation of virtual balises in the framework of GNSS-based railway localization systems has been conducted. Then, the appropriate abstraction level to establish the behavioral models has been identified. The underlying idea was to make a focus on the various artifacts that may impact the uncertainties on the estimated train position, while abstracting away the aspects which are irrelevant w.r.t. to the conducted analysis.

Correctness of the models: A number of features on the model, namely w.r.t the absence of *deadlock*, the *liveness* and the *non-Zenoness*, as well as the proper reachability of the model states, have been verified.

Model validation: Various model-testing and simulations have been conducted at each stage of the model development and refinement activities. To this aim, numerous *nominal* and *abnormal* scenarios have been executed, and the models have been fine-tuned in light of the obtained results.

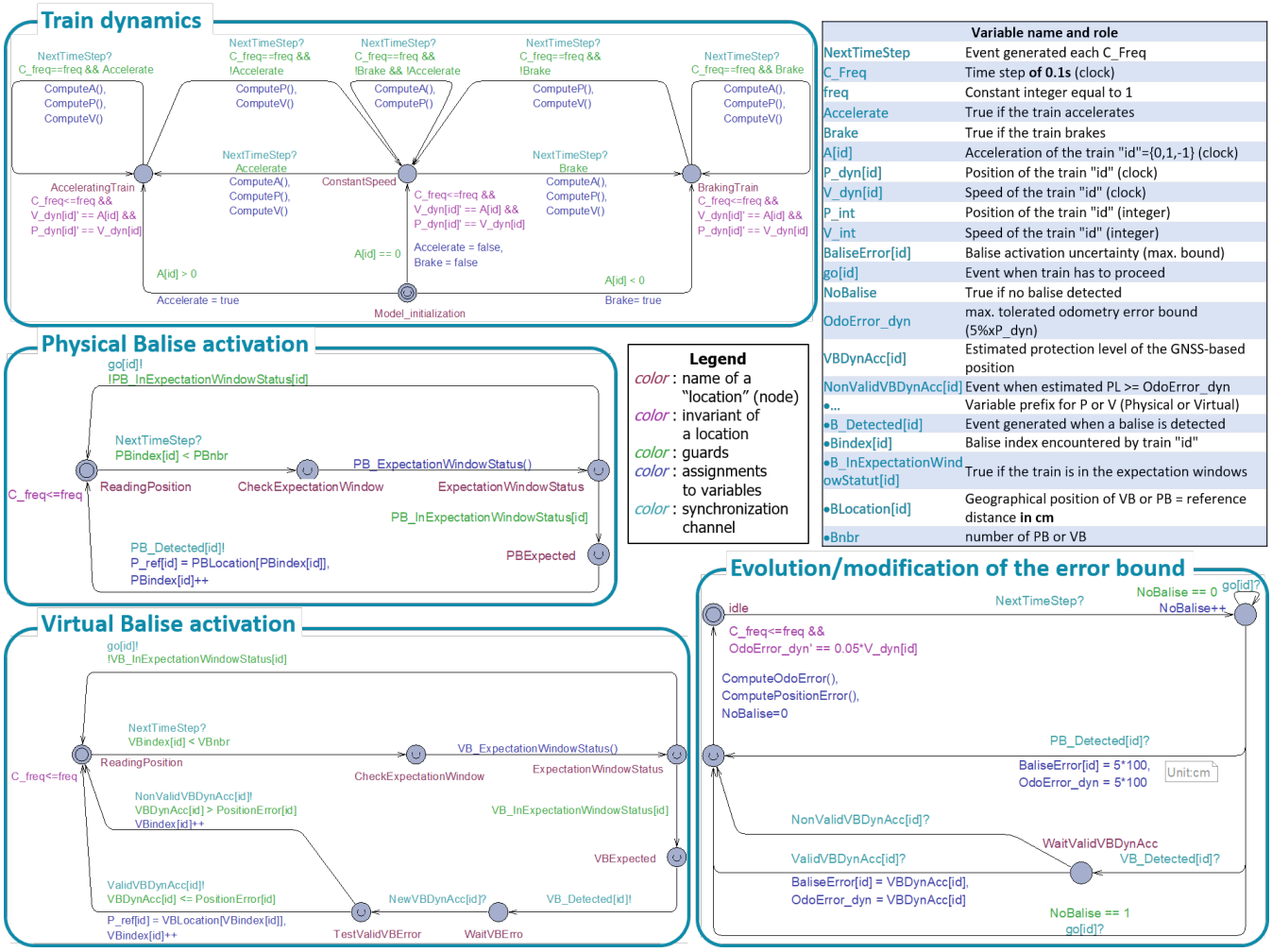
As discussed above, the various sources of uncertainties on the train position are considered in our models. In the following section, we explain how the various parameters that may impact the position error bound can be integrated in our model. The impact of these parameters in terms of performance and safety objectives will then be analyzed in Section V.

IV. MODEL PARAMETERIZATION

In order to investigate globally on a line, the uncertainty on the train position with the introduction of VB, the first step is to identify the factors that can influence this uncertainty. In particular, we mainly identify three relevant factors that impact the train position error:

1) The ratio between the number of PB and VB, as the use of VB introduces more uncertainties compared to PB.
2) The space distance separating consecutive balises, as this distance determines the odometry error accumulation.

[6] https://github.com/juliebeugin/ETCSL3Localization



Variable name and role	
NextTimeStep	Event generated each C_Freq
C_Freq	Time step **of 0.1s** (clock)
freq	Constant integer equal to 1
Accelerate	True if the train accelerates
Brake	True if the train brakes
A[id]	Acceleration of the train "id"={0,1,-1} (clock)
P_dyn[id]	Position of the train "id" (clock)
V_dyn[id]	Speed of the train "id" (clock)
P_int	Position of the train "id" (integer)
V_int	Speed of the train "id" (integer)
BaliseError[id]	Balise activation uncertainty (max. bound)
go[id]	Event when train has to proceed
NoBalise	True if no balise detected
OdoError_dyn	max. tolerated odometry error bound (5%xP_dyn)
VBDynAcc[id]	Estimated protection level of the GNSS-based position
NonValidVBDynAcc[id]	Event when estimated PL >= OdoError_dyn
•...	Variable prefix for P or V (Physical or Virtual)
•B_Detected[id]	Event generated when a balise is detected
•Bindex[id]	Balise index encountered by train "id"
•B_InExpectationWindowStatut[id]	True if the train is in the expectation windows
•BLocation[id]	Geographical position of VB or PB = reference distance **in cm**
•Bnbr	number of PB or VB

FIGURE 5. Modeling modules of the localization function [11].

