Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control

Julie Beugin, Cyril Legrand, Juliette Marais, Marion Berbineau, El Miloudi El Koursi

Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control

Julie Beugin, Cyril Legrand, Juliette Marais, Marion Berbineau, *Member, IEEE,* and El-Miloudi El-Koursi

***Abstract*—The use of Global Navigation Satellite Systems (GNSS) will provide significant advantages for ensuring the control of train movements on railway networks equipped with ERTMS/ETCS. Indeed, this disruptive technology can play an important role for reducing the rail infrastructure's equipment by enabling trains to determine their position in an autonomous way. Specific associated hazards have to be considered in the European signaling system. From this perspective, performances of GNSS-based localization systems were analyzed in different past studies. They highlighted what they can bring to the railway domain. For going further than performance-centric analyses to help inserting these systems safely in rail applications, this work want also to focus on their operating uses. For that, the safety evaluation proposed in this paper is able to handle specific estimated confidence-related data that are associated to an estimated position. This article firstly details the managed risks in ETCS due to the localization function with, in particular, those that may arise due to GNSS-based systems. It discusses the evolution of these risks when dealing with moving block operation of the ETCS-level 3. The safety evaluation approach is then explained. It relies in fact on extended integrity data handled in the case of the train spacing. Finally, it is applied in different operational cases to show evaluation results when real GNSS data are measured in a railway environment.**

***Index Terms*—ERTMS, moving block, GNSS, localization integrity risk, railway safety assessment, probability of hazardous situation.**

I. Introduction

TO answer current economic challenges, railway domain focuses on 100% increase of the capacity, 50% reduce of the life cycle costs and, 50% increase of reliability and punctuality [1]. Reducing costs while increasing capacity is an urgent target particularly for secondary and regional lines. However, the changes will only be accepted if the achieved level of performance by the improved system is at least equal to what the current systems can provide today, this is true especially concerning safety.

In Europe, changes in the global railway system, which can impact the current safety level, are governed by the European legal framework. The main safety-related texts are, in the one hand, the CSM regulation (Common Safety Method) [2] that defines a harmonized risk management process to be applied to new rail systems or when a change appears in operating conditions. On the other hand, they concern the railway safety standards EN50126, EN50128 and EN50129. For evolutions aiming at improving or renewing on-board and trackside subsystems that insure the management of train movements on the European rail network, the European railway community has defined a common standardized framework called ERTMS (European Rail Traffic Management System). The train control and protection part of the ERTMS is the ETCS (European Train Control System) and is governed by the TSI-CCS (Technical Specification for Interoperability for the 'Control-Command and Signalling' subsystems) [3]. The ETCS can be implemented with different technological levels (three are possible) according to the migration efforts envisaged to enhance current installations.

Satellite-based localization systems (using GPS or Galileo for example) are new technologies that can play an important role for reducing the rail infrastructure costs because, instead of relying on equipment installed all along the tracks (track circuits, axle counters, etc.), trains can use satellite signals to calculate their position in an autonomous way. Such possibility makes Global Navigation Satellite Systems (GNSS) appear as "game-changers", especially for ERTMS stakeholders that see them a serious opportunity to implement the latest stage of ETCS. Confirming this idea, a new ERTMS Memorandum of Understanding was signed in September 2016 between these railway actors [5]. ETCS-level 3 relies on the idea that a train can be associated with a surrounding virtual zone that is dynamically obtained knowing the train position and its velocity. Such safety buffer, in which the train resides (with a ban on going out) and in which other trains are forbidden to enter, is called a moving block [4]. It leads to fluidity in train traffic because the size of the authorized route for a train becomes flexible and no longer preset by the existing fixed blocks (delimited currently by track circuits with optical trackside signals or with beacons). To ensure the safety of train traffic following the moving block principle, a *continuous and accurate* train positioning service is essential. GNSS, not standalone, but hybridized with one or several other localization devices in an integrated navigation solution, allows these features to be fulfilled. The added devices enable positions to be provided continuously, especially when satellite signals are not received like in tunnels. The GNSS measurements enable positions to be provided more accurately when coupled with other devices, especially since data are sampled frequently and periodically. Diversity in equipment properties also make errors balance each other for a better accuracy.

However, a challenging issue remains to demonstrate the safety of the localization function realized by an on-board GNSS-based system. Environmental conditions encountered

J. Beugin, J. Marais, M. Berbineau, and E.-M. El-Koursi are with IFSTTAR, the French institute of science and technology for transport, development and networks, University of Lille Nord de France, IFSTTAR, COSYS, F-59650 Villeneuve d'Ascq, France.

C. Legrand is with EPSF which is the French railway safety authority, F-80000 Amiens, France and with the Railenium technological research institute, F-59300 Famars, France.

by such systems can lead to a position estimate whose error is greater than the expected user requirements. Previous studies focused on the safety performances of different technical architectures [6], [7] and qualified errors with railway criteria [8]. But, safety appraisal relies not only on the system performance evaluation. It also strives from ensuring that all safety conditions are fulfilled when the system is in use. Thus, train interactions (routes, headway, different speeds, etc.) have to be considered, otherwise the safety analysis remains insufficient.

The on-board installation could only be considered as safe if its operational use is analyzed both by performance indicators and through the analysis of the risk levels linked to identified hazardous scenarios. Safe conditions in a scenario are assessed depending on the respect (or not) of a tolerable error limit associated to the rail operation. The question is then how to demonstrate that the out-of-tolerance cases occur few enough times, or with a sufficiently short duration, to be accepted. The safety analysis could then bring the evidences that existing risks are acceptable in different railway operational conditions.

This work wants to go further than the past studies concerning the safety analysis of a GNSS-based localization system by focusing on a specific railway operation rather than only on technical performances. For that, the safety appraisal proposed in this paper is able to handle specific estimated confidence-related data that are associated to an estimated position. These data are obtained from the integrity monitoring method explained in [9] and briefly reminded in the article. Using the obtained extended integrity data, the novel approach will lead to evaluations according to railway safety accepted criteria. It will make possible to bring evidence for safety demonstration of railway localization systems based on GNSS, especially in the context of ETCS level 3.

This article is structured as follows. Section II will present how risks linked to the localization function are managed in today implementation of ETCS level 2 and what are the associated safety targets. We will discuss how risks could be managed in ETCS level 3 when GNSS-based systems are used to enable train operation with moving blocks. Section III will present the proposed safety evaluation approach in the case of the train spacing. In section IV, results on an evaluation performed with real GNSS data will be detailed. Finally, section V will conclude and address perspectives.

II. Risks of the localization function in ETCS

In ERTMS documentation, made publicly available by the EUAR[1], high-level safety requirements are defined for ETCS levels 1 and 2 with precise argumentation in the Subset-91 [10]. They include global quantitative targets in terms of safety level for the whole ETCS and for its different technical parts (on-board, trackside and transmission parts), given a generic train mission profile and rail operation assumptions. They also list the safety-related functions connected to these parts and more specifically their failure modes in order to specify the list of hazards, which have to be taken into account in the apportionment of the global safety targets into sub-targets. Such sub-targets are actually not defined in the ETCS safety requirements (except for very specific component like balises, see hereafter). Indeed, target apportionment depends on the chain of failure causes proper to the supplier equipment. However, indicative failure relationships are given with functional fault trees detailed in the Subset-88 [11].

In subsection II-B, we will focus on the main hazardous events linked to the localization function and highlight their connection to the ETCS core hazard: *exceedance of the safe speed or distance as advised to ETCS*. The purpose is to show which parts of the ETCS safety analysis will be impacted when using GNSS-based systems. We will rely on ETCS level 2 that constitutes the technical basis for making ETCS evolved toward the level 3, in particular with the use of the virtual balise concept (detailed in this paragraph). Before, subsection II-A will recall essential basics on railway safety analyses, mainly to introduce key vocabulary also employed in this article. Subsection II-C will then give the safety targets today allocated to the localization-related hazards. Subsection II-D will present hazardous situations potentially caused by a GNSS based-system. We will finally discuss about how ETCS level 3 can consider them operationally.

A. Basics on railway safety analyses

Several recent works have dealt with safety analysis for complex railway systems [15]–[17] and especially for the ETCS system [18]–[20]. Approaches rely on identifying system hazards first, as depicted in the European CSM regulation. The hazard analysis aims to give a structured list of unsafe events for a system (called also feared events as they can lead to an accident). With an associated occurrence frequency and degree of gravity of consequences when the accident occurs, a hazard forms a risk. Hazards are identified from a functional analysis if the technical design of the system is not yet known, otherwise they are deduced from the system technical architecture behavior. A list of such events allows defining safety measures to be implemented inside but also outside of the system and they are reported in the safety case [21]. Thus, a global (systemic) point of view has to be adopted in a railway safety analysis, i.e. not only a system-centric point of view. Finally, actions for insuring safety against hazards can be set in a general way by:

- preventing hazard occurrence using internal safety barriers. If a hazard occurs even so, different external safety barriers are envisaged to avoid the unwanted consequence (e.g. by modifying operational conditions, using other external technical systems, by enabling human actions),
- attaining an accepted level of risk by reducing the hazard occurrence and/or the degree of gravity of its consequences,
- counteracting the causes of the hazard rather than mitigating its consequence. The aim is to avoid it or to reduce its possible occurrence to a safety target expressed with very low frequency values, namely tolerable hazard rates (THR). External triggering events and internal causes due to the technical system are investigated.

[1]In 2017, current versions of ERTMS requirements are provided on the European Union Agency for Railways website at: http://www.era.europa.eu/core-activities/ertms/pages/set-of-specifications-2.aspx

This article will concentrate on the third point and gives elements of discussion for the other points.

B. Main hazards in the existing ETCS level 2 linked to the localization function

Before presenting the localization-related hazards in ETCS level 2 and how they are counteracted to obtain today an acceptable safety level, let us remind briefly how the localization information intervenes in this system. A position is obtained indirectly through a measured distance provided by a device fitted on locomotive bogie axles or wheels, an odometer. Its errors are punctually reset with geo-referenced beacons (balises). Thus, two ways are combined to localize a train: absolute positioning by balises and relative positioning by the odometry device.

Balises are often grouped in batches from two to eight. They are placed the one behind the other on a few meter track zone and they are characterized with an internal sequence number. Such configuration has several purposes: to ensure a safe redundancy of transmitted information, to detect the direction of a train (nominal or reverse) and, when the length of a message to be transmitted is large, to send the message in several concatenated balise telegrams. If grouped, the position of the first balise in the balise group (BG) defines the location reference. To have an idea on the number of balises, in the generic train mission profile presented in [11], 400 single balises or BG are encountered per hour. For another example, considering the implemented East-Europe high speed line from Paris to Strasbourg equipped with ETCS-L2, around 3 single balises or BG are encountered per kilometers, resulting in 1800 devices. The balise subsystem is finally composed of single balises or clusters of balises at the ETCS trackside level (called also information points, noted IP) and of BTM (Balise Transmission Modules) at the ETCS on-board level.

Three main hazards related to balises have been identified (their main relationships to the ETCS core hazard are shown in Fig. 1): *corruption of transmitted message* (incorrect message received as consistent), *deletion of message* (IP not detected) and *insertion of message* (message received from an adjacent IP). Their allocated targets are presented in the next paragraph. Different techniques are employed to avoid such hazards: balises have to be sufficiently spaced between each other to avoid "cross-talk" phenomenon. It refers to the fact that a train can read the wrong message, i.e. not the one of the BG on which it passes over but the message of another close BG (cf. [13]). If cross-talks still happen, to protect against them, IP can be internally marked as linked, i.e. a "linking" information is registered into the balise to anticipate the next coming IP. Thus, when checking the linking data, if the on-board system reads a balise from an adjacent track with a not pre-announced identification number, it is able to react accordingly by rejecting the balise (and waits for the following IP) or by braking the train. The linking information also permits to determine whether an IP has been missed, i.e. not found within the expected time window.

The odometry device measures train distance from the last IP (named also LRBG for *Last Relevant Balise Group*) thanks to a dead-reckoning method. It relies on velocity data that often come from angular speed sensors located on locomotive wheels. Inaccuracy of such device depends on the intrinsic characteristics of the device that can lead to small errors but that accumulate in time if they are not reset. It depends also on unpredictable environment conditions, in particular bad adhesion conditions between the wheel and the rail. These conditions can generate wheel slipping during train start or wheel blocking during train braking [22]. Resulting inaccuracies can lead to *incorrect determination of train position relative to LRBG*. Such hazard is represented by Gate 58 in the functional fault tree of Fig. 2 that also shows the main relationships between this hazard and the ETCS core hazard.

