Toward Formal Safety and Performance Evaluation of GNSS-based Railway Localisation Function

Ouail Himrane, Julie Beugin, Mohamed Ghazel

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 54-2 (2021) 159–166

Toward Formal Safety and Performance Evaluation of GNSS-based Railway Localisation Function

Ouail Himrane * **Julie Beugin** * **Mohamed Ghazel** *

* *COSYS-ESTAS, Univ Gustave Eiffel, IFSTTAR, Univ Lille, Villeneuve d'Ascq, France (e-mail: firstname.lastname@univ-eiffel.fr).*

Abstract:
European Train Control System (ETCS) is the signalling and control component of the European Rail Traffic Management System (ERTMS). This system is essential to guarantee the safe and interoperable operation of trains. To enhance the competitiveness of rail transport services, the introduction of innovative solutions are under study in view of the evolution of ETCS. In this context, the adoption of Global Navigation Satellite System (GNSS) for train localization is investigated as a technology which can ensure an undeniable added value for railways. Yet, a main challenge is to provide safety evidence permitting the certification of these new systems. In particular, the classical safety analysis approaches show limitations in dealing with the complexity of such systems. Therefore, more adapted safety and performance analysis techniques have to be elaborated. In this paper, a model-based approach, adapted for the evaluation of GNSS-based localisation systems in railway, is presented. Considering the safety-critical aspect of the localisation function in railways, formal methods which are based on rigorous mathematical foundations are adopted in the present work. Concretely, a set of formal models are elaborated to ensure a modular representation of trains dynamics in the context of GNSS-based localization. Namely, probabilistic timed automata formalisms are adopted to this aim. Such notations allow for considering stochastic and dynamic aspects, so as to reflect reality in a trustworthy way. The safety and performance properties to be checked can then be formulated by means of temporal logics. Finally, the analysis of such features can be achieved by means of model-checking and simulation techniques. This evaluation phase yields both qualitative and quantitative results and allows for assessing the impact of various parameters and functional choices on both safety and performance. UPPAAL-SMC engine was used to set the tooling chain of our approach, and an illustration considering specific operational test cases is provided.

Keywords: GNSS-based train positioning, Model-based analysis, Formal verification, ERTMS/ETCS, Railway Safety and performance evaluation, Intelligent transportation systems, Railway critical operations.

1. INTRODUCTION

Transportation systems are safety-critical systems whose failures may result in considerable losses. In railway transportation, this may involve damage to equipment and environment, serious injury to people or even the loss of human lives. In order to avoid train collision or derailment, three main safety functions are implemented, namely: management of routes allocation, safe distance separation between trains, and over-speed prevention. These functions are at the core of railway signalling systems, and provide the driver with the relevant information and warnings to adapt the speed of the train or brake when necessary (Yin et al., 2017).

Historically, all European rail signalling systems were developed on a national basis. Hence, the absence of common technical and operational standards has considerably limited the railway interoperability between countries. That is why the ERTMS (European Rail Traffic Management System) standard was defined. Namely, it aims to harmonise the railway control and signalling systems throughout Europe, so as to ensure railway interoperability in Europe and enhance the competitiveness of the railway sector (Ranjbar and Olsson, 2020).

The ERTMS/ETCS standard defines three different operational levels, depending on the various trackside and onboard configurations. Operational levels 1 and 2 are currently adopted in Europe, while level 3, which is supposed to provided the maximum benefits, is only conceptualized. In levels 1 and 2, trackside equipment are used to detect track occupancy. Level 2 specifically implements a radio link to reduce the trackside visual markers and allows the train positions to be continuously tracked.

The basic principle of levels 1 and 2 is the decomposition of the track into fixed blocks named *sections*, each of these physical track sections being equipped with train detectors

⋆ This work is part of ELSAT2020 programme co-financed by the European Union with the European Regional Development Fund, the French state and the Hauts-de-France Region Council.

10.1016/j.ifacol.2021.06.049

such as balises and track circuits, (Commission Regulation (EU) 2016/919, 2016). Each block cannot be occupied by more than one train at the same time. The length of these blocks is determined according to the speed limit of the line, the braking characteristics of the operated trains and the targeted traffic density. However, to ensure safe railway operations, the length of the blocks is constrained by the most restrictive configuration. As a result, the faster the trains are allowed to run, the longer is the braking distance and, consequently, the longer the blocks must be. Obviously, this directly impacts the line capacity.

With the aim to implement the ERTMS level 3, a number of technological innovations, in particular GNSS-based localisation solutions, are under study. The main objective is to increase the capacity of the railway lines as train position accuracy can be improved, reduce the maintenance costs as trackside equipment can be removed, while maintaining or even improving the safety of train operations.