3) The PL associated with each VB, since PL is used to reset the position uncertainty.

Figure 6 presents the parameters that serve for expressing the aforementioned influencing factors in the models described in Subsection B. The associated UPPAAL variables are detailed below. Note that the parameters pertaining to the train dynamics (i.e., traction and braking characteristics) are also represented as they influence the global behavior.

1) PB / VB configuration

Regarding the number of VB and PB, one can logically admit that an infinite number of combinations is possible. For the sake of simplicity, we choose to adopt regular configurations (e.g. 1PB-2VB, 1PB-3VB, etc.). Should a particular line balises layout needs to be analyzed, more specific configurations can easily be considered.

2) Inter-balise distance

As for the space separating consecutive balises, a variable distance d is used to set the different balise locations.

3) Protection Level (PL)

The reset resulting from the detection of a VB is performed using PL. Therefore, the PL evolution and its associated parameters must be integrated in our behavioral model. Namely, we implement an UPPAAL module whose objective is to generate the PL values depending on different environmental classes which, in turn, represent the quality of the GNSS signal reception (cf. Figure 6). The values of this variable are generated according to some predefined probabilistic distributions, one distribution being defined for each environmental class. It should be noticed that the generation of PL values is *"memoryless"*. In other terms, these values are solely dependent on the active PL distribution related to the activated VB, independently of the previous balises encountered. It is worth noticing that characterizing the uncertainty on the PL values according to the surrounding environment is a topical issue of the scientific community specialized in GNSS-based localization. Among other means, field experiments and existing databases are used. In fact, presenting how the quality of the GNSS reception can be characterized would require long discussions, and cannot be done in the present paper as it

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

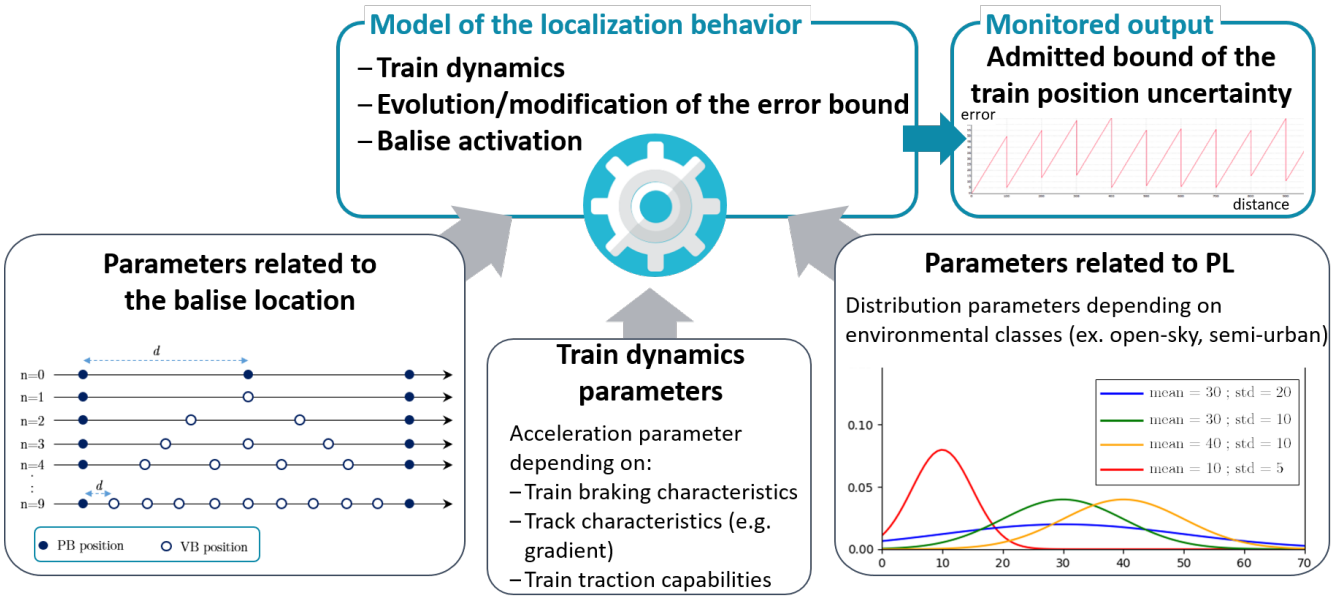


FIGURE 6. **Identified parameters affecting the train position uncertainty [11].**

is out of the scope of our contribution. Yet, the reader can refer to the survey in [57] where some research works in the literature, which are relevant to this topic are presented. In the sequel of this paper, some distributions are chosen only for the sake of illustrating our approach. Nevertheless, different distributions can easily be considered by simply adapting the model variables (e.g. type of distribution, mean value, standard deviation), since a placeholder is present in the model. This offers the possibility to refine the PL-related probabilistic distributions according to the inputs coming from ongoing research projects. We also assume that the algorithms developed by GNSS practitioners to calculate the PL values are correct, i.e. the determined value of PL always bounds the position error for the different considered operational contexts with a guaranteed localization integrity risk (cf. Subsection B). To sum up, in our model, the PL value is represented by a random variable which directly depends on some predefined environmental classes.

For the sake of clarity and in order to generate the PL values, in the next section we assume that the environmental conditions are roughly the same all along the train run. Thus, one single probabilistic distribution (here, a normal distribution with positive values) is used to generate the PL values for the different VB locations.

V. VERIFICATION PHASE

The developed models allow us to emulate the behavior of the train localization when a train runs on a railway line involving some given configuration of PB and VB. Moreover, the models implement the various uncertainty aspects pertaining to the train position. In the present section, we will show how various safety and performance properties can be checked based on our model. Namely, we will take advantage of the Statistical Model-Checking (SMC) facilities of UPPAAL to check a number of features while considering specific operational scenarios.