Readjusting the long-term drift of the current odometry device no longer by balises on track but by a GNSS receiver embedded in train is entirely possible, providing thus positioning markers at higher frequency. This appears as an interesting solution to implement the moving block principle without trackside equipment. In such a way, GNSS receiver play the role of a virtual balise (VB), functionally equivalent to a physical one (or to a balise group). It permits to keep existing ETCS specifications and reference architecture while introducing a continuous localization mean through satellite. Some adaptations of the ETCS documentation will be obviously necessary with, for example, the definition of specifications relative to an embedded module reading VB (in particular, how VB are detected compared to recorded locations in a digital geographic database). But specifications relative to the BTM can serve as a basis. The presented functional fault trees will also have to be adapted. This VB concept has been investigated in lots of European research projects [24] and their safety aspects begin to be explored in recent works such as in NGTC [23] and STARS projects [25]. However, VB functionalities with GNSS are not available in areas where satellite signals are blocked like in tunnels and will still need physical balises in specific locations where GNSS positioning is not performing. This concept will also depend on the interaction between the physical and virtual balises, in particular if the linking information is used.

To go further in the ETCS evolution toward level 3, several other projects have tested different on-board localization solutions. A review of projects and their solutions is respectively detailed in [24] and [26] to show their advantages and drawbacks. To overcome possible GNSS signal obstruction and interference, GNSS hybridized with other devices than the odometer is recommended. In particular, the use of devices not mounted on train driving axles is interesting to eliminate errors due slip and slide phenomena, like inertial navigation system (INS) or Eddy current system. As ETCS-level 3 implementation is open and not yet fixed by requirements, GNSS combined with INS constitutes an advantageous solution for implementing this level. Section III focuses on the safety analysis of such systems. In this section, before addressing hazards due to GNSS that impact ETCS operations, existing targets defined for the ETCS hazards due to current localization techniques are set out.

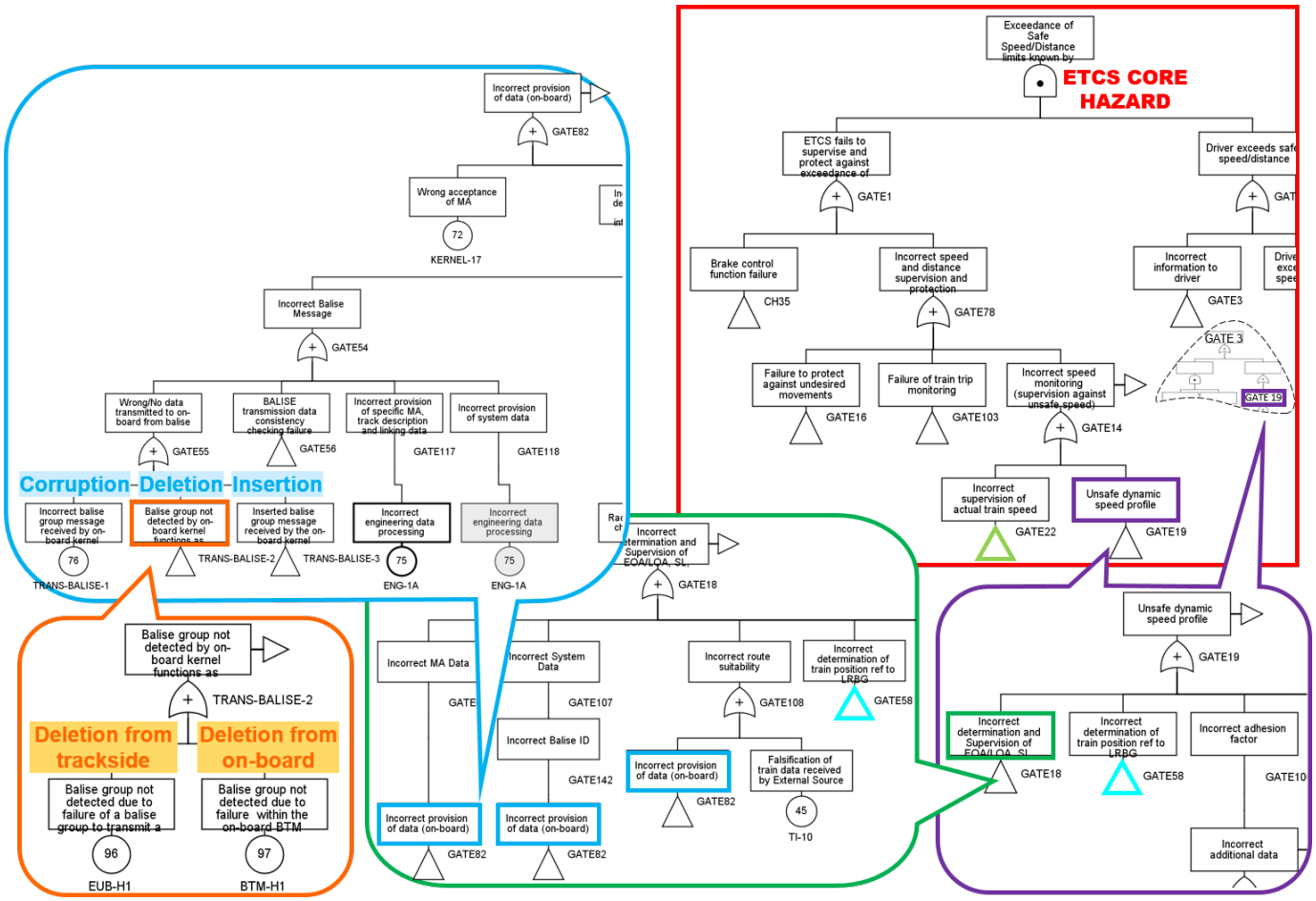

Fig. 1. Main parts of the generic functional fault tree proposed in [11] including failures related to the absolute positioning via balise in ETCS level 2

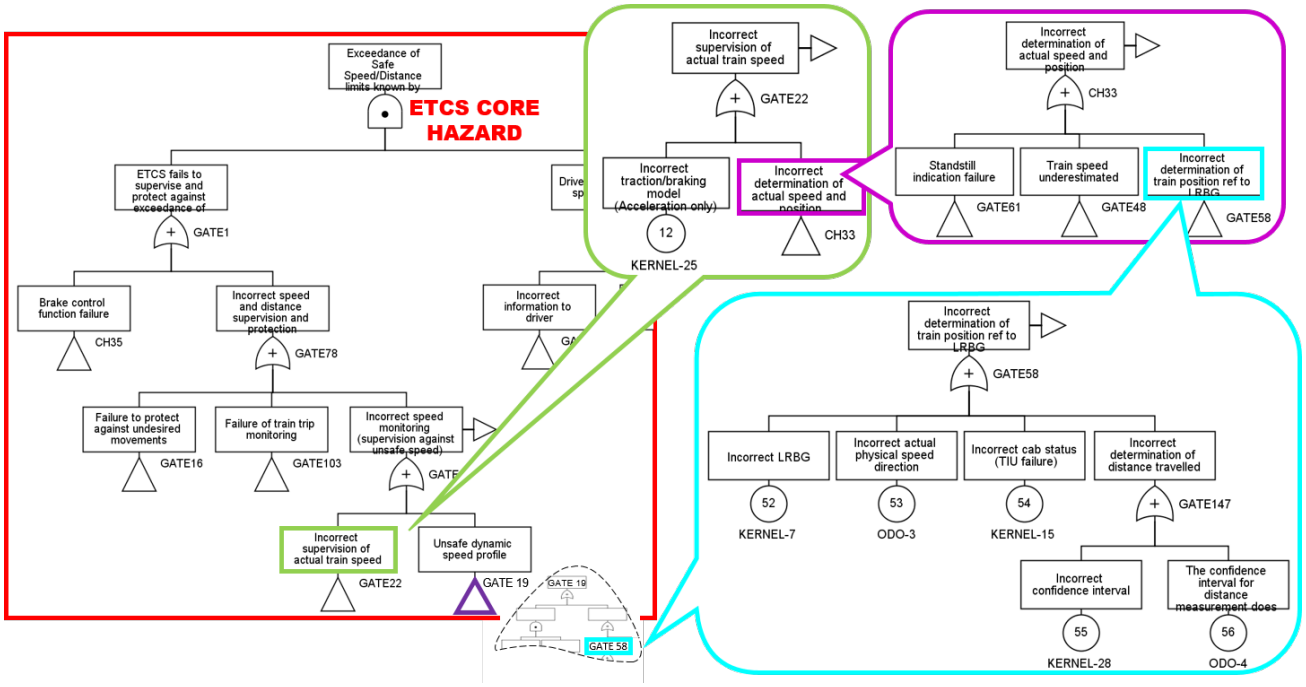

Fig. 2. Main parts of the generic functional fault tree proposed in [11] including failures related to the distance measurement function in ETCS level 2

C. Current targets set to localization-related hazards and discussion on their evolution

In terms of targets, the TSI-CCS [3] refers to a value of THR reaching 10^{-9} failure per operating hour for the entire ETCS on-board system. This target is apportioned to the ETCS constituents in the case of ETCS-level 1 and level 2 in [11], especially to the failures relative to the localization like the balise failure modes: *corruption*, *deletion* and *insertion* of messages. No target allocation has been undertaken further in the case of the level 3. Table I presents the allocated targets for the *deletion* and *insertion* failure modes (on-board and trackside parts have been considered distinctively for the first one). Risk reduction target for the *corruption* failure mode is finally considered as negligible since cryptographic safety code is assumed to bring sufficient protection.

The risk evaluation and assessment CSM [2] stipulates that a function, which can potentially directly lead to a catastrophic consequence if it fails, requires a THR of at most 10^{-9} failure per operating hour. This target is today often the unique target retained for the localization function. However, this very constraining requirement can be moderated. It is accepted that this risk reduction weight refers to the technical system plus actions of external safety measures or operational actions that attenuate the possible consequences of out-of-bound positions. This allows relaxing the safety constraint on the localization function.

When taking such existing targets into account, an issue remains for undertaking the sub-apportionment of the allowable THR to the on-board localization sub-functions based on GNSS. This task potentially implies transferring the THR apportionment of the trackside part, for which some functionalities will be removed, to the on-board part. It remains an issue because it will depend on the operating mode of the train control system. For example, the *Start Of Mission* procedure in the *Stand-By* ETCS mode is particularly demanding in terms of accuracy since, often, no reliable history on localization data are known at the start of the train. It is less demanding in term of risk reduction as the localization function has time to obtain a first fix (position) over several minutes [27] (concerned operating profiles will be addressed in next subsections).

Another issue, that the methodology proposed in the article wants to answer, is once targets are laid down, achievement of THR needs to be demonstrated from the architecture retained for realizing the localization function. Hazard occurrence related to the localization also depends on the train situation on the track, therefore the demonstration should be divided according to the different potential accident scenarios. The target allocation and the target demonstration are in fact two different tasks to be processed. The target retained in the rest of the paper is 10^{-9} h^{-1}. A SIL (*Safety Integrity Level*) can then be demonstrated as there exists a THR / SIL correspondence, but only when the quantitative requirements associated with the different SIL are examined [28]. SIL verification also implies the demonstration of the control of systematic failures which are not quantifiable.

TABLE I
ETCS BALISE REQUIREMENTS [10] [13]

Hazard description	Target
Failure of balise group detection (ETCS on-board)	THR of 10^{-7} dangerous failure /h
Failure of a balise group being detectable (ETCS trackside)	THR of 10^{-9} dangerous failures /h (individual balise unavailability is $< 2.10^{-5}$ /h)
Cross-talk of balise group (on-board and trackside)	THR of 10^{-9} dangerous failures /h

D. Hazardous situations potentially caused by a GNSS based-system

1) Features of causes: Hazardous situations (HZS) in railway operation potentially generate train accident scenarios (a collision or a train derailment, for example). They can be caused by failed train positions. GNSS errors are part of the HZS causes related to the integrated navigation solution. This subsection will not detail the error sources since they can be found in literature as in [29]. We can just retain that there exists nominal GNSS errors that keep position error (PE) in user bounds and otherwise, errors leading to position failures ($PE >$ user tolerance). PE is the difference in meters between the true position and the calculated position. PE is naturally usable for the entire integrated solution. Three types of problems characterize the HZS causes stemming from an integrated navigation solution:

- Hardware failures. These are material faults due to the embedded localization sensors.
- Software failures. These are problems related with the data fusion algorithm that gives out-of-bound positions due to a wrong configuration or evolution of the parameters of the system equation model. These may be wrong digital data coming from a track database employed for map-patching and/or from satellite augmentation systems used to improve position accuracy (if such means are employed). These may be faults undetected by an implemented monitoring mechanism when it should have to detect them.
- Faults in GNSS signal. These come from perturbations in signal propagation mainly due to environment elements such as tunnels, rail canyons, stations, foliage, etc. They also come from corruption of data carried by a signal.