The adoption of such satellite-based systems should permit the train to autonomously and continuously determine its location. Hence, more flexible operating principles shall be possible, in particular, two main operational modes are being investigated currently, and are at the core of several research projects:

- Using virtual fixed blocks instead of physical blocks, *Hybrid ETCS Level 3* (EEIG ERTMS Users Group, 2018): Under this mode, a large number of physical balises can be replaced by immaterial entities, called virtual balises. The functions of these balises are implemented on-board trains. In contrast with the physical division of the track, the logical division by means of virtual blocks allows for adjusting the length of the blocks to the real operational conditions.
- Using moving blocks (Basile et al., 2020): Rather than dividing the track into fixed blocks, the main principle here is to dynamically determine a safe zone, called *moving block*, around each train. This safe zone is established and adapted according to the continuous estimated positions and velocities of the trains. As a result, the trains can run closer to each other while keeping spaced by a safe braking distance (including some safety margin).

In this context, several European projects were conducted in the last two decades (Marais et al., 2017). Yet, although several system architectures were proposed for GNSS-based train localisation, none of these projects has resulted in an operational technical solution that fulfills the railway safety requirements. It is worth recalling that the GNSS systems were initially developed for the aviation sector. Hence, the safety demonstration approaches associated to these systems, as currently defined, are not adapted for the railway environment (Filip et al., 2017). The operation principle of GNSS is based on the constellation of satellites in orbit. These satellites transmit signals allowing a receiver to estimate its position. This estimation is calculated based on the signal propagation delay from the transmitter to the receiver (Groves, 2013). In the railway operation context, the presence of some items in the operation environment, such as vegetation and buildings, can lead to signal perturbations. Moreover, GNSS coverage cannot be continuously guaranteed due to signal loss in harsh environment, such as in tunnels. Having said that, it is clear that adequate safety and performance demonstration means, for the evaluation of GNSS in the railway context, still need to be elaborated so as to ensure the safety confidence levels required in railways (Baigen et al., 2020).

In this paper, a model-based approach, adapted for the evaluation of GNSS-based localisation systems, is presented. Considering the safety-critical aspect of the localisation function in railway, formal methods are adopted. In particular, the proposed approach consists in developing parameterizable models that allow for depicting various railway operational scenarios, considering GNSS-based localisation. The elaborated models are based on formal notations with rigorous syntax and semantics.Using these models, various safety and performance properties can be specified with formal notations. Therefore, model-checking algorithm can be brought into play to qualitatively and quantitatively investigate such features. In this paper, we particularly focus on the representation of the train localisation function, under nominal conditions. Various aspects are considered in the developed models: the odometer related position errors, the balises detection and activation mechanism, and the train movement dynamics. The UPPAAL-SMC modelling and verification tool (David et al., 2015) is used to develop our models and perform the analysis. Probabilistic and timed automata are adopted as a modelling notation, which permits the consideration of stochastic and dynamic aspects.

The remainder of this paper is organized as follows. Section 2 introduces the context and motivation of this work. The general principles of the proposed model-based approach are presented in section 3. Then, section 4 is dedicated to the elaboration of the behavioural models. In section 5, we show how the model-checking can be exploited to investigate a number of operational scenarios and check various safety and performance properties. Finally, some concluding remarks as well as the perspectives of this work are addressed in section 6.

2. CONTEXT AND RELATED WORKS (NEED FOR MORE ADAPTED METHODS)

In the last few years, several academic and industrial projects have been conducted to address the introduction of GNSS-based localisation systems in the railway applications. These projects resulted in multiple innovative solutions supporting the evolution of European control and signalling systems. The combination of a GNSS receiver with other technologies, such as inertial sensors for instance, was proposed. Other contributions investigate the use of onboard power measurements for online train motion estimation (Sessa et al., 2020). The main objective is to adapt GNSS technology, initially developed for avionic utilisation, to land mobility applications. Although these technical solutions are promising, the lack of relevant safety demonstration tools remains a key obstacle facing their wide deployment for safety-critical applications.

On the one hand, the traditional safety analysis methods, such as fault tree analysis or FMEA, are well established techniques, which are widely adopted in the railway sector.However, these methods suffer from inherent limita-

tions, particularly due to the required inputs, namely dependability parameters, such as the components failure rate for instance. The acquisition of these characteristics requires enormous amount of time for data collection. Yet, for such new systems no enough data and feedback are available so far. Furthermore, classical approaches are strongly dependent on the architecture of the system, and no standard/reference architecture is available for GNSS-based railway localisation function. Finally, most of these methods are static. That is why they do not allow for finely considering the dynamic impact of the operational environment.

On the other hand, on-site testing approaches benefit from a great power of conviction. However, the implementation of these methods is both expensive and time-consuming. In addition, the obtained results are strongly dependant of the testing environment conditions. Consequently, for the case of GNSS-based railway localisation, since it is awkward to finely emulate the real environment conditions, the experiment results may be questionable at the end.