A. VERIFICATION PRINCIPLE

Unlike classic Model-Checking (MC), which issues a binary result (whether the property is satisfied or not), SMC provides a quantitative result, namely how likely (probability value) the examined property is satisfied by the model. Furthermore, the generated result is associated with a confidence interval. The SMC algorithm is, in fact, based on the classical Monte Carlo simulation, *i.e.*, using sampling. Therefore, while the outcomes issued by SMC algorithms offer a probabilistic characterization of some investigated property, they are well considered as a formal technique in the sense that they provide a quantification of the likelihood associated with the fulfillment of such a property, as well as the certainty/uncertainty associated with the issued result. Such a qualification of the SMC outcome provides a valuable characterization in terms of the confidence that one shall associate with the obtained result. Besides, it is worth noting that SMC algorithms are well adopted in the verification of safety critical applications in diverse domains, as highlighted in the survey conducted in [58].

In what follows, we will mainly analyze how likely the uncertainty on the train position can exceed a certain threshold during the whole run of the train along some given lines while considering specific PB/VB arrangement. This property has to be expressed as a temporal logic formula to be analyzed by the model-checker. The aforementioned feature can be formulated as follows:

$$Pr\,[<= bound\,]\,(<>\,PositionError > threshold) \quad (1)$$

where:

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

To evaluate different error limits, it is sufficient to adapt the threshold value in the previous formula. Hence, for each generated query (representing a different threshold), the SMC tool executes an important number of runs on the system model to explore the reachable states. At the end of each run, the algorithm checks whether or not the query is satisfied. This is, in fact, analogous to a Bernoulli problem with a set of logical answers (true or false). The obtained outcomes are then aggregated to quantitatively estimate the probability of the property being satisfied (with a corresponding confidence interval). Namely, the 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.

B. THE CONSIDERED CASE STUDY

As mentioned in Subsection A, using VB to implement the train localization function under ETCS L3 can be envisaged in two main situations:

1) The case of a new ERTMS L3 railway line,
2) The upgrade of an existing line (e.g. operated in ERTMS L2) towards ERTMS L3.

In both situations, performance and safety targets have to be evaluated. In our case study, we will consider Case 1), i.e. the design of a new ERTMS L3 line to be operated with FVB.

From an operational point of view, the pursued objective is that the new ERTMS L3 line should provide at least the same capacity that would have been obtained under ERTMS L2 operation (with PB exclusively). Obviously, a direct benefit of ERTMS L3 over ERTMS L2 is that fewer PB shall be deployed, since the used balises will be mostly virtual.

In this context, we assume that the configuration of the ERTMS L2 line used as a comparison basis can be summarized as follows:

- Only physical balises are used for odometry calibration,
- All the PB are equivalently spaced on the track, and the distance separating two successive (group of) balises is $d = 2000\ m$.

Such an ERTMS L2 line configuration implies that the global train position uncertainty varies between $5\ m$ (immediately following the activation of a PB) and $105\ m$ ($5{+}5\%{\cdot}d$ with $d = 2000\ m$, right prior to the activation of a PB).

We recall that the capacity of the ERTMS L2 line depends on three main parameters: the maximum uncertainty value on the train position, the braking distance of the trains, and the length of the blocks. Since the braking characteristics of the operated trains remain unchanged, only the uncertainty on train position and the distance separating balises determine the variation in terms of line capacity between the L2 reference line and the L3-FVB line. Accordingly, in our case study we will mainly focus on the maximum error bound on train position and the block length as comparative parameters. In fact, on the one hand, the block length can be directly compared, namely according to the distance separating two successive (group of) balises. On the other hand, the maximum train position uncertainty needs to be analyzed in order to check if the bound (i.e., $105\ m$) remains satisfied (with a tolerable confidence level) in the new ERTMS L3 line, while using VB.

Through our case study, we seek to illustrate how to safely address the position uncertainties under FVB operation by means of formal verification using the developed models. Considering the same speed, constant acceleration, and the same dynamic characteristics for all trains in our case study, the model managing the variation of each train dynamics parameter is not considered here; this model has already been investigated in [11]. Thus, in the present paper we concentrate the analysis on the PL characterization related to VB activation. Besides, the cumulative error due to the traveled distance can be regarded as a constant when considering the same size for each block section; this can be the case for a new ERTMS L3 line operated with FVB, ERTMS L2 lines being not necessarily equipped with block sections sized identically. Therefore, the model part related to the PL characterization will be analyzed in the sequel. Using 3 possible settings related to the PL distribution, the impact on train position uncertainty will be particularly investigated. Namely, we will address the following question: *"How should the balises be arranged on the line in order to guarantee that the uncertainty on the train estimated position does not exceed a predetermined threshold?"*. It is worth highlighting that the aforementioned investigated issue is given here for the sake of illustrating how safety analyses can be conducted on the basis of our formal models; in general, further analyses can be undertaken. Depending on the investigated problem, the development of additional behavioral modules can be required, yet the whole approach remains the same.

C. ANALYSIS PHASE

As explained earlier in the paper, 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 are generated automatically by means of Python scripts we have developed. Indeed,

This article has been accepted for publication in IEEE Open Journal of Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/OJITS.2023.3267142