The disruption of the GNSS-provided service when insufficient number of satellite signals are received, is not a source of HZS when other devices conjointly run to provide positions. There is also no HZS when no devices run because of hardware failures, as the absence of position is easily manageable in safety. A hybridized solution is of interest when a train meets masking areas regularly. The temporary operation of this solution without the GNSS receiver must be on a limited period of time since sensors like tachometers, odometers, or INS have errors that accumulate with time.

2) Different operating profiles in which the HZS can occur: To show the iobtainmpact of aforementioned causes, remind that train movements are today realized in safety with the

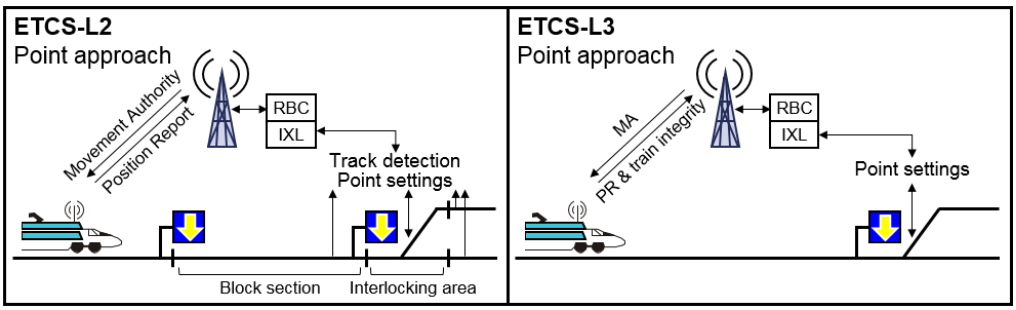

Fig. 3. Illustration of interlocking system and radio messages exchanged in ETCS L2 and L3

control/command and signaling system thanks to three main functions:

i) to assign train routes by insuring no conflict between train movements,
ii) to prevent train over-speed,
iii) to prevent a train entering into an unauthorized section (overrun).

ETCS-Level 3 will allow the implementation of on-board functions *ii)* and *iii)*. For function *i)*, it refers to the *interlocking system* that aims to establish and maintain routes in area where conflicts can exist (junction, bifurcation, crossing). In detail, after verifying route clearance, the interlocking system preempts a route for a given train and locks –according to a safe logic– each concerned infrastructure part until all consists have passed over all track sections reserved for this route [4]. For example, it fixes the states of the point machine to select a given itinerary in an interlocking area. So it gets in input train occupying information from trackside equipment (e.g. obtained from axle counters or track circuits). It outputs commands to trackside devices, often based on relays to make automatic settings and, it gives information to the train on the block section until which it is allowed to proceed. Latter information constitutes the so-called *movement authority* (MA). The MA is given thanks to radio messages by the *Radio Block Center* (RBC) to the on-board unit in the case of the ETCS-Level 2 or 3 (cf. Fig. 3), or, in the case of ETCS-Level 1, thanks to signals and switchable balises (different to the geo-localised balises) to the train driver [30]. Interlocking systems (IXL in abbreviated form) are traditionally trackside national systems based on national signaling rules, however they are also subject to discussions in order to harmonize their functioning and their interfaces, especially with the ETCS components (cf. the past INESS project and the current EULYNX initiative, which aim to formalize models leading to requirements for a future common interlocking system [31]). Therefore, the technological changes striving for employing GNSS in ETCS-Level 3 will also affect the interlocking system logical rules in order to operate according to the moving block principle. With all signaling sub-systems considered, failures of the GNSS-based localization function will have impacts principally on the following operating profiles:

- running the *Start of Mission* ETCS procedure to obtain the train position when the vehicle has been energized,
- controlling train integrity ; the train integrity is a function that verifies if the train did not lose any wagon,
- train spacing ; trains are separated with a safety distance which is determined by the movement authority ; a MA is needed in *Full Supervision*, *Limited Supervision* and *On-Sight* ETCS modes,
- operating in *Staff Responsible* ETCS mode ; in this case, the driver has more responsibility in assuring safety, for example in degraded operations,
- moving along on a point ; tracks are joined at points –also called switches or turnouts–, point equipment can guide trains onto different tracks depending on equipment settings,
- moving along on a diamond crossing ; it is an intersection of two rail routes where no point equipment is needed.

The next subsection focuses on the train spacing case. It leaves interlocking areas aside as such areas rely on country-related heterogeneous rules.

3) Dangerous train separation operation due to localization problem in ETCS-Level 3 context: Track occupancy management according to moving block principles are modeled in several studies for verifying formal and logical safety properties related to train operation (or reciprocally, to verify inconsistencies). For example, “the intersection of moving blocks of two different trains is always empty” is a safety property analyzed using formal Z notation in [32]. Causes leading to obtain wrong size of moving block or causes hindering the on-board reception of information in order to adjust the size of a block, are another safety issue to be analyzed. Indeed, they can engenders hazards such as a too small protection zone placed around a train or a zone placed incorrectly around it. [33] has examined causes of radio reception delays endured by track-to-train or train-to-track messages due to errors in the used telecommunication medium (GSM-R) and has studied their impact on moving block operation in the train spacing case with generalized stochastic Petri net models. However, errors in localization data carried by the train-to-track messages (called *Position Report* or PR in ETCS and referring to the locomotive position) are not really addressed. Only is highlighted that the RBC has to consider the obsolescence of a received PR when generating afterwards a Movement Authority (i.e. the train continues to progress after sending its PR). The RBC has also to consider the fact that the resulting MA will not reach immediately its destination due to radio delays. Possible uncertainties in the train position

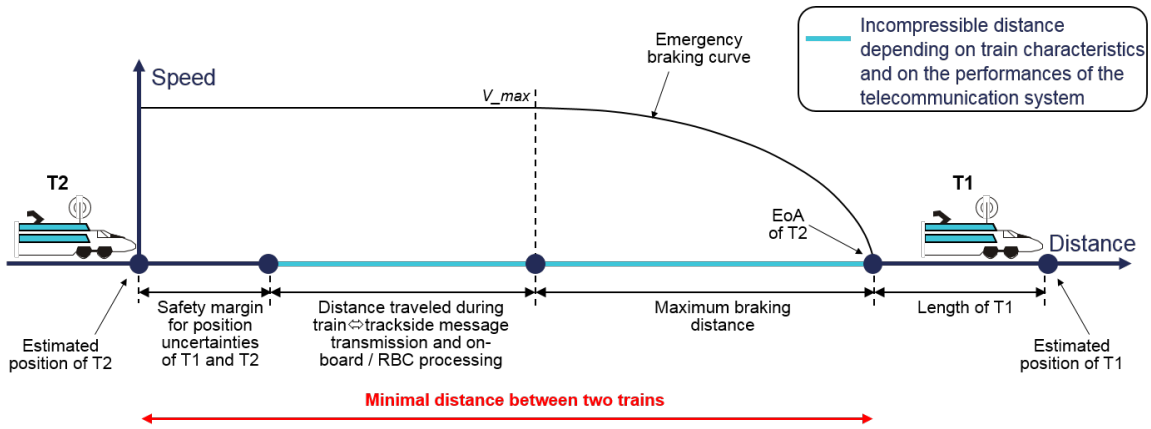

Fig. 4. Illustration of safety distances intervening in train separation operation

data are of course considered in moving block operation but only by taking a safety margin to absorb them. This margin is often considered in a conservative way for separating two trains with a sufficient distance in order to avoid a collision [34]: the braking of the train behind will be triggered according to the last known position of the ahead train, this one being projected in a situation where it has encountered an unexpected event and has stopped. Nevertheless, if a position is out of the limit of this margin due to specific errors (here those due to new technological devices based on GNSS), there exists a critical safety problem that can lead to an accident if this situation is not revealed. Fig. 4 illustrates the necessary minimal distance between two trains (comprising the braking distance and the other additional distances taken for safety reasons). The railway line is assumed with no gradient, T2 has constant speed and then takes a constant deceleration when it received the order to stop. Such assumptions are kept in the rest of the paper.

In ETCS-Level 3, the MA does not refer anymore to the allowed block section occupancy but to the distance the train is allowed to travel (with respect to its last position transferred to the RBC). For that, a limit of the zone the train must not exceed is included in the MA and is called *End-of-Authority* (EoA). The main risks when operating in moving block can then be described using this EoA notion. A risk can occur when:

i) train driver errors or equipment failures imply that the train goes beyond an EoA without having a new MA,
ii) trackside system provides a dangerous EoA to be displayed to the driver (i.e. leaving an insufficient distance for a safe braking),
iii) the 'Train-EoA distance' supervised on-board is incorrectly estimated and leads to the absence of reaction of the ETCS protection function when it should.

The safety evaluation approach of section III will focus on the case *iii)* on which the GNSS-based localization system failures may have dangerous impacts (we will neglect the other cases). Rather than reasoning with the minimal Train-EoA *distance* in red on Fig. 4, we will consider in the following the *time* taken by a train to travel this distance (the minimal headway).

Moreover, the localization system will be considered, in the next sections, as being a hybrid GNSS/INS solution given advantages presented before for trains. We will assume this system is equipped with a fault detection function, which is a safety barrier essential for safety-critical applications of navigation [35]. A detection mechanism adapted to hybrid solutions will be used according to given principles that will be described. Such mechanism aims at monitoring the *localization integrity*, a notion stemming from the aeronautical domain (concept slightly different from the *safety integrity* largely used in the railway domain), whose characteristics will be briefly reminded in this section. We will also assume this system does not undergo hardware failures (sometimes called fault-free case) and it will not integrate a digital map of the track or an augmentation system. Even if such means can enhance the system accuracy, the objective of the paper is to focus more on the methodological possibilities for evaluating safety given considering an operational scenario than to find an optimal technological solution. To evaluate the safety of the considered train separation operation using the GNSS-based localization solution, the Hazardous Situation (HZS) occurrence has to be quantified. We will precisely explain how HZS are determined and the way to quantify associated safety criteria using the localization integrity risk.

III. Evaluating Safety Using Extended Integrity Data

A. Integrity concepts in the aeronautical domain and discussion on their use in the railway domain

Integrity is a safety performance defined in aeronautical domain for navigation systems. It refers to "a measure of the trust that can be placed in the correctness of the information supplied by the total system" [36], which is probabilistic by nature. It refers also to the ability of the system to alert external entities (other systems or an user) when the localization is out of tolerance: "Integrity includes the ability of a system to provide timely and valid warnings to the user". On the one hand, the integrity performance is rather expressed with its opposite the *integrity risk* (probability IR). On the other hand, the ability of a system to insure integrity (i.e. to provide alerts) necessitates the use of particular parameters, which are standardized as well:

i) the *Alert Limit* (AL in meters) refers to "the error tolerance not to be exceeded without issuing an alert" (user requirements define often the tolerable position error PE with its horizontal and vertical components HAL and VAL),

ii) the *Time-To-Alert* (TTA in seconds) refers to "the maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the equipment enunciates the alert".

Actually, PE cannot be observed as the exact position of the user receiver is unknown (except in test conditions with reference measurements). Consequently, processes that monitor the localization integrity, estimate a statistical error bound, a *protection level* (PL in meters), which represents the maximal position error guaranteed with a given confidence level. Such level is expressed thanks to a very low probability of misleading the user. This probability has a negative power of ten and represents, finally, a probability of missed detection P_{md} that refers to the integrity risk. If the monitoring process states $PL > AL$, the localization system is considered, in aviation domain, as unavailable for the intended phase of mission. Note that in the railway domain, a large error bound could potentially be managed during train operation by imposing specific operational constraints to allow train to continue their mission rather than to brake. Indeed, if it is sure the train is included in a given perimeter, even large was it, the safety distance between trains can a priori be adapted as a function of this bound (cf. union of confidence intervals in [37]).