The adoption of formal verification methods for the evaluation of safety-critical applications, such as railway localisation, is highly recommended (Ferrari et al., 2019). These approaches are based on rigorous mathematical formalisms with clear semantics, which reduces the errors resulting from human interpretation. Moreover, several techniques are available and allow for investigating various properties on the established behavioural model, automatically. In addition, a main benefit of such techniques is pertaining to the exhaustiveness of the analysis which, in general, remains unreachable by means of classical dependability techniques and testing when we deal with complex systems.

The aim of this contribution is to propose an adapted complementary method that permit to overcome the current limitations. In this context, the next section is dedicated to the introduction of the proposed approach.

3. PROPOSED METHOD

The approach we propose attempts to bring formal methods into play for assessing the safety of GNSS-based railway localisation. It considers the safety and performance analysis of the localisation system as *model-checking* (MC) problems. MC is a technique that allows for checking some feature, expressed as temporal logic property, on some model that describes the system behaviour. The main advantages of this technique are related to its exhaustiveness and the fact that it is fully automatic. In addition, if the property is not satisfied on the model, a counter-example is provided, which consists a substantial support for the debugging activities. However, the results obtained by means of MC are as good as the elaborated models are realistic, *i.e.*, reflect the real behaviour faithfully. Hence, the modelling remains a crucial phase in model-checking approaches, and is highly dependent on the user expertise both in terms of modelling and system expertise.

In our approach, we advocate for elaborating various modules to represent the behaviour of the GNSS-based localisation function. The underlying idea is to set up a modular approach that can be adaptable to different functional architectures. The models are developed using a variant of finite state machines, which is the probabilistic timed automata of UPPAAL. On the other hand, the properties to be verified are expressed as temporal logic assertions. The verification engine automatically checks the properties against the model, and in case a property is not satisfied, an evidence illustrating a sequence that leads the violating state is issued. These unexpected but possible behaviours have to be addressed to refine the system technical specification.

To rigorously model the possible behaviours of the system, the first step consists in the consideration of the technical specifications of the system to translate its nominal behaviour.

In the context of safety analysis, it is required that the used models are as close as possible to the actual behaviour of the system. Moreover, the possible dysfunctional behaviour of the system (exp. component failure, communication problems) has to be considered.

As regards GNSS-based localisation in railways, since the performances of such function highly rely on environmental parameters, several projects have focused on the characterisation of the railway operating environment from the GNSS localisation point of view. In our work, a special attention was paid so as to allow the integration of the impact related to the rail operational context. Therefore, the results of the aforementioned results can be taken into consideration. For a more complete presentation of this particular aspect, the reader is invited to consult our previous paper, (HIMRANE et al., 2020).

Another aspect that we address in our work is to enable considering different operational scenarios. This issue is presented in more details in section 5.

Figure 1 outlines the general idea of the approach, while further details are provided on the various steps in the following section.

4. ESTABLISHMENT OF THE BEHAVIOURAL MODELS

A main step of the proposed approach consists in modelling the nominal behaviour of the system. In this section, the various aspects that are relevant for the description of the GNSS-based localisation function in railways are addressed.

4.1 Choice of the adapted modelling tool

Given the various requirements that we have discussed earlier in this paper, the modelling tool must allow a formal and modular representation of the system behaviour. Moreover, it must enable to consider probabilistic, temporal and dynamic aspects, in order to ensure a realistic representation of the behaviour. Furthermore, the generated models must be configurable. This allows their re-usability, in order to address different architectures and operating contexts. In our work, we adopted the UPPAAL tool which is a formal modelling and verification tool that fulfills the aforementioned requirements. This tool allows for representing the system behaviour in the shape of communicating timed automata. In fact, the system is subdivided