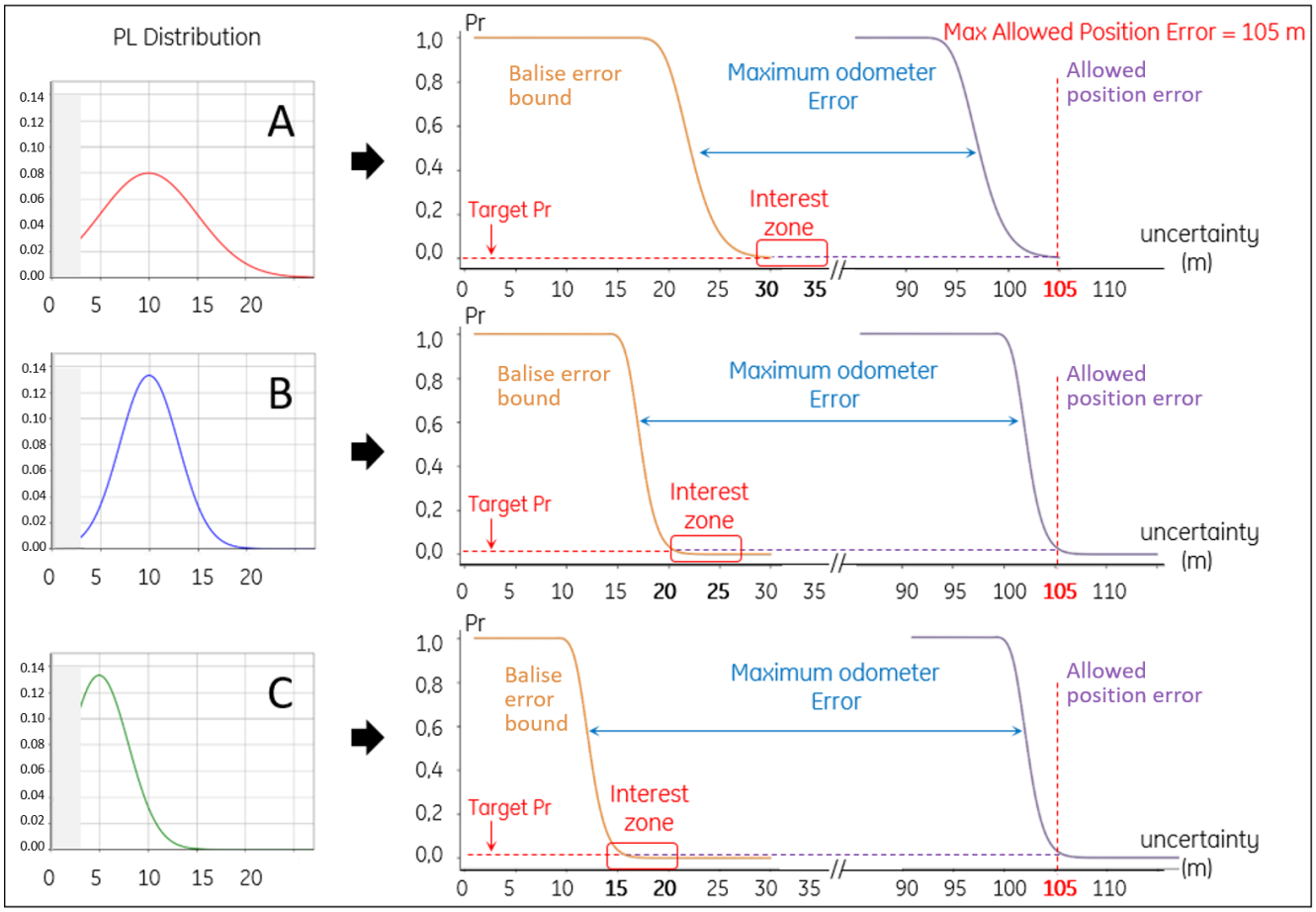


FIGURE 7. **SMC Results on the Balise activation error bound following the PL characterization models A,B, and C.**

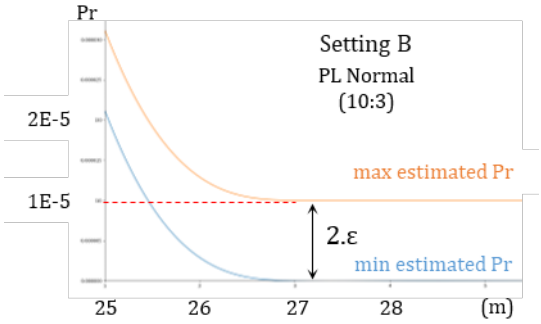


FIGURE 8. **Zone of interest with PL:** $Normal(10:3)$, $\alpha = 1E{-}5$ **and** $\epsilon = 5E{-}6$.

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. These aspects are further discussed in the explanations provided with our models in the public repository.

In the analyzed ERTMS L3-related case study, we choose to employ only $10\ \%$ of PB for illustrating how the probabilistic distributions related to different GNSS signal reception environments can vary in our models while maintaining an accepted system residual risk. Accordingly, the balises configuration of *(1PB - 9VB)* is adopted in the remainder of our study. This means one (group of) PB while the 9 next successive balises are virtual (VB), etc.

As stated before, for the sake of clarity, we assume that the operational environment is invariable in one scenario, in terms of GNSS reception quality, all along the considered line. Hence, the same probabilistic distribution is used to characterize the PL values in each scenario. Namely, we aim to study the impact of three illustrative normal distributions on the VB separation distance (cf. Table 1).

Note here that, for the sake of obtaining realistic PL values, we define a minimum acceptable PL value equal to $3\ m$ for each distribution. Hence, if the generated PL value is smaller than this bound, a new value is generated until

TABLE 1. Parameters related to PL

PL Distribution	Mean (in meters)	Standard deviation (in meters)
A	10	5
B	10	3
C	5	3

obtaining an accepted PL value. Such a minimum setting can be adapted to represent different PL distributions.

We recall that the results sought via our analysis intend to provide indicators regarding the physical and virtual balises *safe configuration* along the new line. In this context, we assume the distance separating successive balises (denoted as d') to be constant. Moreover, since the *OdoError_dyn* variable (i.e., the odometer accumulated error) component of the *PositionError* variable (i.e. the allowed train position error) only depends on the traveled distance from the last balise (which can be either a PB or VB), one can easily infer the maximum value of *OdoError_dyn* from d'. In contrast, the *BaliseError* variable (resulting from the activation of a VB) depends on the various PL values and represents the uncertain part of the *PositionError* variable. Hence, such a variation needs to be finely investigated. This can be done by adapting and formally checking the property expressed in formula (1).

For each threshold value (e.g., from 1 to 35 meters), the SMC algorithm handles the associated query and estimates the probability that the *BaliseError* variable exceeds the investigated threshold. The obtained results are processed to obtain the charts represented in Figure 7. The results pertaining to the *maximum balise error* are depicted via the orange plots, which show the relation between the various error thresholds and the probability that these limits are exceeded by the balises activation error bound.

D. RESULTS INTERPRETATION

We recall that, in contrast with the case of PB where the fixed value of $5\ m$ bounds the value of the *BaliseError* variable, no maximum value is defined for the PL associated with the activation of a VB. Indeed, large PL values can be reached, especially in unfavorable GNSS reception conditions. Instead, an *Alert Limit* (*AL*) is used as an upper bound on the accepted PL values. If the estimated PL is lower than the value of AL, the PL value is accepted and associated with a *'confidence level'*. On the contrary, if the estimated PL exceeds AL, the GNSS position is deemed unavailable and, hence, rejected by the on-board system.