A lot of error detection mechanisms exist for GNSS and rely mainly today on differential techniques (locally or widely deployed like with the EGNOS augmentation system) or RAIM algorithms (Receiver Autonomous Integrity Monitoring). We will not detail the numerous possible techniques since they are synthesized in references such as in [38]. Globally, they are based on statistical techniques reasoning either in position domain or in pseudorange domain. In the first domain, the evolution of the estimated position outputs of the navigation solution is monitored to identify probable position failures. In the second domain, the evolution of the pseudoranges (the measured satellite-to-receiver distances) is monitored to control the presence of outages in signal reception that lead to position failures.

The TTA notion is difficult to understand by railway safety analysts for who a failure or an error is present or it is not. They assign probability to its occurrence but not to its duration. Probability per hour exists but it does not deal with an event that lasts one hour but with an event that can appear during this period. In aeronautics, for GNSS, TTA is an operational time that includes the aggregated time spans taken by each monitoring part, distant from the user, to identify an unsafe condition. For example, ground-based infrastructures like the EGNOS RIMS (Ranging Integrity Monitoring Stations) take time to analyze satellite signals, Master Control Centres' facilities also take an additional time to process data. TTA also includes the delay to transmit an alert message in order to inform the user. If the monitoring is rather directly at the user side with a detection algorithm integrated in the user equipment, like a RAIM, the processing is quasi-instantaneous.

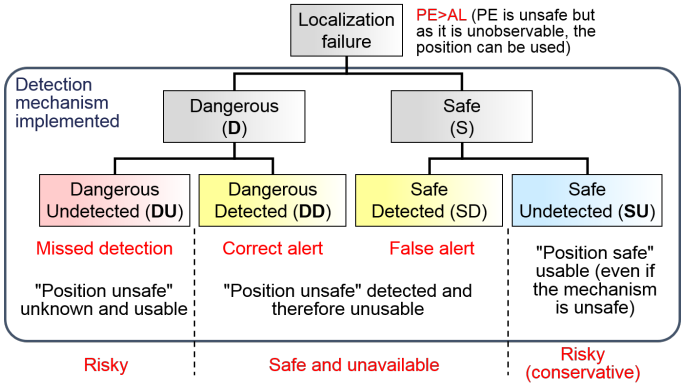

Fig. 5. Classification of the localization states

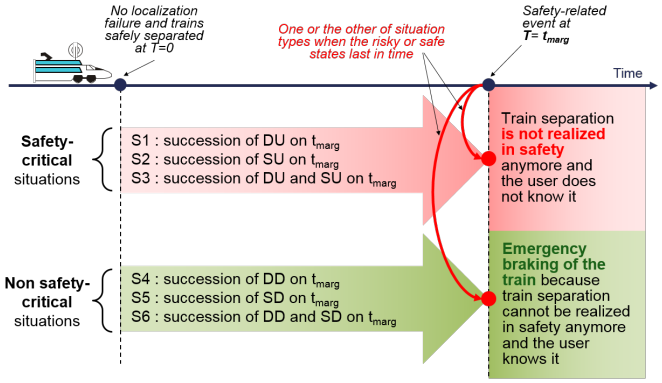

Fig. 6. Railway situation types according to localization states

Consequently, an alert can be raised immediately. However, in this case, the maximal delay between the appearance of an unsafe condition at the input of an user receiver and the announcement of an alert by the monitoring can also be considered, for characterizing the TTA (while remaining consistent with its definition) by: the time from which the monitoring does not react when it should until it ends up reacting. This reaction has to happen just before TTA to respect user requirements otherwise the non-detection becomes dangerous for the application. We will explain later, according to this point of view, which situations are related to safety or risk of a GNSS-based localization system. We will propose in Section IV possible requirement for AL and TTA values in train separation operation of ETCS-Level 3.

B. Railway situations related to safety or risk with regard to the localization integrity

Following the approach in [39] and [40], failures of a GNSS-based localization system equipped with a detection mechanism, are first classified in safe or dangerous states depending on the states of the detection mechanism (missed detection and false/correct alert) as summarized in Fig. 5. In this figure, the *dangerous undetected* (DU) event is trivially indicated as risky. In the aeronautical domain, the *safe undetected* (SU) event is often considered also as risky because, even if the error remains below a tolerable error limit, the detection mechanism does not operate correctly and may cause

problems later ; it is a conservative point of view. This can be observed for example in some Stanford diagrams used to represent the different states of a detection mechanism (in testing conditions where PE is known) on a graph with PE in horizontal axis and PL in vertical axis. The risky area of the graph is often the whole part below the diagonal such as $PL < PE$ (i.e. PL does not correctly bounds PE) even in the case where $PE < AL$ [41].

Here DU or SU events are seen regardless of their occurrence or duration over time. It should be pointed out that a failure that lasts for one second is unlikely to have an effect on the train separation case, especially when a related safety margin for localization between trains (cf. Fig. 4) traveled with a timeout noted t_{marg} in Fig. 6, is considered. Therefore, the DU and SU events create a safety-critical situation (HZS) only if they last according to the conditions shown in Fig. 6 for situations $S1$, $S2$ and $S3$. These conditions imply that either DU or SU events come one after another long enough to exceed the safety timeout. In that case, this time duration has to be taken into account to define the three HZS and appears to be an operational railway constraint, even a railway requirement, exported on the GNSS-based localization system. It easily comes into view that the duration t_{marg} has the same purpose than the TTA defined at the end of Subsec. III-A. Note that detected events (DD and SD) allow the train to be brought to a safe situation ($S4$, $S5$ or $S6$), i.e. their knowledge allows the train MA to be canceled if they last until t_{marg} bringing the train to a halt within a given braking distance.

Hereafter, we will propose a way to evaluate a probability estimation of the HZS highlighted in this paragraph by using an estimation of the integrity risk IR linked to the occurrence of $S1$, $S2$ and $S3$. Given the discussions made up to now, IR will be expressed depending on the occurrence of DU and SU states. These states depend on specific parameters of a detection mechanism. This IR estimation will be translated into a safety criterion understandable in the railway domain.

In the next subsection is addressed an applicable monitoring algorithm for a localization system architecture hybridizing GNSS with proprioceptive sensors. The algorithm, summarized from [9], will permit to define an extended integrity risk usable in the railway domain and adapted to hybrid architecture composed of a GNSS receiver and an inertial system (INS).

C. Proposition of an applicable integrity monitoring mechanism

The specific algorithm of integrity monitoring is developed in regard to known errors undergone by a GNSS/INS integrated system used in a railway environment (cf. Subsec. II-D). It is worth here to notice that mainly two GNSS/INS integration solutions are possible [35]: the embedded and the aided ones, using what is called respectively a tightly or a loosely coupled architecture. In the embedded solution, the GNSS receiver is an integral part of the INS system as GNSS raw data (the pseudoranges measured by the receiver) are directly integrated into the positioning process. In the aided solution, GNSS data are processed independently by the receiver and the resulting position is used to update the INS one after given time intervals. The algorithm of the implemented integrity monitoring is based on a tightly coupled architecture (an example will be given in section IV) and it aims at detecting:

- instantaneous biases that can corrupt the value of pseudorange estimated by the GNSS receiver in such a way that an aberrant position error is obtained (such biases arise when satellite signals are deviated on elements of the surrounding receiver environment),
- progressively growing errors (called later PGE) coming from the inertial part and leading to out-of-bound conditions.

As both types of error can lead to an out-of-bound position, they can also be called faults. The different steps of the algorithm are described in Alg. 1 which can be split into two phases: the first one integrates the detection methods adapted to the previous mentioned errors and the second estimates the protection level (PL is estimated when no alert is triggered after the running of the two error detection processes). The following subsections describe the main elements of these phases.

Algorithm 1 Integrity monitoring proposed for a hybrid GNSS/INS localization solution

Require: INS and GNSS measurements, $P_{false-alarm}$, AL
  for the duration of a given mission **do**
    Extraction of residuals from measurements
    Save residuals in a database
    Run *Chi-squared test* for instantaneous biases detection
    Run *Difference test* for PGE detection
    if Instantaneous bias detected **or** PGE detected **then**
      Alert of the presence of a possible out-of-bound position
    else
      Calculate PL
      if $PL > AL$ **then**
        Alert of the unavailability of the integrity monitoring
      else
        Use the position
      end if
    end if
  end for

1) Phase of detection: This phase is based on the estimation of residuals. Residuals are determined by the difference between the measurement of different observable quantities that expresses the system state evolution (measurement vector), and their prediction computed by an estimator (an Extended Kalman Filter will be used and explained in the Section IV). For the detection, the normalized sum of squared error ($NSSE$) is a test variable that is largely used in satellite navigation monitoring, especially in RAIM, and is obtained using the residuals on pseudoranges. This variable is commonly supposed to follow a Chi-squared distribution as the errors affecting the measurements are assumed to be Gaussian [42]. Statistical tests exist to detect if the distribution is central or non-central. In the last case, the shift reveals the presence

of a potential position failure. Here, to distinguish the type of error that leads to a failure, the proposed algorithm integrates two different statistical tests: a classical Chi-squared one for instantaneous bias detection and a test called *difference test* imagined by [44] for slowing growing error (SGE) detection. This last detection is initially thought only for GNSS measurements that can in particular cases suffer from SGE ; but due to the nature of INS errors that accumulate with time, the method has been reused here for PGE detection.

Basically, a statistical test is based on the rejection or acceptation of a null ($H0$) or an alternative hypothesis ($H1$). Here, $H0$ refers to a central distribution and $H1$ a non-central distribution. To set the detection threshold of the test in order to determine which hypothesis to retain, a requirement on the probability of false alarm (P_{fa}) is used. The table II describes $H0$ and $H1$ for each detection method.

The *difference test* uses the SSE variable (Sum of Squared Error), more exactly a difference of SSE at different instants called $Dif_{\Delta t}$. Several Δt can be fixed to detect different evolution (rapid or slow) of PGE. Three points in time separated by Δt are ideally recommended to detect such evolution, so three detection thresholds are required. In [43], the distribution of $Dif_{\Delta t}$ is approximated by a normal distribution $\mathcal{N}(\mu_{Dif}, \sigma_{Dif})$.

In the *Chi-squared test*, the quantity $m - n$ is the degree of freedom of the Chi-squared distribution (χ^2) and it is an integer equal to the difference between: the size of the measurement vector and, the size of unknowns of in the state vector linked to measurements. λ is the non-centrality parameter of the χ^2 law.

TABLE II
HYPOTHESES AND THRESHOLDS IN DETECTION METHODS

Test	Hypotheses	Thresholds
Chi-squared test	$H0$: $NSSE \sim \chi^2_{m-n}$	$thres_{bias} = (\chi^2_{m-n})_{1-P_{fa}}$
	$H1$: $NSSE \sim \chi^2_{m-n,\lambda}$	
Difference test	$H0: Dif_{\Delta t} \sim \mathcal{N}(0, \sigma_{Dif})$	$thres_{PGE_{1,2,3}} = \mathcal{N}(\mu_D, 1)_{1-P_{fa1,2,3}}$
	$H1: Dif_{\Delta t} \sim \mathcal{N}(\mu_{Dif}, \sigma_{Dif})$ with $\mu_{Dif} \neq 0$	

2) Phase of Protection Level estimation: While the previous two detection methods reason in the measurement domain, the protection level (PL) is linked to the position domain by giving a bound on the position error (PE) in output of the navigation system. Several protection level computations exist, their choice depends of the importance given to the impact of measurement noises on the position error or on the residuals [42]. In absence of information about the impact of measurements noise on the residuals, it is considered as not negligible. In consequence, a PL expression corresponding to this consideration is given by Eq. 1, where the quantity $\sigma_{\delta z}\sqrt{\lambda}$ is often called minimal detectable error and represents the sensibility of the detection, δz refers to the whole residual vector (cf. appendix) and λ to a non-centrality parameter. $max(SLOPE)$ represents the steepest slope linked to the measurement that has the smallest influence on the test statistic ($NSSE$ or Dif_{Δ_t} according to the detection test) while causing a high position error. j is the j^{th} source of measurement.

$$PL = \max_j(SLOPE_j) \cdot \sigma_{\delta z}\sqrt{\lambda} \quad (1)$$

It is a classical form of PL used in RAIM algorithm for GNSS instantaneous bias detection when $\sigma_{\delta z}$ refers to the standard deviation only concerning the residuals on pseudorange errors, the pseudoranges being not corrected by other system. It goes under the assumption that a bias only exists in the j^{th} satellite measurement and the others are free of noise [43]. PL can then be compared to a required AL in such a way that the algorithm raises an alert or not.