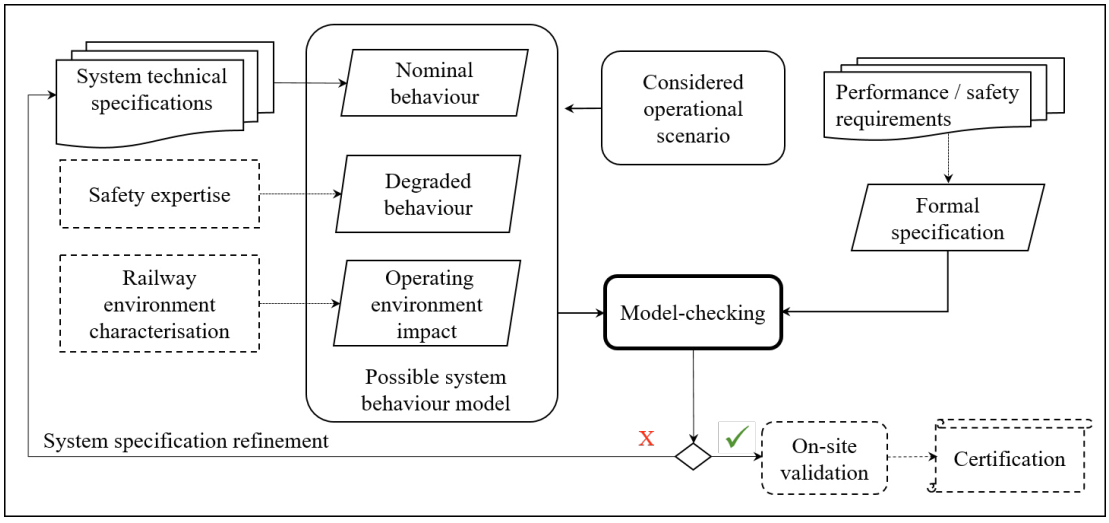

Fig. 1. Overview of the proposed method

into several interacting elements modules. Each module is modelled by means of a timed automaton, extended with clocks, variables and synchronization channels. The composition of these automata allows for translating the behaviour of the global system, with the possibility to integrate global variables and clocks. In addition, through its SMC extension, UPPAAL makes it possible to take into consideration uncertainty in the system behaviour, by means of stochastic automata. Finally, UPPAAL offers powerful verification facilities implemented as classical and statistical [1] model-checking algorithms.

For a more complete presentation of the UPPAAL SMC tool, the reader is invited to consult David et al. (2015).

4.2 Representation of the train localisation function

In this contribution, we mainly focus on the localisation function in railways. Conventionally, this railway function is mainly performed by odometers. The odometer is a relative position sensor. More precisely, it enables to estimate the travelled distance from some given reference position. The operating principle is based on the calculation of the number of revolutions of the wheels. The the travelled distance can then be derived, knowing the wheel circumference.

Due to the deviations due to wheel jamming and slipping on the track, as well as the inherent imprecision of the odometer, some errors are accumulated as the travelled distance increases. Therefore, it is crucial to take into account such deviations in the models of the localisation function. According to the technical specifications of the odometer (Commission Regulation (EU) 2016/919, 2016), this position error must not exceed $5m+5\%$ of the travelled distance.

4.3 Odometric reset by activation of physical balises

In order to correct the position error accumulated by the odometer, physical balises (PB) are positioned on the track. These balises are passive components. They can only be activated using the energy supplied by some devices in the passing trains. Namely, the train continuously emits an electromagnetic signal while running in order to activate any encountered balise. Once activated, the balise sends a telegram containing information on its position along the track to the train onboard. This telegram is received and interpreted by a computer on-board the train. Therefore, the train determines its exact position every time a PB is encountered. Such a position is then used as a new reference for localisation. This behaviour is translated as an automaton model called *balise transmission module*.

4.4 Virtual balise detection

As mentioned in the introduction of this paper, a main motivation behinds the ERTMS standard is to reduce life-cycle costs in railways. Mainly, this can be achieved by reducing the number of track equipment. Indeed, this allows cost-savings associated with the installation and maintenance of such equipment. In this context, the introduction of GNSS shall allow the reduction of PB needed to help localise trains. However, as discussed earlier, the use of GNSS as the only localisation means does not comply with railway safety requirements. Therefore, GNSS technology needs to be combined with additional means to help tackle the inherent errors related to GNSS. In particular, the onboard odometer facility shall be kept. In addition, some concepts are being investigated to substitute to PB. The concept of *virtual balise (VB)* falls into this context. VB are abstract entities which *emulate* PB, but which do not correspond to some physical device along the track. Namely, the information regarding the position of these balises are directly stored on-board the train computer. The activation of the VBs is no longer achieved via an electromagnetic wave, but through the use of the GNSS position. To this end, the computer compares the position given by the GNSS with the position of the next expected VB. When these two positions match, the information associated with the VB are extracted. The position of the virtual balise is then used as the new reference position. This enables the position error related to the odometer to be readjusted. The above described behaviour is translated

[1] Also denoted as SMC

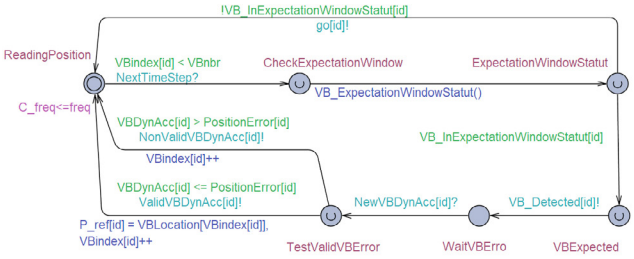

Fig. 2. Virtual balise reader (VBR) module

as an automaton model called *virtual balise reader (VBR) module* and shown in Figure 2.