In our context, we consider this *'target confidence level'* as an input parameter to our analysis. In fact, such probabilistic threshold stands for an accepted residual risk (according to the safety targets). For instance, let us assume that the risk of PL exceeding the balise error bound must be smaller than 10^{-5} with a confidence of 0.99999. Considering this target probability (i.e., 10^{-5}), particular zones of interest (i.e., uncertainty value corresponding to the target probability) are identified according to the results obtained previously. These zones (illustrated with red boxes in Figure 7) require an in-depth exploration. Accordingly, the SMC tool parameters are further adapted as follows: $\alpha = 1 - 0.99999$ and $2 \times \epsilon = 10^{-5}$).

For instance, the interest zone corresponding to the setting of the parameters related to a PL distribution $Normal(10:3)$ (Setting B) is zoomed in and presented in Figure 8. The other PL distributions are addressed similarly.

Having obtained the *BaliseError* values associated with the investigated PL distributions, the second part of the study focuses on the *Global train position uncertainty*, as this parameter is key for determining the maximum distance between consecutive balises, and accordingly the size of the FVB. To do so, let us consider the following: *MaxAllowedError* = *MaxOdoError_dyn* + *BaliseError*, where:

- *MaxAllowedError* denotes the target bound on the train position uncertainty (i.e., $105m$),
- *MaxOdoError_dyn* = $5\% \times d'_{max}$,
- d'_{max} : maximum allowed distance between consecutive balises.

Therefore, it is straightforward to infer d'_{max} as in relation (2) below, and the obtained results are reported in Table 2, where all distances are indicated in meters (m):

$$d'_{max} = \frac{1}{5\%} \times (MaxAllowedError - BaliseError) \quad (2)$$

TABLE 2. Results

PL distribution (*mean* (m) : *std* (m))	*BaliseError* (m)	d'_{max} (m)	PB ratio L2 vs. L3
Setting A (10:5)	37	1360	14.7 %
Setting B (10:3)	27	1560	12.8 %
Setting C (5:3)	22.5	1650	12 %

In the last column of the table, we compare the number of PB needed in the new L3 FVB line respectively to their number in the reference ERTMS L2 line. One can notice that the number of PB is reduced by more than 85% in the three investigated scenarios. Indeed, even if the balises are closer to each other in the new line, only one out of ten balises is a physical balise. One can also notice that the lower the uncertainty on the value of PL is, 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 depend highly on the PL distributions adopted as input parameters.

Moreover, since the FVB lengths (d'_{max}) are smaller than the block length of the reference ERTMS L2 line $(2\ km)$, the line capacity shall be increased. Besides, it should be noted that such d'_{max} values stand for the *maximum* distance separating successive balises. Hence, the actual

balises separation distance to be adopted can be smaller than the calculated d'_{max} value. In particular, the increase of the balises number is particularly relevant since 90% of the balises are virtual. As a result, less odometry error accumulation and even shorter FVB can be obtained, thus making it possible for further increasing the line capacity. 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.

E. DISCUSSION ON OPERATIONAL ENGINEERING RULES

For the sake of the transferability of our approach, this subsection is dedicated to discussing the implication of the obtained results, as well as the limitations of the analysis in the context of future research and innovation projects. Indeed, beyond the methodological aspects, some operational questions can arise when employing the proposed approach, as will be discussed in what follows.

Regarding the balise location along the track, we adopted the following generic rule: we assume that there is one balise (physical or virtual) by block section and balises are placed at the beginning of each block. Indeed, there is no standard regarding installation engineering rules for balises, and no guidelines regarding these aspects can be found in the scientific or technical literature. Also, based on some discussions with railway experts, we could infer that balises were today placed in a very heterogeneous way. The location of balises can be chosen for historical reasons related to the line, for topographical reasons, due to possible interference with other balises or conductive materials in the vicinity, or also for some maintenance considerations often related to the inspection of other trackside equipment in parallel. Indeed, for practical purposes, it is better to regroup all equipment in an easily accessible area where all devices can be inspected without moving monitoring/repair apparatuses from one place to another. Moreover, "beaconage plans" do exist especially in the case of new lines, but they are naturally not shared for security reasons and are the properties of the suppliers and the organization that operates the railway line. Therefore, they cannot be analyzed to infer some generic engineering rules.

Nowadays, requirements on physical balises exist in ETCS [59], and are referred to as FFFIS (Form-Fit Functional Interface Specification), which are concretely technical requirements on the balises. These specifications include the following installation requirement types for such devices: tolerances for balise installation and mounting on the track, balise installation in narrow curves, the distance between consecutive balises in a Balise Group (BG), the grouped data of balises in a BG providing the reference position to the train. However, it can be noticed that they only refer to local installation rules and not to global rules related to a line, and operating performances are not considered. The contribution discussed in the present paper therefore ambitions to help provide a practical answer to this global aspect.

Besides, considering Virtual Balises (VB), allows some local physical installation constraints to be overlooked. However, it should be noted that the use of GNSS technologies for ensuring the train localization function based on VB induces some other considerations of VB placing, i.e. they have to be found in locations where GNSS signal reception conditions are optimal or, at least, associated with well-controlled error models. These optimal places have to be determined based on tests and analyses that do need to be performed with the help of GNSS experts. Consequently, a VB can be placed further in a block section rather than at its beginning.

VI. CONCLUSION AND PERSPECTIVES

Satellite technologies are considered as a strategic facility in the rise of advanced railway CCS, particularly ERTMS. Bringing into play GNSS-based solutions to fulfill the railway localization function would lead to a significant breakthrough in terms of railway operation and asset management. In fact, allowing the train localization to be realized onboard rather than by means of trackside equipment, GNSS-based positioning systems enable reducing the equipment along the track with direct savings in terms of infrastructure installation and maintenance costs. Moreover, a substantial capacity gain is expected since efficient operation modes can be implemented, such as FMB, FVB, or virtual coupling [60], [61]. Besides, 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.

In this paper, we address the safety of the train localization function relying on Virtual Balises as a substitute for physical ones. In particular, a special focus is made on the analysis of the position uncertainty sources related to VB detection. The analysis approach is based on formal models that were elaborated to mimic the behavior of the localization function. These models rely on the rigor and expressiveness of automata-based formalisms and are modular and configurable, making it possible to address a variety of railway line configurations. Thus, the process intends to assist and guide the railway signaling practitioners for the safe configuration of virtual balises on a railway track. To implement the approach, a case study is considered in this paper and addresses the layout of virtual and physical balises along a new ERTMS L3 line operating according to the FVB principle. Specific parameter settings used in the VB detection process are investigated while fixing other identified parameters in order to illustrate our approach. However, adapting the model-oriented approach to cope with real line characteristics is fairly easy, making the proposed formal models highly re-usable.