In summary, to define an applicable integrity monitoring mechanism for railway localization systems, a GNSS error detection process (taken from classical RAIM known in GNSS community) has not only been employed but also a PGE detection process. Both are then followed by a PL calculation. The associated algorithms are based on measurement residuals obtained from an Extended Kalman Filter that handles multisensor systems. These processes lead to the introduction of specific integrity parameters compared to those set out in Subsec. III-A that can serve for quantifying the integrity risk IR. Here, it is worth pointing out that the goal in this subsection was not to built an efficient and robust detection function but to show how this can lead to a comprehensible safety evaluation approach for railway actors. This safety approach will be presented after describing which criteria can be assessed.

D. Type of safety criteria usable in the railway domain

Two main criteria are defined in the IEC 61508 standard, which is the international generic and multi-domain standard for functional safety of E/E/PE safety-related systems (Electrical/Electronic/Programmable Electronic):

- the *probability of failure on demand* (PFD), which is a value that defines the probability that a system realizing the function fails to respond to a demand (the demand being not greater than one per year),
- the *frequency of dangerous failure per hour* (PFH), which is an average failure frequency over a continuous period of the function utilization (the dangerous failure of the system is considered leading directly to a hazard in this standard).

The three railway standards EN50126, EN 50128, and EN 50129 are domain-specific standards and, as they are adapted from the generic one, they allow the use of properties defined in the IEC 61508 “umbrella” standard. For railway safety-related systems, since the ability to answer to a demand is often considered as being continuous, the PFH is more adapted for safety evaluations.

Tolerable Hazard Rate (THR) is a criterion that has been only introduced in the railway standards. It is not only linked to the loss of the ability of a system to protect against damages (called safety system) or to a system malfunctioning provoking critical consequences (called safety-related system), but to an identified operational scenario (among others) that leads to

a potential accident, i.e. the considered system failure is a cause triggering identified hazards (overspeed, train running with doors open, etc.). A THR requirement is often allocated to the hazard provoked by a system after taking into account the risk-reducing weight provided by external barriers that are put in place to control the risk linked to the hazard. Thus studies focus on Hazard Rate (HR) evaluations by handling system failure causes with for example fault tree or event tree methods to determine if HR are tolerable or not.

In the EN 50126 standard (in the current used version and in the future version to be published in the coming months) are listed, in annex, examples of safety performance parameters such as: *Mean Time Between Hazardous Failure* ($MTBF$), *Mean Time Between Safety System Failure* ($MTBSF$), *Hazard Rate* ($H(t)$), *safety-related failure probability* ($F_S(t)$), *probability of safe functionality* ($S_S(t)$), *probability of wrong-side failure* (p_{wsf}), *Time to Return to Safety* ($TTRS$). Some works do not directly refer to an abbreviated criterion name but to a textual expression. For example, in [27] a "rate of undetected dangerous failure over a mission time" is mentioned but finally, this refers to a PFH when the rate is brought back to a mission time of one hour. p_{wsf} and PFH are kept for the approach presented below. PFH is of interest to determine a *Safety Integrity Level* used in the railway domain since it exists a PFH / SIL correspondence according to the IEC 61508 standard.

E. The safety appraisal approach to express the HZS probability with the extended IR

For this approach, the idea is to express p_{wsf} and PFH according to IR_{extend} and on a duration corresponding to the whole system mission time. This supposes a long observation duration of the system in operation to derive statistical values. Subsequently, a four step process is defined as follows:

Step 1: Identification of risky localization events: DU and SU events have to be identified in the data set obtained during experiments realized on rail tracks. For that, conditional statements encompassing Boolean expressions can be set down. These statements are defined depending on alert events delivered by the fault detection process. SU is recognized when $(PE \leq AL)$ and $\big((PL < PE)$ and $test_{bias} = false$ and $test_{PGE} = false\big)$. DU is recognized when $(PE > AL)$ and $\big((PL \leq AL)$ and $test_{bias} = false$ and $test_{PGE} = false\big)$. $test_{bias}$ and $test_{PGE}$ are two Boolean variables that are true when an instantaneous bias or a PGE is respectively detected, and false otherwise. Trials with the localization system have to make available reference and estimated positions in order to know PE.

Step 2: Estimation of p_{wsf}: For aeronautical and railway domains, wrong side failures for a localization system can be considered when risky events arise (cf. Subsec. III-B), thus $p_{wsf}(t) = P_{DU}(t) + P_{SU}(t)$. When considering a set of localization data obtained during a train run on a given itinerary, namely a scenario, risky localization states can be identified at each discrete instant t_i of the whole scenario time period T_m (the mission time) following Step 1. i is an integer for the i^{th} time step and T_e is the time step size such as $0 \leqslant i \leqslant int(T_m/T_e)$ (the time unit is supposed in seconds in the following). By making DU and SU events undifferentiated at each discrete time such as $A_t = \{SU_t \cup DU_t\}$, an average value of p_{wsf} is estimated on T_m according to Eq. 2 (denominator is in fact $int(T_m/T_e)$).

$$p_{wsf_{avg}} \approx \frac{\#\text{ of time } A \text{ is observed}}{total\ \#\text{ of time steps}} \tag{2}$$

Step 3: Estimation of IR_{extend}: Events linked to Integrity Risk can be considered when $S1$, $S2$, $S3$ situations arise (they refer to HZS in Subsec. III-B). An average value of IR_{extend} is estimated on T_m with the average number of HZS occurrences. These ones depend on the appearance of a DU or SU event (i.e. A event) at t_i and also on the prolongation of the risky state between t_i and $t_i + TTA$, more exactly between t_i and $t_{i+int(TTA/T_e)}$). A formulation of $IR_{extend}(t_i)$ is shown in Eq. 3 (with A_{t_j} assumed independent). In Eq. 4, an approximation IR_{extend} is derived with the average number of $S1$, $S2$ or $S3$ occurrences on a scenario. Note that when repeating the same train run to obtain several scenarios with different position estimations, an average value of IR_{extend} can be calculated at each instant in order to get an estimation of $IR_{extend}(t_i)$.

$$IR_{extend}(t_i) = \prod_{j=i}^{i+int(TTA/T_e)} P(A_{t_j}) \tag{3}$$

$$\begin{aligned} IR_{extend\_avg} &\approx \frac{\#\text{ observed of (S1 OR S2 OR S3) on } T_m}{int(T_m/T_e)} \\ &\approx \frac{\#\text{ observed of } (A_{t_i}, ..., A_{t_i+TTA}) \text{ on } T_m}{int(T_m/T_e)} \end{aligned} \tag{4}$$

Step 4: Relation between safety criteria: Eq. 5 shows the link between p_{wsf} and IR_{extend} using the discussion in Step 2 and considering p_{wsf} is constant. From Step 3 and given PFH is an average frequency that a hazard occurs over one hour, it can be simply calculated with IR_{extend_avg}/T_m. As T_m is in seconds, finally Eq. 6 is obtained.

$$IR_{extend}(t_i) = \prod_{j=i}^{i+int(TTA/T_e)} p_{wsf}(t_j) \tag{5}$$

$$\Rightarrow p_{wsf}(t_i) = (IR_{extended}(t_i))^{\frac{1}{int(TTA/T_e)}}$$

$$PFH = \frac{3600.IR_{extend\_avg}}{T_m} \tag{6}$$

This approach needs to address an important size of data to provide precise estimation of the researched quantities. In the approach application hereafter, where the size will not be so important even if there is already a relatively large amount of data, results can show the feasibility of the proposed process. Before presenting these results, characteristics of the analyzed GNSS and INS data will be presented as well as the values serving as integrity requirements for determining correct and dangerous positions. The architecture of the considered localization system hybridizing GNSS with INS will also be detailed with the associated equation model handled by the

EKF estimator. It is worth to remarking that this system and its model constitute a non-optimized "textbook case" on which safety reasoning can be conducted.

IV. Application of the Safety Appraisal Approach in Different Operational Cases

A. Dimensioning integrity requirements considering the train spacing case

To identify the localization states contributing to integrity risk and threatening railway safety, it is necessary to dimension AL, i.e. the tolerable limit on the position error PE in output of systems including GNSS. In ERTMS performance requirements [12], a limit is described by stating that for every traveled distance d by a train, the error shall be better or equal to $\pm(5+5\%\,\mathrm{d})$ meters. This depicts a drift and, consequently, refers to the relative positioning error created by odometry devices used in current ETCS implementation. A limit on the absolute positioning error is specified in ERTMS requirements specific to balises [13] by stating that it shall be within ± 1 m for each balise in vital purpose applications. For train spacing case involving two trains, both limits can be multiplied by two to obtain the position safety margin shown in Fig. 4. Finally, to define a global localization error bound consistent with the ERTMS requirements and with the considered operating case, a limit for AL can be laid down to 20 m. Such value was retained in [33] for the same case too, whatever the localization system in use. Moreover, to support this value, note that the IEEE 1474 standard dedicated to CBTC, those systems making possible the implementation of moving block for subways, recommends a maximal error of 10 m for one train.

Next, to identify hazardous situations that depend on risky state duration, the related TTA duration needs to be dimensioned. A first helpful characteristic defined in [12] is the frequency for sending position reports PR. Specific variables exist in train-to-track message structure. T_CYCLOC variable refers to such frequency and M_LOC variable can be set to define the location/moment where the train has to report its position [14]. No frequency value is given in the current version of Subset 041 (it has to be laid down by railway operators), but passed versions of this Subset mentioned a value of 5 seconds. This was also retained in [33]. A second helpful characteristic is the fact that a "location of the train head indicated in a PR shall be estimated less than 1 second before the beginning of sending of the corresponding PR" [12]. Finally, to avoid an out-of-bound error propagation from one PR to the next PR to be sent, TTA can be assigned to a value of 4 seconds considering previous characteristics. To our knowledge, no value has been proposed and argued like here in past works.

B. Description of the architecture hybridizing GNSS with INS

The architecture employed in this section is inspired by the hybridized GNSS / INS solution presented in [35] where a GNSS receiver is associated with an INS including an IMU part (Inertial Measurement Unit) and a software part. In particular, we refer to the tightly-coupled architecture for which a corrected INS solution forms the integrated navigation solution. A close-loop method for correcting INS raw errors is implemented, the principle is to use the integrated solution to correct the INS solution within the integration algorithm. The implemented EKF processes then all available measurements (regardless of their accuracy) to estimate the current value of variables of interest, especially the position. It is based on knowledge of the system and of the dynamics of the measurement devices, on the statistical description of the system noises, of the measurement errors and of the uncertainty in the dynamic model. In appendix of this article are described the dynamic model parameters (modeled in matrices $\mathbf{\Phi}$, $\mathbf{H}$), the noise statistics (modeled in covariance matrices $\mathbf{Q}$ and $\mathbf{R}$), and the state vector $\mathbf{x}$. The EKF algorithm leads to residuals that are processed by the integrity monitoring algorithm presented in Subsec. III-C. Finally, by confronting the results of the detection mechanism (alert or no alert at each time step) with the position error known in experimental test conditions, it is possible to identify and quantify hazardous situation occurrences. For illustrating these principles included in the safety appraisal approach presented in section III, positions constituting the points of several discretized vehicle trajectories are estimated by bringing different data sets in input of the localization system. These data sets are presented below.

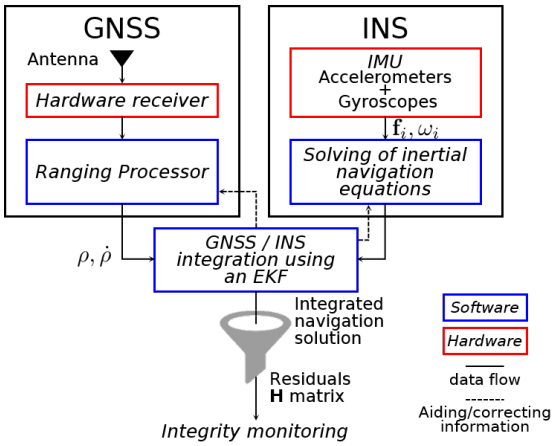

Fig. 7. Architecture of the GNSS / INS localization system

C. Description of input data

Real GNSS data are available and are recorded from a receiver mounted on a road vehicle (a test car in possession of the GEOLOC team from IFSTTAR-Nantes). Even if, such data are not obtained on a rail track, they can be considered as representative for this study since types of environment encountered by a train are almost the same than those encountered by a car (presence of vegetation, buildings, mountains, etc. around vehicles). So, perturbations of GNSS signals before being received at user level are considered of the same order. Table III presents the characteristics of two data sets recorded in Paris on the same traveled itinerary. This one is part of a dense urban environment, which is indisputably sources of perturbations for GNSS signals (presence of signal blockage, attenuation, reflection or diffraction, multipath interference).