4.5 Position Error reset

As detailed previously, one of the main roles of the balises is to correct the error accumulated by the odometer. However, the absolute position provided by the PB is not considered as rigorously accurate. The reason is that there are errors related to the accuracy of the recorded position of the balise on the track. In addition, the activation of the PB by electromagnetic energy may cause an offset. Therefore, a position interval is considered as a safety margin related to the detection of the PB. This error, characterized by the variable 'Q_{LocAcc}+ *offset*' in the ERTMS specifications, is considered in our models for odometer resetting (Fig. 3).

In the case of VBs, since they do not correspond to physical entities, the errors related to the physical positioning along the track do not apply anymore. However, the associated error is related to the GNSS error at the time of the activation of the VB. As a result, the resetting of the odometer is no longer associated with a fixed value which is common to all the balises, but by a dynamically calculated *protection level* (PL) value specific to each virtual balise.

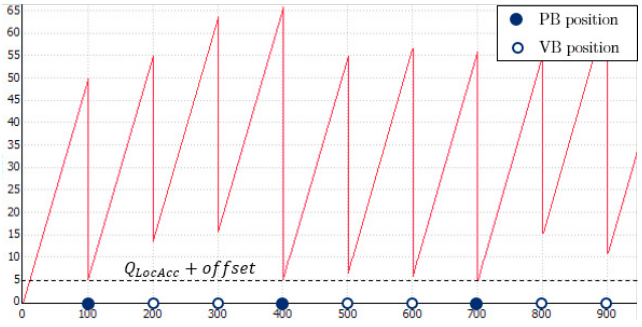

Fig. 3. Train position error reset

4.6 Train movement dynamics

The other aspect to consider in the models is the train dynamics. This involves the representation of the train movement while depicting the various speed phases (acceleration and braking). This allows us to track the trains positions and speeds in time, finely and continuously. These parameters are of paramount importance in railway. As an illustration, a train that runs at a speed of 300 km per hour can require up to 3 km to stop. Obviously, such a braking distance needs to be foreseen to avoid that the trains enters some danger zone (see Fig. 4).

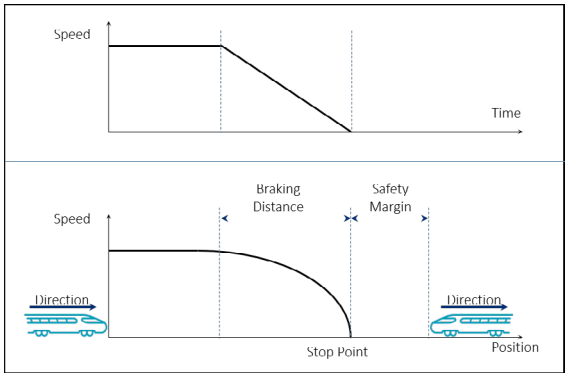

Fig. 4. Braking Distance

In our approach, a model is dedicated to represent the evolution of the train position according to its different dynamical phases (Fig. 5). In this model, three states are mainly distinguished according to the value of the acceleration. At each time step, a function compares the current speed of the train with the target speed value communicated by the trackside. This allows us to automatically adapt to the speed limitations. On the other hand, the train position is continuously updated, while taking into account the acceleration and speed values of the train. It should be noted here that the developed models are configurable, in the sens that the dynamic characteristics of the train (acceleration, braking, etc.) can be set as parameters according to the type of the train (passengers, freight, etc.) and the weather conditions of the track (dry, wet, etc.).

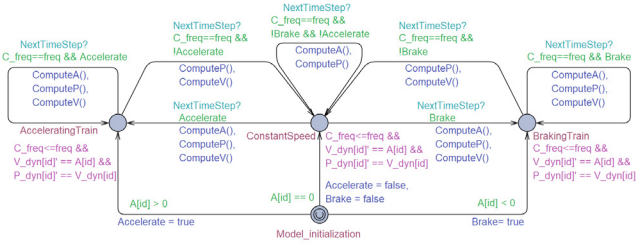

Fig. 5. Train Dynamics Model

In fact, the train localisation function can be depicted by combining the various model introduced in this section. Since we aim to analyse some safety and performance features pertaining to localisation function, in the next section we will focus on the operational scenarios to be investigated as well as the safety and performance properties to be checked.

5. APPLICATION FOR SAFETY AND PERFORMANCE RESULTS ANALYSIS

5.1 Train speed profile description

The first aspect to be considered for the modelling of the operational scenario is pertaining to the speed profile of the train. This speed profile determines the targeted speed all along the train route (Fig. 6). Depending on the scenario to be investigated, the targeted speed may correspond to the maximum speed allowed at each portion of the train route, or to some particular speed determined by the user. The train dynamics module, introduced in

section 4, shall automatically adapt the train speed by either accelerating, braking, or maintaining the train speed.