In fact, the present contribution falls within the general context of *i)* reducing the costly and time-consuming railway on-site tests, and *ii)* adopting highly recommended formal models and approaches for safety studies, as stated in EN 50128 railway safety standard. Our aim is to bring model-based approaches and formal verification techniques into play, to evaluate safety and performance properties related to the use of GNSS-based train positioning solutions. The outcomes of such analysis can be advantageously used by railway experts in both the engineering and safety demonstration phases.

In the present work, we mainly focused on the uncertainties related to the 'protection level' of the GNSS-based system in order to provide at least the same capacity that would have been obtained under ERTMS L2 operation, by using formal verification methods that are highly recommended in safety analyses. In future works, we intend to consider specific hazardous scenarios that can arise, such as the train collisions, by considering the localization 'integrity risk' related to a given GNSS-based system. 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. Finally, it should be noted that 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. Moreover, we are currently extending our models to tackle various scenarios involving several trains, while considering the case of operation under full moving block. In future work, we intend to develop further extension to tackle the case of operation under virtual coupling.

ACKNOWLEDGMENT

This research has received funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation program under Grant Agreement N. 101015416 (PERFORMINGRAIL). The JU receives support from the European Union's Horizon 2020 research and innovation program and the Shift2Rail JU members other than the Union.

The information and views set out in this document are those of the authors and do not necessarily reflect the official opinion of Shift2Rail JU. The JU does not guarantee the accuracy of the data included in this article. Neither the JU nor any person acting on the JU's behalf may be held responsible for the use which may be made of the information contained therein.

REFERENCES

[1] P. Griffe, "Automation will Enhance Quality and Security of Meteor 14th Line of Paris Metro," in *IFAC Transportation Systems, 30(8): 1163–1168*, Chania, Greece, 1997.

[2] J.-L. Boulanger and M. Gallardo, "Validation and verification of METEOR safety software," in *VIIth International Conference on Computers in Railways*, Bologna, Italy, 2000, Sept.

[3] J. Pachl, *Railway Operation and Control (4th ed.)*. Mountlake Terrace, USA: VTD Rail Publishing, 2018.

[4] M. Ghazel, "Formalizing a subset of ERTMS/ETCS specifications for verification purposes," *Transportation Research Part C: Emerging Technologies*, vol. 42, pp. 60–75, 2014.

[5] N. Furness, H. Van Houten, L. Arenas, and M. Bartholomeus, "ERTMS Level 3: the Game-Changer," *IRSE–Institute of Railway Signal Engineers*, pp. 2–9, 2017, April.

[6] F. Rispoli, G. Siciliano, and C. Brenna, "GNSS for ERTMS train localization, a step-change technology and new business model," *Inside GNSS*, pp. 48–54, 2017.

[7] Shift2Rail, IP2 projects (Innovation Programme): https://shift2rail.org/research-development/ip2, Accessed on 2022/09/01.

[8] J. Marais, J. Beugin, and M. Berbineau, "A Survey of GNSS-Based Research and Developments for the European Railway Signaling," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2602–2618, 2017.

[9] TSI CCS (EU) 2016/919 regulation, *Technical Specification for Interoperability relating to the 'Control-Command and Signalling' subsystems of the rail system in the European Union*. European Commission regulation, 2016, 27th May.

[10] O. Himrane, J. Beugin, and M. Ghazel, "Towards a model-based safety assessment of railway operation using GNSS localization," in *ESREL 2020 and PSAM 15, 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, Venice, Italy, 2020, Nov.

[11] ——, "Toward formal safety and performance evaluation of GNSS-based railway localisation function," in *CTS 2021, 16th IFAC Symposium on Control in Transportation Systems*, Lille, France, 2021, June.

[12] EEIG-EUG, *Hybrid ERTMS/ETCS Level 3*. European Economic Interest Grouping - ERTMS Users' Group, reference 16E042, version 1D, 2020.

[13] Deutsche Bahn, "Demonstration der ETCS Level 3 Technologie im Living Lab der DB Netz," https://www.youtube.com/watch?v=FjKnugbmrP4 - German and English languages, Accessed 2022-09-01, 2018, Sept.

[14] D. Hansen, M. Leuschel, P. Körner, S. Krings, T. Naulin, N. Nayeri, D. Schneider, and F. Showron, "Validation and real-life demonstration of ETCS hybrid level 3 principles using a formal B model," *International Journal of Software Tools for Technology Transfer*, vol. 22, pp. 315–332, 2020.

[15] Subset 088, *ETCS Application Levels 1 and 2 - Safety Analysis*. UNISIG, Union Industry of Signalling, issue 3.6.0, 2016-06-20, 2016.

[16] C. Legrand, J. Beugin, J. Marais, B. Conrard, E.-M. El-Koursi, and M. Berbineau, "From extended integrity monitoring to the safety evaluation of satellite-based localisation system," *Reliability Engineering and System Safety*, vol. 155, pp. 105–114, 2016.

[17] N. Kubo, M. Higuchi, T. Takasu, and H. Yamamoto, "Performance evaluation of GNSS-based railway applications," in *International Association of Institutes of Navigation World Congress (IAIN)*, Prague, Czech Republic, 2015, Oct.

[18] ICAO, *International Standards and Recommended Practices, Annex 10 to the Convention on International Civil Aviation, Volume 1: Radio Navigation Aids (7th ed.)*. International Civil Aviation Organization, 2018, July.

[19] J. Marais, J. Beugin, F. Rispoli, P. Gurnik, and A. B. Toma, *State of the art of EGNSS projects for the rail application*. Delivrable 5.1 of the STARS project - Satellite Technology for Advanced Railway Signalling, H2020 European programme, 2017.

[20] A. Filip, S. Sabina, and F. Rispoli, "A framework for certification of train location determination system based on GNSS for

ERTMS/ETCS," *Journal of Transport Development and Integration*, vol. 2, no. 3, pp. 284–297, 2018.