TABLE III
2 DATA SETS OBTAINED WITH THE LEA-6T GNSS RECEIVER

	1st data set	2nd data set
Travel time (in sec)	7 117	7 529.8
# of pseudorange	288 925	312 841
Average # of satellite	8.1	8.3
Average position error (in m)	11.08	9.91
# of unavailable positions[a]	156	559
Availability (%)	99.56	98.52

[a]when less than 4 satellites are visible

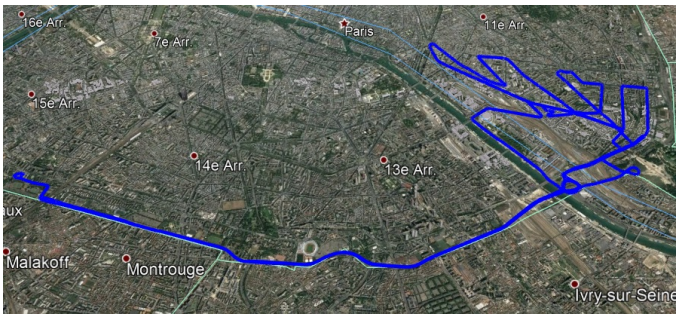

Fig. 8. Itinerary traveled in Paris

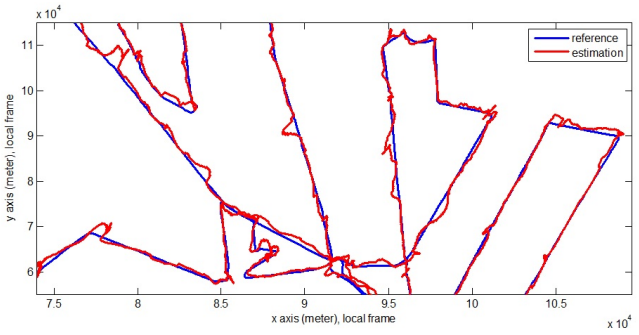

Fig. 9. Zoom on Paris itinerary

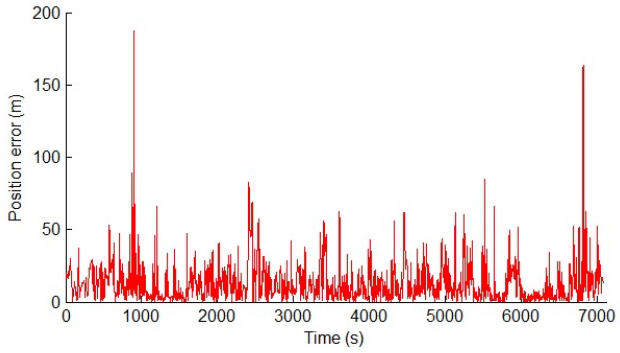

Fig. 10. Horizontal position error obtained for the 1st data set

A Ublox LEA-6T GNSS receiver is used with a time interval for records of 0.2 second. These 2 data sets are called later operational cases and their itinerary is shown in Fig 8.

Reference positions are measured thanks to a very precise and high-range quality INS mounted also on the test car, therefore each positioning error PE is known. Also, data coming from an INS of mid-range quality are needed for the purpose of this study, however such device is not installed on the car. In the absence of INS field data, simulated data are generated and used. To obtain them, common INS characteristics, the specific force $\mathbf{f}_i$ and the angular rate ω_i, are first deduced from the reference position. Noises and biases are added using the tactical-grade IMU model provided in [35].

D. Description of output errors

Positions belonging to each discretized trajectory are estimated with the GNSS / INS integrated system using Matlab® routines provided in [35] (under a free modified BSD license, Berkeley Software Distribution). INS outputs are corrected using GNSS receiver outputs every 1 second. Fig. 9 zooms on the previous figure to show at the same time the reference trajectory and the estimated position using the 1st data set. Fig. 10 illustrates the evolution of the horizontal PE for this data set in which important errors can be observed at different instants. This reveals the perturbing effect of the environment on GNSS signals. Table IV shows the accuracy for each operational case using the 95th percentile of the error distribution.

E. Description of integrity monitoring outputs

Residuals and $\mathbf{H}$ matrix calculated during the EKF algorithm processing are handled in the integrity monitoring mechanism described in Subsec. III-C to detect faults (i.e. when a threshold overrun indicates a potential position failure) or to provide a bound on PE with PL when no detection occurs (it includes missed detection). Table V details the number of detection events by distinguishing correct, false and missed detection for both types of fault: instantaneous biases on GNSS pseudoranges (IB) and progressively growing errors of INS (PGE) that can lead to out-of-bound conditions (correct and false detection events are later taken indifferently since a safety conservative point of view is adopted). Thresholds for detecting these faults have been set in the integrity monitoring using specific requirements: probabilities that an alert incoming from a given test method is false ($P_{fa} = 1 \times 10^{-7}$ for the IB detection process and $P_{fa1} = P_{fa2} = P_{fa3} = (1 \times 10^{-7})^{1/3}$ for determining the 3 thresholds of the PGE detection process). Values of test variables $NSSE$ and $Dif_{\Delta t_i}$ obtained at each instant can be then compared to their respective thresholds and, depending on the result (overrun), the monitoring will inform on-board controlling parts of the user vehicle. Table V also presents the number of PE correctly bounded or not. Values in this table show that unfortunately the implementing monitoring process taken from [9] has poor performances especially when looking at the number of missed detection

TABLE IV
POSITION ERROR CHARACTERISTICS ASSOCIATED TO EACH OPERATIONAL CASE

	1st data set	2nd data set
Average error (in m)	13.35	12.09
Accuracy (at 95 %)	37.43	32.16

TABLE V
PERFORMANCES OF THE DETECTION AND THE OVERBOUNDING PROCESSES

	1st data set	2nd data set
# of tested points (1/sec. with GNSS avail.)	7 085	7 418
Instantaneous biases		
Correct detection	0	0
False detection	2	1
Missed detection	721	514
Progressively growing errors		
Correct detection	430	212
False detection	1 409	1 789
Missed detection	497	355
Bound of PE with PL when no detection occurs		
Correctly bounded with alert[a]	2068	2037
Correctly bounded without alert[b]	1 636	2 330
Uncorrectly bounded without alert[c]	1 242	949

[a](PL > PE > AL) [b](PE ≤ PL ≤ AL) [c](PE > PL and PL ≤ AL)

TABLE VI
OCCURRENCES AND PROBABILITY APPROXIMATIONS FOR THE SAFETY-CRITICAL SITUATIONS (S1 TO S3)

	1st data set	2nd data set
HZS occurrence		
# of $S1$	170	112
# of $S2$	268	262
# of $S3$	61	45
Probability approximation on T_m seconds		
Situation $S1$	2.4 E-2	1.51 E-2
Situation $S2$	3.78 E-2	3.53 E-2
Situation $S3$	8.6 E-3	6.1 E-3
Probability approximation on 1 hour		
Situation $S1$	1.22 E-2	7.3 E-3
Situation $S2$	1.92 E-2	1.71 E-2
Situation $S3$	4.4 E-3	2.9 E-3

TABLE VII
SAFETY-CRITERIA DETERMINED WITH THE PROPOSED APPROACH

	1st data set	2nd data set	Both data sets considered
IR_{extend_avg} on T_m	7.04 E-2	5.65 E-2	6.35 E-2
PFH on 1h	3.58 E-2	2.74 E-2	3.16 E-2

events for the first fault detection method and the number of false and missed detection events for the second method. Such results are in fact not really surprising since errors estimated with EKF residuals are supposed to be Gaussian. This hypothesis is strong especially for the pseudorange errors (cf. Subsec. III-C) that do not follow such distribution in case of multipath phenomena. However, finding a correct error model for such errors and for correctly estimating an error bound, i.e. a PL, remain research issues that are not covered in this article as the objective was to focus on the way to evaluate safety according to railway criteria. Note also that there will be always a compromise between the specified values of P_{fa} and P_{md} used to tune the sensibility the tests in the detection algorithm, i.e. reducing the one implying augmenting the other.

Besides the description of the integrity monitoring performances, the number of risky localization events mentioned in *Step 1* of the safety evaluation approach proposed in Subsec. III-E, can be quantified thanks to Table V values. In particular, when there is no detection and ($PE > PL$ and $PL \leq AL$) whatever PE greater or lesser than AL, is a condition that leads to the number of wrong side failure events $A = \{SU \cup DU\}$ (found at the last line of the table). Following *Step 2*, this leads to $p_{wsf_{avg}} = 0.175$ for the 1st data set, and $p_{wsf_{avg}} = 0.128$ for the 2nd data set, that are very high probabilities for characterizing safety ; this aspect will be more discussed at the end of the article.

F. Estimation of the integrity risk using the operational cases and discussion

The integrity risk evaluation follows *Step 3* of the proposed approach. The temporal succession of integrity monitoring events presented in previous subsection will be now analyzed to identify hazardous situations $S1$, $S2$ and $S3$ (cf. Subsec. III-B). This step considers a sliding windows of TTA seconds on the mission time of each operational case to quantify the number of HZS. Results of this step are presented in Table VI. Table VII sets out their associated integrity risks, their associated PFH values following *Step 4* of the evaluation approach and, a global value for IR_{extend_avg} and PFH considering together both scenarios as they are traveled on the same itinerary. These values are approximation of probabilities that can be reduced with a higher number of scenarios and also, with a higher number of points in these scenarios.

Safety of the GNSS/INS system in the considered operational case study can be discussed from the obtained PFH value equal to 3.16 E-2. Considering the IEC 61508 standard, we can conclude that the GNSS/INS system evaluated in this example has to be considered unsafe and unusable as its PFH is larger than all PFH intervals related to the SIL defined in the standard.

However, it is important to note that this result is obtained with the strong hypotheses evoked before, both in the integrity algorithm put in place and, in the configuration of GNSS/INS algorithm used to estimate a position. The obtained value has also to be interpreted as regards the taken accuracy requirement of 20 meters for AL. Indeed, other studies like in Locoprol project have obtained a safe architecture but considering an acceptable positioning error of 200 to 400 meters for 95% of the time [37]. In the future, it is necessary to consider improved algorithms by following also the progresses of the researches stemming from the communities dealing with the satellite navigation integrity and with the modeling of integrated multisensor systems.

V. CONCLUSION

GNSS-based localization on board of trains foreshadows important benefits for the railway domain in the coming years thanks to the reduction of ground-based equipment. However, the developed embedded systems will be regarded as safe only

if their conditions of use are analyzed not only by performance indicators but also through the analysis of the risk levels linked to identified hazardous scenarios.

This article has proposed a safety appraisal method concentrated on the train spacing scenario. The method focused on the integrity risk concept taken from the aeronautical domain and extends this concept to a multisensor solutions used in a railway environment. A detection mechanism is considered, it relies on a classical GNSS integrity monitoring and on the detection of cumulative errors. The main contribution of this work is devoted to introduce the four-step approach to estimate confidence-related parameters, in particular those leading to the extended integrity risk. With these steps, we showed how to handle integrity parameters in order to evaluate safety criteria related to the train spacing operational case. A particular care was taken to propose a graspable and manageable safety evaluation methodology consistent with railway expectations and addressing fundamental safety concepts both in aeronautical and in railway domains. The approach has been illustrated on a GNSS/INS architecture using real GNSS data that suffer from perturbations provoked by a transport environment.

In a close future, the interest will be to apply such methodology on a more robust hybridized solution in order to evaluate the safety of progressing solutions developed for rail [26]. In terms of application, a perspective will also be to evaluate the safety considering different situations encountered during the moving block operation.