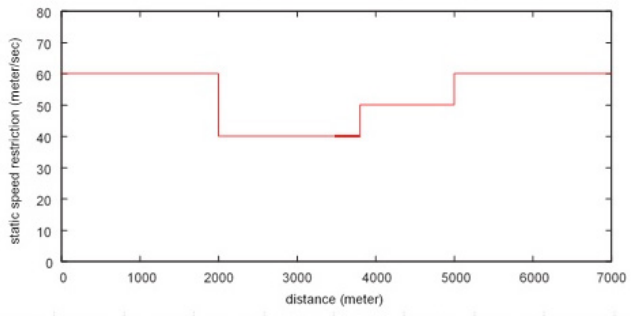

Fig. 6. Train speed profile description

5.2 Balises position configuration

Regardless of the complexity of the railway network on which a train is running, the train route can be defined by a series of balises that the train shall encounter during its journey. As a consequence of the introduction of GNSS-based means for localisation, this suite of balises will no longer consist exclusively of physical balises, but will also include virtual balises. This raises the issue on how to set the PB and VB along the track. In our work, two main parameters have been considered for this purpose:

- The distance d between two consecutive balises, and
- The number n of virtual balises positioned between two physical balises.

Thus, by simply adjusting these two parameters, different configurations can be represented, as illustrated in Figure 7.

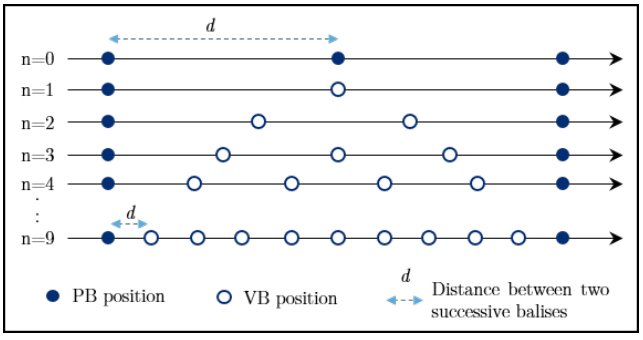

Fig. 7. Balises configuration along the track

5.3 Environment type

As explained in section 3, the performance of the localisation systems using GNSS is heavily impacted by the surrounding environment. Therefor, in our models, we take into account this variability in terms of the environment conditions w.r.t. GNSS localisation. Namely and for the sake of simplicity, we consider two main types of operating environment conditions as follows.

- *OpenSky*: which represents an open environment suitable for the reception of direct GNSS signals;
- *NonOpenSky*: representing a constrained environment that degrades the performance of the GNSS sensor, due to line of sight obstruction for instance.

On this basis, several combinations of these two variants of the environment conditions can be made to represent the set of the case study scenario. It should be mentioned that, depending on the user need, more variants could be derived in the same way.

5.4 Localisation unit characterization

As mentioned earlier in section 4, the main purpose of setting balises along the track is to correct the accumulated position error of the odometer. While the value of the reset value corresponding is statically encoded in the PB, the reset value in the case of VB is estimated dynamically on board the train. This value corresponds to the *protection level* calculated by the localisation unit based on the GNSS signals received at the time of detection of the VB.

This aspect is of particular importance when it comes to evaluate the impact of the introduction of GNSS-based localisation units, according to the virtual block operating principle. In our work, we use different probabilistic (normal) distributions to represent the protection level related to VB, as shown in Figure 8.

In our case, the normal distribution *(mean =10, standard deviation =5)* is adopted to characterize the quality of the GNSS localisation information in the OpenSky environment. As for the route portion where the light of sight is not ensured (*i.e.*, NonOpenSky), several other normal distributions can be used to reflect the degradation of the GNSS signal. It should be noted that these distributions are adopted here for illustrative purpose only. Different distributions may easily be configured in our models.

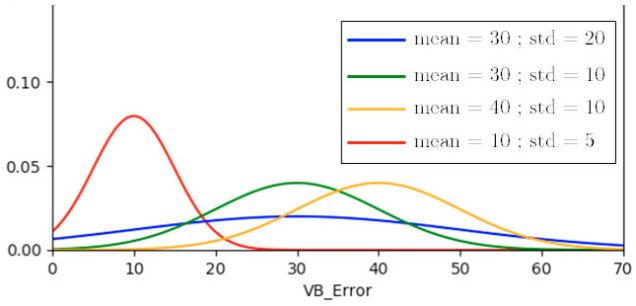

Fig. 8. Characterization of the VB detection protection level

5.5 Formulation of the properties to be checked

In the rail sector, the two major critical incidents that must be avoided are train derailments and collisions. In order to avoid derailments, train speed must be kept below a safety threshold specific to each section of the track. To prevent collisions, the position of the trains must never exceed a certain position representing a danger point. Therefore, one must continuously ensure that the train is able to before reaching this danger point (see Figure 9).