[21] A. Filip, F. Rispoli, and R. Capua, "A safety regulatory framework for certification and authorization process of selfdriving cars: Experience from european railways," in *ESREL 2020 and PSAM 15 - 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, Venice, Italy, 2020, Nov.

[22] C. Wullems, F. Sperandio, M. Basso, S. Sturaro, and S. Sabina, "A Preliminary Apportionment of Safety Targets for Virtual Balise Detection using GNSS in Future Evolutions of ERTMS." in *16th International Conference on Intelligent Transportation Systems Telecommunications (ITST)*, Lisboa, Portugal, 2018, Oct.

[23] D. Lu, D. Tang, and D. Spiegel, "Hazard Rate Estimation for GNSS-Based Train Localization Using Model-Based Approach," *Chinese Journal of Electronics*, vol. 29, no. 1, 2020.

[24] T. P. K. Nguyen, J. Beugin, and J. Marais, "Method for evaluating an extended fault tree to analyse the dependability of complex systems: Application to a satellite-based railway system," *Reliability Engineering and System Safety*, vol. 133, pp. 300–313, 2015.

[25] J. Beugin, C. Legrand, J. Marais, M. Berbineau, and E.-M. El-Koursi, "Safety appraisal of GNSS-based localization systems used in train spacing control," *IEEE Access*, vol. 6, pp. 9898–9916, 2018.

[26] J. Goya, G. De Miguel, S. Arrizabalaga, L. Zamora-Cadenas, I. Adin, and J. Mendizabal, "Methodology and Key Performance Indicators (KPIs) for Railway On-Board Positioning Systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 4035–4042, 2018.

[27] D. Lu and E. Schnieder, "Performance evaluation of GNSS for train localization," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 1054–1059, 2015.

[28] J. Beugin and J. Marais, "Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization," *Transportation Research Part C (Emerging Technologies)*, vol. 22, pp. 42–57, 2012.

[29] D. Basile, M. H. Ter Beek, A. Fantechi, S. Gnesi, F. Mazzanti, A. Piattino, D. Trentini, and A. Ferrari, "On the industrial uptake of formal methods in the railway domain: a survey with stakeholders," in *14th IFM 2018, International Conference on Integrated Formal Methods*, Maynooth, Ireland, 2018, Sept.

[30] M. H. Ter Beek, A. Borälv, A. Fantechi, A. Ferrari, S. Gnesi, C. Löfving, and F. Mazzanti, "Adopting formal methods in an industrial setting: The railways case," in *3rd FM 2019, Formal Methods-The Next 30 Years*, Porto, Portugal, 2019, Oct.

[31] M. H. Ter Beek, S. Gnesi, and A. Knapp, "Formal methods for transport systems," *International Journal on Software Tools for Technology Transfer*, vol. 20, no. 3, pp. 237–241, 2018.

[32] J.-L. Boulanger, *Formal methods applied to complex systems: Implementation of the B method*. Hoboken, NJ, USA: Computer Engineering Series, Wiley, 2014.

[33] A. Fantechi, W. Fokkink, and A. Morzenti, *Chapter 4: Some Trends in Formal Methods Applications to Railway Signaling*. Wiley-IEEE Computer Society, 2012, pp. 61–84.

[34] A. Fantechi, "Twenty-five years of formal methods and railways: What next?" in *SEFM 2013, International Conference on Software Engineering and Formal Methods*, Madrid, Spain, 2014, Sept.

[35] A. Fantechi, A. Ferrari, and S. Gnesi, "Formal methods and safety certification: Challenges in the railways domain," in *7th ISoLA 2016, Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications*, Corfu, Greece, 2016, Oct.

[36] A. Ferrari, A. Fantechi, S. Gnesi, and G. Magnani, "Model-based development and formal methods in the railway industry," *IEEE Software*, vol. 30, no. 3, pp. 28–34, 2013.

[37] A. Ferrari, F. Mazzanti, D. Basile, M. H. Ter Beek, and A. Fantechi, "Comparing formal tools for system design: a judgment study," in *ICSE'20: IEEE/ACM 42nd International Conference on Software Engineering, Association for Computing Machinery*, Seoul, South Korea, 2020.

[38] F. Mazzanti and A. Ferrari, "Ten diverse formal models for a CBTC automatic train supervision system," *Electronic Proceedings in Theoretical Computer Science*, vol. 268, pp. 104–149, 2018.

[39] F. Mazzanti, A. Ferrari, and G. O. Spagnolo, "Towards formal methods diversity in railways: an experience report with seven frameworks," *Journal on Software Tools for Technology Transfer*, vol. 20, no. 3, pp. 263–288, 2018.

[40] A. Baouya, O. Ait Mohamed, D. Bennouar, and S. Ouchani, "Safety analysis of train control system based on model-driven design methodology," *Computers in Industry*, vol. 105, pp. 1–16, 2019.

[41] A. Ferrari, M. H. Ter Beek, F. Mazzanti, D. Basile, A. Fantechi, S. Gnesi, A. Piattino, and D. Trentini, "Survey on formal methods and tools in railways: The ASTRail approach," in *RSSRail 2019: International Conference on Reliability, Safety, and Security of Railway Systems*, Lille, France, 2019, June.

[42] A. Ferrari and M. H. Ter Beek, *Formal Methods in Railways: a Systematic Mapping Study*. ACM Computing Surveys, 2022.

[43] Q. Cappart, C. Limbrée, P. Schaus, J. Quilbeuf, L.-M. Traonouez, and A. Legay, "Verification of interlocking systems using statistical model checking," in *IEEE 18th International Symposium on High Assurance Systems Engineering (HASE)*, Singapore, 2017.

[44] P. L. Laursen, V. Trinh, and A. E. Haxthausen, "Formal modelling and verification of a distributed railway interlocking system using UPPAAL." in *ISoLA 2020, 9th International Conference on Leveraging Applications of Formal Methods, Verification and Validation: Applications, Lecture Notes in Computer Science, 12478*, Rhodes, Greece, 2020, Oct.

[45] A. E. Haxthausen and K. Hede, "Formal verification of railway timetables - using the UPPAAL model checker," *From Software Engineering to Formal Methods and Tools, and Back: Essays Dedicated to Stefania Gnesi on the Occasion of Her 65th Birthday*, pp. 433–448, 2019.