APPENDIX A
LINEARIZED AND DISCRETE TIME MODEL OF A GNSS/INS SYSTEM USED INTO AN EKF FOR ESTIMATING THE TRAIN POSITION

A Kalman Filter is a recursive and real time data processing algorithm used to estimate states of a dynamic linear system in a noisy environment. In an EKF, state and measurement equations concern a nonlinear system. Considering they depend of the time t, they are respectively modeled with Eq. 7 and Eq. 8 (Note that all the theoretical aspects presented in this appendix are taken from [35] from which the same notations are kept). $\mathbf{f}$ and $\mathbf{h}$ are nonlinear functions to be applied to the state vector $\mathbf{x}$ for describing respectively the system evolution and the measurement update. $\mathbf{z}$ is the vector of sensor measurements. $\mathbf{w}_s$ and $\mathbf{w}_m$ respectively model the system noise and measurement noise.

$$\dot{\mathbf{x}}(t) = \mathbf{f}(\mathbf{x}(t), t) + \mathbf{w}_s(t) \tag{7}$$

$$\mathbf{z}(t) = \mathbf{h}(\mathbf{x}(t), t) + \mathbf{w}_m(t) \tag{8}$$

Given the discrete time k (iteration number of the EKF), Eq. 9 and Eq. 10 are obtained when linearizing the state and measurement models around the state vector estimate $\hat{\mathbf{x}}$. Then, $\mathbf{\Phi}$ and $\mathbf{H}$ are the evolution and the measurement matrices obtained by linearization. The content of each matrix mentioned in this appendix is given hereafter. For the EKF (whose steps are reminded in Fig. 11), the linear system model employed is more specifically related to the residuals or innovations associated to the states (generally noted with a δ). To update the state vector at each EKF iteration, the innovation $\delta\mathbf{z}$ is used and obtained, as presented for the tightly coupled GNSS/INS architecture in [35], by the difference between GNSS measurements (pseudoranges ρ and pseudorange rates $\dot{\rho}$) and a prediction of those measurements using the INS raw solution.

$$\mathbf{x}_k = \mathbf{\Phi}_{k-1}\mathbf{x}_{k-1} + \mathbf{w}_{s,k-1} \tag{9}$$

$$\mathbf{z}_k = \mathbf{H}_k\mathbf{x}_k + \mathbf{w}_{m,k} \tag{10}$$

In the following, $\mathbf{Q}$ and $\mathbf{R}$ are the covariance matrices of $\mathbf{w}_s$ and $\mathbf{w}_m$. The state vector $\mathbf{x}$ is partitioned into two sub-vectors $\mathbf{x}_{INS}$ of 15 states and $\mathbf{x}_{GNSS}$ whose states depends of the number of visible satellites. $\mathbf{P}$ is the covariance matrix of the system error. The estimated attitude and velocity are earth-referenced and resolved in a local navigation frame, while the position error is given in latitude, longitude and height. The content of the matrices and vectors are detailed below:

- $\delta\psi$ is the vector of attitude angle errors, $\delta\mathbf{v}$ and $\delta\mathbf{r}$ are the velocity and position error vectors, $\mathbf{b}_a$ and $\mathbf{b}_g$ are vector describing biases linked to the accelerometers and gyroscopes of the INS ([35] approximates them as white noises), τ_S is the time interval used in the EKF (here 0.2 s)
- in the $\mathbf{\Phi}$ matrix, partitioned into two sub-matrices $\mathbf{\Phi}_{INS}$ and $\mathbf{\Phi}_{GNSS}$, the matrices $\mathbf{F}^n_{21}$, $\mathbf{F}^n_{23}$, $\mathbf{F}^n_{32}$, and $\mathbf{T}^n_b$ are such as:
  - $\mathbf{F}^n_{21} = [-(\mathbf{T}^n_b\mathbf{f}^n_b)\wedge]$, where $\mathbf{T}^n_b$ is described below, the symbol $\wedge$ refers to an antisymmetric matrix (i.e. $\mathbf{A}^T = -\mathbf{A}$), and $\mathbf{f}^n_b$ is a specific force (measured by the accelerometer part of the inertial unit)
  - $\mathbf{F}^n_{23} = -\frac{2g_0(L_b)}{r_{eS}(L_b)}\begin{bmatrix}0&0&0\\0&0&0\\0&0&1\end{bmatrix}$, where r_{eS} is the geocentric radius at the earth surface, g_0 is the acceleration due to gravity, both are function of the latitude of the vehicle L_b,
  - $\mathbf{F}^n_{32} = \begin{bmatrix}\frac{1}{R_N(L_b)+h_b}&0&0\\0&\frac{1}{(R_N(L_b)+h_b)cos\,L_b}&0\\0&0&-1\end{bmatrix}$, where h_b is the height of the vehicle, R_N is the radius of curvature of the WGS84 ellipsoid for the north-south motion function,
  - $\mathbf{T}^n_b$ is the coordinate transformation matrix from the frame centered on the vehicle (or body coordinate frame) to the local navigation frame (North, East, Down),
- in the $\mathbf{Q}$ matrix, partitioned into two sub-matrices $\mathbf{Q}_{INS}$ and $\mathbf{Q}_{GNSS}$, the elements are:
  - S_{rg}, S_{ra}, S_{bad}, and S_{bgd} are the power spectral densities of, respectively, the gyro random noise, accelerometer random noise, accelerometer bias variation, and gyro bias variation (assumed as independent of frequency),
  - S^a_{cf} is the receiver clock frequency drift PSD and $S^a_{c\phi}$ is the phase drift PSD,
- the $\mathbf{H}$ matrix is an approximated form of the measurement matrix using $\mathbf{u}^e_{as,j} = \frac{\mathbf{r}^e_{es,j}(t_{st}) - \mathbf{r}^e_{ea}(t_{sa})}{|\mathbf{r}^e_{es,j}(t_{st}) - \mathbf{r}^e_{ea}(t_{sa})|}$; it is a unit

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_{INS} \\ \mathbf{x}_{GNSS} \end{bmatrix} \text{ with: } \quad \mathbf{x}_{INS} = \begin{bmatrix} \delta\psi \\ \delta\mathbf{v} \\ \delta\mathbf{r} \\ \mathbf{b}_a \\ \mathbf{b}_g \end{bmatrix} \text{ and } \mathbf{x}_{GNSS} = \begin{bmatrix} \delta\rho \\ \delta\dot{\rho} \end{bmatrix}$$

$$\mathbf{\Phi} = \begin{bmatrix} \mathbf{\Phi}_{INS} & 0 \\ 0 & \mathbf{\Phi}_{GNSS} \end{bmatrix} \text{ with: } \quad \mathbf{\Phi}_{INS} = \begin{bmatrix} \mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{T}_b\tau_S \\ \mathbf{F}^n_{21}\tau_S & \mathbf{I}_3 & \mathbf{F}^n_{23}\tau_S & \mathbf{T}^n_b\tau_S & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{F}^n_{32}\tau_S & \mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{I}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{I}_3 \end{bmatrix} \quad \text{and } \mathbf{\Phi}_{GNSS} = \begin{bmatrix} 1 & 0 \\ \tau_S & 1 \end{bmatrix}$$

$$\mathbf{Q} = \begin{bmatrix} \mathbf{Q}_{INS} & 0 \\ 0 & \mathbf{Q}_{GNSS} \end{bmatrix} \text{ with: } \quad \mathbf{Q}_{INS} = \begin{bmatrix} S_{rg}\mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & S_{ra}\mathbf{I}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & S_{bad}\mathbf{I}_3 & \mathbf{0}_3 \\ \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & \mathbf{0}_3 & S_{bgd}\mathbf{I}_3 \end{bmatrix} (\tau_S) \quad \text{and } \mathbf{Q}_{GNSS} = \begin{bmatrix} S^a_{c\phi}\tau_S & 0 \\ 0 & S^a_{cf}\tau_S \end{bmatrix}$$

$$\mathbf{H} = \left[\begin{array}{ccccccc} 0_{1,3} & 0_{1,3} & (\mathbf{u}^e_{as,1})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ 0_{1,3} & 0_{1,3} & (\mathbf{u}^e_{as,2})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1,3} & 0_{1,3} & (\mathbf{u}^e_{as,m})^T & 0_{1,3} & 0_{1,3} & 1 & 0 \\ \hline 0_{1,3} & (\mathbf{u}^e_{as,1})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \\ 0_{1,3} & (\mathbf{u}^e_{as,2})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0_{1,3} & (\mathbf{u}^e_{as,m})^T & 0_{1,3} & 0_{1,3} & 0_{1,3} & 0 & 1 \end{array}\right] \text{ and } \mathbf{R} = \left[\begin{array}{cccc|cccc} \sigma^2_{\rho 1} & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ 0 & \sigma^2_{\rho 2} & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \sigma^2_{\rho m} & 0 & 0 & \dots & 0 \\ \hline 0 & 0 & \dots & 0 & \sigma^2_{r1} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \sigma^2_{r2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & \sigma^2_{rm} \end{array}\right]$$

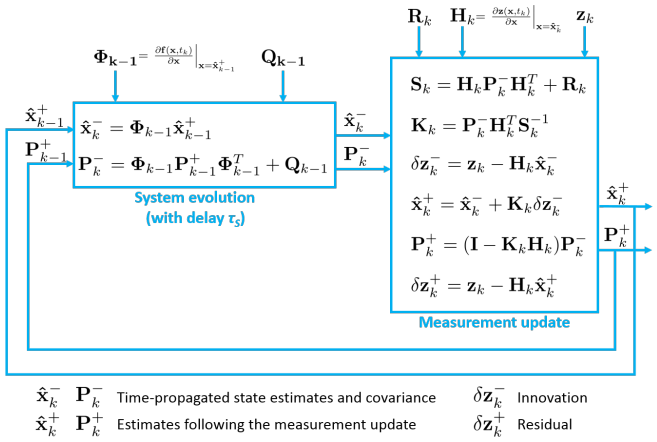

Fig. 11. Illustration of inputs, outputs, steps and matrix notations used in the EKF

vector, which describes the direction from which a line-of-sight satellite signal s arrives at the user antenna a where $\mathbf{r}^e_{es,j}(t_{st})$ and $\mathbf{r}^e_{ea}(t_{sa})$ are respectively the position coordinates of the j^{th} satellite signal at the time t_{st} (time of signal transmission) and the position coordinates of the receiver antenna at the time t_{sa} (time of signal arrival) in a ECEF frame e,

- in the $\mathbf{R}$ matrix, $\sigma^2_{\rho j}$ et σ^2_{rj} are respectively pseudorange error variances and pseudorange rate error variances that depend on the elevation of the j^{th} satellite.

GLOSSARY

AL Alert Limit
BG Balise Group
BTM Balise Transmission Module
CBTC Communication-Based Train Control
CSM Common Safety Method
DD Dangerous Detected event
DU Dangerous Undetected event
EGNOS European Geostationary Navigation Overlay Service
EKF Extended Kalman Filter
EoA End-of-Authority
ERTMS European Rail Traffic Management System
ETCS European Train Control System
EUAR European Union Agency for Railways
EULYNX European Initiative Linking Interlocking Subsystems
GNSS Global Navigation Satellite System
GPS Global Positioning System
HZS Hazardous Situations
IMU Inertial Measurement Unit
INESS INtegrated European Signalling System
IP Information Point
IR Integrity Risk
IXL Interlocking
LRBG Last Relevant Balise Group
MA Movement Authority
NGTC Next Generation Train Control
NSSE Normalized Sum of Squared Error
PE Position Error
P_{fa} Probability of False Alarm
PFH Frequency of dangerous failure per hour
PGE Progressively Growing Errors
PL Protection Level
P_{md} Probability of Missed Detection
PR Position Report
p_{wsf} Probability of Wrong-Side Failure
RAIM Receiver Autonomous Integrity Monitoring
RBC Radio Block Center
SD Safe Detected event

SGE Slowing Growing Error
SIL Safety Integrity Level
SSE Sum of Squared Error
STARS Satellite Technology For Advanced Railway Signalling
SU Safe Undetected event
THR Tolerable Hazard Rate
TSI-CCS Technical Specification for Interoperability for the Control-Command and Signalling subsystems
TTA Time-To-Alert
VB Virtual Balise

ACKNOWLEDGMENT

The authors would like to thank the technological research institute Railenium for funding the PhD researches of Cyril Legrand. All our thanks too, to the GEOLOC team from IFSTTAR-Nantes for allowing the use of GNSS and reference positioning data very useful for the accomplishment of this work. The contributions brought in this paper are also the result of interesting exchanges conducted within the framework of STARS and Smarties projects. STARS (Satellite Technology for Advanced Railway Signalling) is an integrated research project within the European H2020 research and innovation programme. Smarties (Smart, Fail-Safe Communication and Positioning Systems) is a project of the ELSAT2020 programme co-financed by the European Union with the European Regional Development Fund, the French state and the Hauts-de-France Region Council.