The definition of the danger point depends on the operational principle of the line. If the line is operated according

to fixed block principles, the danger point represents the entry point of an occupied block section. If the line is operated according to moving block principles, the danger point represents the position of the safe rear end of the preceding train.

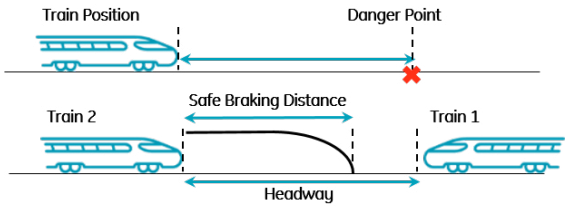

Fig. 9. Railway danger cases

To bring into play model-checking for the verification phase, the features to be checked need to be expressed as formal properties (Ghazel, 2014). To help expressing such properties, we adopt the watchdog artefact Mekki et al. (2012). It consists in representing the property as an automaton model which includes a particular state that represents the property violation. In practice, the verification of the corresponding property can be achieved by checking (by means of model-checking in our case) whether the violation state can be reached or not (see Figure 10). In our case, in order to check the aforementioned risks, namely train collision and derailment, the train position, speed, and distance from a danger point are continuously monitored. Moreover, by considering the trains position confidence interval and depending on the current train speed, the necessary braking distance is computed. This braking distance is the main factor that determines the safety distance to be maintained between the train and the danger point.

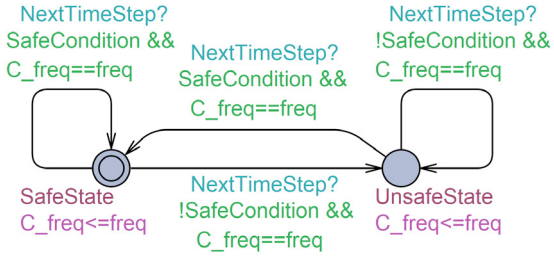

Fig. 10. Use of a watchdog to check some safety property

5.6 Property verification results

The execution of the model checking algorithms included in the UPPAAL tool provides two types of results:

- Qualitative: we can check whether some location in the model, which represents the unsafe situation can be reached. If so, a sequence that leads to this situation is also provided.
- Quantitative: probabilistic distribution, frequency diagram and confidence interval resulting can be derived from the statistical model-checking (eg. Estimate max position error, Probability of train velocity exceeding the speed limit...).

Being given the modularity and the configurability offered by the models we have developed, it becomes possible to consider a multitude of track layouts (PB and VB implementation) and environment conditions (variability in terms of GNSS signal quality). For the sake of illustration, let us consider an operational scenario characterized by the following aspects:

- Environment conditions: *OpenSky* all along the route,
- $d = 1km$,
- $n = 2$,
- A constant speed $360km/h$ all along the route.

In this particular configuration, the maximum value of the position *protection level (PL)* is estimated through the statistical model checking algorithm. Each simulation run provides a resulting value (from 55m to 82m). The final results are displayed in figure 11, where the x-axis presents the position error PL and the y-axis presents the corresponding probability.

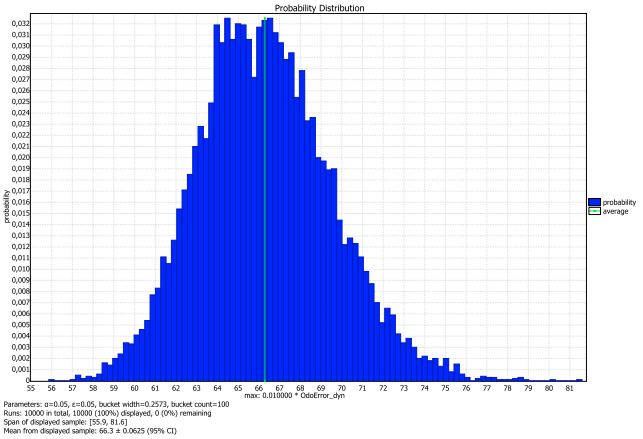

Fig. 11. Example of the simulation results

The PL represents the maximum deviation between the train estimated position and the safe position considered for the train spacing calculation. Such a gap is bounded by a fix threshold when only PB are used. Therefore, the PL can be predicted on the basis of the train position only. When using VB, the PL depends on dynamic aspects that cannot be known in advance. In this regard, the the results obtained through SMC have a particular benefit, since they permit to characterize the localisation error in this context. This paves the way to the analysis of the impact of introducing GNSS-based localisation techniques on line capacity. Moreover, the movement authorisation assignment policy may be adapted while taking these results into account.