[46] D. Basile, M. H. Ter Beek, and A. Legay, "Strategy synthesis for autonomous driving in a moving block railway system with UPPAAL Stratego," in *FORTE 2020, 40th International Conference on Formal Techniques for Distributed Objects, Components, and Systems, Lecture Notes in Computer Science, 12136*, Valletta, Malta, 2020, June.

[47] D. Basile, M. H. Ter Beek, and V. Ciancia, "On the industrial uptake of formal methods in the railway domain: a survey with stakeholders," in *ISoLA 2018, 8th International Conference on the Leveraging Applications of Formal Methods, Verification and Validation: Verification, Lecture Notes in Computer Science, 11245*, Limassol, Cyprus, 2018, Nov.

[48] D. Basile, M. H. Ter Beek, A. Ferrari, and A. Legay, "Modelling and analysing ERTMS L3 moving block railway signalling with Simulink and UPPAAL SMC," in *FMICS 2019, 24th International Conference on Formal Methods for Industrial Critical Systems, Lecture Notes in Computer Science, 11687*, Amsterdam, The Netherlands, 2019, Aug.

[49] ——, "Exploring the ERTMS/ETCS full moving block specification: an experience with formal methods," *International Journal on Software Tools for Technology Transfer*, vol. 24, pp. 351–370, 2022.

[50] D. Basile, A. Fantechi, L. Rucher, and G. Mandò, "Analysing an autonomous tramway positioning system with the UPPAAL statistical model checker," *Formal Aspects of Computing*, vol. 33, pp. 957–987, 2021.

[51] Subset 041, *Performance Requirements for Interoperability*. UNISIG, Union Industry of Signalling, issue 3.2.0, 2015-12-17, 2015.

[52] L. Lo Presti and S. Sabina, *GNSS for rail transportation, challenges and opportunities*. PoliTO Springer Series, 2018.

[53] M. Ghazel and E.-M. El-Koursi, "Two-half-barrier level crossings versus four-half-barrier level crossings: A comparative risk analysis study," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 3, pp. 1123–1133, 2014.

[54] P. Arcaini, J. Kofroň, and P. Ježek, "Validation of the hybrid ERTMS/ETCS level 3 using SPIN," *International Journal on Software Tools for Technology Transfer*, vol. 22, pp. 265–279, 2020.

[55] S. Fotso, M. Frappier, R. Laleau, and A. Mammar, "Modeling the hybrid ERTMS/ETCS level 3 standard using a formal requirements engineering approach," *International Journal on Software Tools for Technology Transfer*, vol. 22, pp. 349–363, 2020.

[56] A. David, K. G. Larsen, A. Legay, M. Mikučionis, and D. Bøgsted Poulsen, "UPPAAL SMC tutorial," in *Technical report of Aalborg University, Denmark, and INRIA/IRISA lab in Rennes, France*, 2018.

[57] N. Zhu, J. Marais, D. Bétaille, and M. Berbineau, "GNSS position integrity in urban environments: a review of literature," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 9, pp. 2762–2778, 2018.

[58] A. Legay, B. Delahaye, and S. Bensalem, "Statistical model checking: An overview," in *First International Conference RV 201, Runtime Verification*, St Julians, Malta, 2010, Nov.
[59] Subset 036, *FFFIS for Eurobalise*. Form-Fit Functional Interface Specification of UNISIG, Union Industry of Signalling, issue 3.1.0, 2015-12-17, 2015.
[60] C. Di Meo, M. Di Vaio, F. Flammini, R. Nardone, S. Santini, and V. Vittorini, "ERTMS/ETCS Virtual Coupling: Proof of concept and numerical analysis," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 6, pp. 2545–2556, 2020.
[61] J. Xun, Y. Li, R. Liu, Y. Li, and Y. Liu, "A survey on control methods for virtual coupling in railway operation," *IEEE Open Journal of Intelligent Transportation Systems*, vol. 3, pp. 838–855, 2022.

OUAIL HIMRANE graduated as an engineer in Industrial Risk Management from the National Polytechnic School of Algiers, Algeria, in 2017. He continued his education at the École Normale Supérieure Paris-Saclay in France, where he earned a M.S. degree in Complex Systems Engineering with a focus on Critical Systems Conception and Control, in 2018. He then joined the ESTAS laboratory (Evaluation of Automated Transport Systems and their Safety) of Gustave Eiffel University to pursue a Ph.D. thesis.

In 2022, he received his Ph.D. from University of Lille for his thesis on 'Safety and Operational Performance Evaluation of GNSS-based Railway Localization Systems Using a Formal Model-based Approach.' Currently, Ouail is a post-doctoral researcher at IRT Railenium, where his research focuses on the safety assurance of AI/ML systems for use in autonomous trains.

JULIE BEUGIN received the engineering degree from INSA Hauts-de-France (National Institute of Applied Sciences) in 2002, the master's degree in automation engineering from Polytechnic University of Hauts-de-France in 2002, and the PhD degree in automation and computing sciences in 2006.

Since 2007, she has been with Gustave Eiffel University as a researcher. Her research interest in the ESTAS laboratory deals with dependability and safety evaluation of complex guided transportation systems. Part of her activities addresses RAMS demonstration issues of GNSS-based solutions embedded in train control applications. She participated in the GaLoROI, ERSAT-GGC, STARS European projects. She has secondment agreements with Railenium to participate to projects in her research fields and with Certifer to realize ISA missions.

MOHAMED GHAZEL is a research director with the University Gustave Eiffel – COSYS department (previously at IFSTTAR), and is the Director of the ESTAS laboratory. He received the Master and Ph.D. degrees in Automatic Control and Industrial Computer Sciences from The École Centrale de Lille in 2002 and 2005, respectively; and the HDR (Habilitation à Diriger des Recherches) from University Lille Nord de France in 2014.

His research mainly focuses on the engineering, safety and interoperability of transportation systems using discrete event models and formal methods. He is co-author of more than 100 papers in international journals, chapters and conference proceedings. Dr. Ghazel is a member of the IFAC technical committees TC 7.4 on Transportation Systems and TC 9.2 on Social Impact of Automation, and has been involved in several French national and European research projects. He acts as an expert for the European Commission in the framework of innovation programs since 2016. He is also a lecturer in several universities and engineering schools in the fields of discrete event systems, system engineering and dependability.