6. CONCLUSION

The introduction of the GNSS-based localisation as a safety-related function in the railway sector constitutes a major technological breakthrough with substantial benefits. However, this challenge can not be achieved unless the safety of the localisation function is proven. The motivation of the present work consists in adopting formal methods to help evaluate the train localisation function when GNSS-based localisation is brought into play. Several formal models have been established to represent the

railway localisation function involving GNSS. In particular, the representation of the position related errors, the mechanisms of balises detection and the dynamics of the trains movements are addressed. In order to deal with the complexity of the system, the system modelling is based on a modular representation. Moreover, the developed modules are configurable in order to allow their adaptability and re-usability according to the needs of the study. In particular, we have shown how different railway operating contexts can be considered. In our study, model-checking for verification purposes. An illustration is provided regarding the monitoring of train position and speed.

The modelling choices adopted in the present approach aim to provide the basis for an evolutive method that can be enriched iteratively. This makes it possible to take into account the complexity of the system in a gradual and progressive manner. Thus, a natural prolongation of this work is to extend our models in order to address more parameters, such as the representation of movement authority generation, for instance. Moreover, the dysfunctional behaviour of the system will be addressed in forthcoming works. The study of more detailed scenarios and the precise evaluation of safety-related properties is foreseen in the continuation of this contribution.

REFERENCES

Baigen, C., Boqian, W., and Debiao, L. (2020). Survey of Performance Evaluation Standardization and Research Methods on GNSS-Based Localization for Railways. *Chinese Journal of Electronics*, 12.

Basile, D., ter Beek, M.H., and Legay, A. (2020). Strategy Synthesis for Autonomous Driving in a Moving Block Railway System with Uppaal Stratego. In A. Gotsman and A. Sokolova (eds.), *Formal Techniques for Distributed Objects, Components, and Systems*, Lecture Notes in Computer Science, 3–21. Springer International Publishing, Cham. doi:10.1007/978-3-030-50086-3.

Commission Regulation (EU) 2016/919 (2016). *Technical Specification for Interoperability relating to the Control-Command and Signalling subsystems of the rail system in the European Union*.

David, A., Larsen, K.G., Legay, A., Mikučionis, M., and Poulsen, D.B. (2015). Uppaal SMC tutorial. *International Journal on Software Tools for Technology Transfer*, 17(4), 397–415. doi:10.1007/s10009-014-0361-y.

EEIG ERTMS Users Group (2018). *Hybrid ERTMS/ETCS Level 3*.

Ferrari, A., ter Beek, M.H., Mazzanti, F., Basile, D., Fantechi, A., Gnesi, S., Piattino, A., and Trentini, D. (2019). Survey on Formal Methods and Tools in Railways: The ASTRail Approach. In *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification*, volume 11495, 226–241. Springer International Publishing, Cham. doi:DOI: 10.1007/978-3-030-18744-6.

Filip, A., Sabina, S., and Rispoli, F. (2017). A framework for certification of train location determination system based on gnss for ertms/etcs. *International Journal of Transport Development and Integration*, 2(3), 284–297. doi:10.2495/TDI-V2-N3-284-297.

Ghazel, M. (2014). Formalizing a subset of ERTMS/ETCS specifications for verification purposes. *Transportation Research Part C: Emerging Technologies*, 42, 60–75. doi: 10.1016/j.trc.2014.02.002.

Groves, P. (2013). *Principles of GNSS, inertial, and multisensor integrated navigation systems*. Artech House, second edition edition.

HIMRANE, O., Beugin, J., and GHAZEL, M. (2020). Towards a model-based safety assessment of railway operation using GNSS localization. In *ESREL 2020 PSAM 15, 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*, 8p.

Marais, J., Beugin, J., and Berbineau, M. (2017). A Survey of GNSS-Based Research and Developments for the European Railway Signaling. *IEEE Transactions on Intelligent Transportation Systems*, 18(10), 2602–2618. doi:10.1109/TITS.2017.2658179.

Mekki, A., Ghazel, M., and Toguyéni, A. (2012). Validation of a new functional design of automatic protection systems at level crossings with model-checking techniques. *IEEE Trans. on Intelligent Transportation Sytems*, 13(2), 714–723.

Ranjbar, V. and Olsson, N.O.E. (2020). Towards mobile and intelligent railway transport: A review of recent ERTMS related research. 65–73. doi: 10.2495/CR200061.

Sessa, P.G., Martinis, V.D., and Corman, F. (2020). Filtering approaches for online train motion estimation with onboard power measurements. 35(5), 415–429. doi: https://doi.org/10.1111/mice.12514.

Yin, J., Tang, T., Yang, L., Xun, J., Huang, Y., and Gao, Z. (2017). Research and development of automatic train operation for railway transportation systems: A survey. *Transportation Research Part C: Emerging Technologies*, 85, 548–572. doi:10.1016/j.trc.2017.09.009.