REFERENCES

[1] http://shift2rail.org, website of Shif2Rail, European initiative to coordinate and manage the EU research and innovation investments in the rail sector, established under Horizon 2020 European program.
[2] Regulation (EU) 402/2013, "Common Safety Method for risk evaluation and assessment and repealing Regulation (EC)352/2009," Commission implementing regulation, 30th April 2013.
[3] Regulation TSI CCS (EU) 2016/919, "Technical Specification for Interoperability relating to the 'Control-Command and Signalling' subsystems of the rail system in the European Union," European Commission regulation, 27th May 2016.
[4] J. Pachl, "Railway Operation and Control," 3rd edition, VTD Rail Publishing, Mountlake Terrace, USA, 284 pages, ISBN 978-0-9719915-6-9, 2014.
[5] F. Rispoli, G. Siciliano, and C. Brenna, "GNSS for ERTMS train localization, a step-change technology and new business mode," in *Inside GNSS*, pp. 48-54, March/April 2017.
[6] D. Lu and E. Schnieder, "Performance evaluation of GNSS for train localization," in *IEEE Trans. on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 1054-1059, April 2015
[7] T.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," in *Reliability Engineering & System Safety*, vol. 133, pp. 300-313, Jan. 2015.
[8] J. Beugin and J. Marais, "Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization," in *Transportation Research, part C: Emerging Technologies*, vol. 22, pp 42-57, June 2012.
[9] C. Legrand, J. Beugin, B. Conrard, J. Marais, M. Berbineau, and E.-M. El-Koursi, "From extended integrity monitoring to the safety evaluation of satellite-based localisation," in *Reliability Engineering & System Safety*, vol. 155, pp 105-114, Nov. 2016.
[10] UNISIG Subset 091, "Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2," Union of Signalling Industry, issue 3.6.0, 2016-05-12.
[11] UNISIG Subset 088, "ETCS Application Levels 1 & 2 - Safety Analysis," Union of Signalling Industry, issue 3.6.0, 2016-06-20.
[12] UNISIG Subset 041, "Performance Requirements for Interoperability," Union of Signalling Industry, issue 3.1.0, 2012-03-01.
[13] UNISIG Subset 036, "FFFIS for Eurobalise," Form-Fit Functional Interface Specifications defined by the Union of Signalling Industry, issue 3.0.0, 2012-02-24.
[14] UNISIG Subset 026-7, "System Requirements Specification - Chapter 7 - ERTMS/ETCS language", Union of Signalling Industry, issue 3.6.0, 2016-05-13.
[15] A. Camillo, E. Guillaume, T. Rogaume, A. Allard, and F. Didieux, "Risk analysis of fire and evacuation events in the European railway transport network," in *Fire Safety journal*, vol. 60, pp. 25-36, August 2013.
[16] D. Macii, S. Dalpez, R. Passerone, M. Corrà, M. Avancini, and L. Benciolini, "A safety instrumented system for rolling stocks: Methodology, design process and safety analysis," in *Measurement journal*, vol. 67, pp. 164-176, May 2015.
[17] D. S. Kim and W. C. Yoon, "An accident causation model for the railway industry: Application of the model to 80 rail accident investigation reports from the UK," in *Safety Science journal*, vol. 60, pp. 57-68, Dec. 2013.
[18] S. Rangra, "Performance shaping factor based human reliability assessment using valuation-based systems – application to railway operations," PhD thesis of University of Technology of Compiègne (France), prepared in the laboratory of Heuristics and diagnostics for complex systems (Heudiasyc), Oct. 2017.
[19] P. Smith, "Safety Case for the Introduction of New Technology into an Existing Railway System," PhD Thesis of the Imperial College London, prepared at the Department of Civil and Environmental Engineering, Centre for Transport Studies, Sept. 2016.
[20] L. H. Vu, "Formal Development and Verification of Railway Control Systems – In the context of ERTMS/ETCS Level 2," PhD Thesis of Technical University of Denmark, prepared at the department of Applied Mathematics and Computer Science (DTU Compute), Oct. 2015.
[21] Y. Luo, M. Van Den Brand, Z. Li, and A. K. Saberi, "A systematic approach and tool support for GSN-based safety case assessment," in *Journal of Systems Architecture*, vol. 76, pp. 1-16, May 2017.
[22] M. Malvezzi, G. Vettori, B. Allotta, L. Pugi, A. Ridolfi, F. Cuppini, and F. Salotti, "Train Position and Speed Estimation by Integration of Odometers and IMUs," *9th World Congress on Railway Research*, Lille, France, May 2011.
[23] P. Gurník, "Next Generation Train Control (NGTC): More Effective Railways through the Convergence of Main-line and Urban Train Control Systems," *6thTransportation Research Procedia*, vol. 14, pp. 1855-1864, April 2016.
[24] J. Marais, J. Beugin, and M. Berbineau, "A survey of GNSS-based Research and Developments for the European railway signaling," in *IEEE Trans. on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2602-2618, Oct. 2017.
[25] J. Marais, J. Beugin, Poumailloux, and M. Gandara, "EGNOS service evaluation in railway environment for safety-critical operations," *7th Transport Research Arena (TRA)*, Vienna, Austria, April 16-19, 2018.
[26] J. Otegui, A. Bahillo, I. Lopetegi, and L. E. Díezin, "A Survey of Train Positioning Solutions," in *IEEE Sensors Journal*, vol. 17, no. 20, Oct. 2017.
[27] M. Thomas, "Safety Analysis," Deliverable D3.4.1 version 2.0 of the GRAIL European project, 6th Framework Programme, 73p, 2008.
[28] K.-A. Ouedraogo, J. Beugin, E.-M. El-Koursi, J. Clarhaut, D. Renaux, and F. Lisiecki, "Toward an application guide for Safety Integrity Level allocation in railway systems," in *Risk Analysis journal*, DOI: 10.1111/risa.12972, Feb. 2018.
[29] I.U. Bhatti and W.Y. Ochieng, "Failure Modes and Models for Integrated GPS/INS Systems," *The Journal of Navigation*, vol. 60, pp 327-348, April 2007.
[30] UIC, "Compendium on ERTMS," Edited by UIC (International union of railways) under the coordination of Peter Winter, Eurailpress, Hamburg, Germany, 260 pages, ISBN 978-3-7771-0396-9, 2009.
[31] P. Sun, "Model-based system engineering for safety of railway critical systems," PhD thesis of the École Centrale de Lille (France), prepared in The Evaluation of Automated Transport Systems and their Safety Laboratory (ESTAS) of IFSTTAR, July 2015.
[32] N.A. Zafar, S.A. Khan, and K. Araki, "Towards the safety properties of moving block railway interlocking system," in *International Journal of Innovative Computing Information and Control*, vol. 8, no. 8, pp. 5677-5690, August 2012.
[33] A. Zimmermann and G. Hommel, "Towards modeling and evaluation of ETCS real-time communication and operation," in *Journal of Systems and Software*, vol. 77, no. 1, pp. 47-54, July 2005.

[34] D. Emery, "Enhanced ETCS L2/L3 train control system," in *WIT Transactions on State-of-the-art in Science and Engineering*, vol. 46, Ed. Bin Ning, Advanced Train Control Systems, WITpress, ISBN: 978-1-84564-494-9, 2010.
[35] P.D. Groves, "Principles of GNSS, inertial, and multisensor integrated navigation systems," Second edition, Artech House, 776 pages, ISBN: 978-1-60807-005-3, 2013.
[36] ICAO, "International Standards and Recommended Practices, Annex 10 - Aeronautical Telecommunications, Volume 1 (Radio Navigation Aids)," Technical report, International Civil Aviation Organization, 2006.
[37] M. Rousseau and D. Cadet, "The LOCOPROL project (LOw COst Satellite based train location system for signalling and train PROtection for Low-density traffic railway Lines)," 7th *World Congress on Railway Research (WCRR)*, Montréal, Canada, June 4-8, 2006.
[38] N. Zhu, J. Marais, D. Bétaille, and M. Berbineau, "Integrity in Urban Environment: A Review of Literature," in *IEEE Trans. on Intelligent Transport Systems*, DOI: 10.1109/TITS.2017.2766768, Jan. 2018.
[39] A. Filip, J. Beugin, J. Marais, and H. Mocek, "Interpretation of the Galileo Safety-Of-Life Service by Means of Railway RAMS Terminology," in *Transactions on Transport Sciences*, vol. 1, no. 2, pp 61-68, June 2008.
[40] J. Beugin, A. Filip, J. Marais J., and M. Berbineau, "Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications," in *European Transport Research Review*, vol.2, no. 2, pp 93-102, May 2010.
[41] B. Roturier, E. Chatre, and J. Ventura-Traveset, "The SBAS Integrity Concept standardised by ICAO. Application to EGNOS," 5th *International Symposium on Global Navigation Satellite Systems*, Seville, Spain, May 2001.
[42] O. Le Marchand, "Autonomous approach for localization and integrity monitoring of a ground vehicle in complex environment," PhD thesis, Université de Technologie de Compiègne, France, June 2010.
[43] S. Feng, W.Y. Ochieng, D. Walsh, and R. Ioannides, "A measurement domain receiver autonomous integrity monitoring algorithm," in *GPS Solutions*, vol. 10, no. 2, pp 85-96, May 2006.
[44] S. Feng and W.Y. Ochieng, "A difference test method for early detection of Slowly Growing Errors in GNSS positioning," *The Journal of Navigation*, vol. 60, no. 3, pp 427-442, Sept. 2007.

Julie Beugin received the Engineering degree from National School of Engineering for Computer Science, Automation, Mechanics and Electronics (ENSIAME), in 2002; the master's degree in automation engineering from University of Valenciennes, France, in 2002; and the Ph.D. degree in automation engineering in 2006. Her Ph.D. dealt with the safety assessment of railway safety-related systems using risk concepts and RAMS evaluation methods (Reliability, Availability, Maintainability and Safety). Since 2007, she has been with IFSTTAR, the French institute of science and technology for transport, development and networks, as a researcher. Her research interest deals with dependability and safety evaluation of complex guided transportation systems. Her activities address RAMS demonstration issues of GNSS-based solutions embedded in train applications and dependability analysis of the LTE-based wireless communication links used in CBTC applications. She participated to the GaLoROI European Project and is currently a part of the STARS EU Project.

Cyril Legrand received the master's degree in automation engineering from University of Valenciennes and Hainaut-Cambresis in 2012. He also received the Ph.D. degree in engineering from the University of Lille in December 2016. With the support of the French institute of science and technology for transport, development and networks (IFSTTAR) and the French Technological Research Institute Railenium, his research activities addressed the safety assessment of GNSS-based localisation systems through the integrity monitoring. These activities were conducted in the context of railway applications especially the European Rail Traffic Management System (ERTMS). He is currently a researcher with Railenium about the evaluation of Safety Management System (SMS) performances within the scope of RESYGESS project. He is also with the French railway safety authority EPSF concerning questions about the harmonization and simplification of ERTMS authorization process in Europe.

Juliette Marais received the engineering degree from Institut Supérieur de l'Electronique et du Numérique and the Ph.D. degree in electronics from University of Lille, France, in 1998 and 2002, respectively. Since 2002, she has been a Researcher with IFSTTAR, the French institute of science and technology for transport, development, and networks. She is currently involved in GNSS performance analyses and enhancement in land transport environments. Since 2000, she has been participating with the European Railway-Related Projects, such as Locoprol, Satloc, GaloRoi, and STARS. She is also involved on two main research projects: integrity monitoring for land transport applications and GNSS propagation characterization in railway environments. Her research interests principally include propagation phenomena, positioning and pseudorange error modeling, filtering technics, and simulation. She has authored and co-authored 80 articles and holds one patent.

Marion Berbineau received the Engineer degree in electrical engineering from Polytech'Lille, France, and the Ph.D. degree in electrical engineering from University of Lille in 1986 and 1989, respectively. She is a full-time Research Director with IFSTTAR, the French institute of science and technology for transport, development and networks. She is an expert in the field of radio wave propagation in transport environments (tunnels), electromagnetic modeling, channel characterization and modeling, MIMO, wireless systems for telecommunications, cognitive radio for railways, and GNSS localization-based for ITS, particularly for the rail and public transport domains. She is active as an expert for the GSM-R and future systems such as LTE-A and 5G. She is involved in several National and European research projects. She has authored and co-authored several publications and patents.

El-Miloudi El-Koursi received the Ph.D. degree in computer dependability sciences in 1985 and the master's degree in electronic in 1982, both from the University of Lille Nord de France, Lille, France. He is currently a Research Director with the Evaluation and Safety of Automated Transport Systems Research Team (COSYS/ESTAS) of the French Institute of Science and Technology for Transport, Development and Networks (IFSTTAR), Université Lille Nord de France. He has 25 years experience in performing assessment and certification of safety-related rail and associated systems. In recent years, he has been involved in various European projects. He also was the leader of the European FP5 Safety Management and Interoperability Thematic Network and the leader of the sixth pole on "safety and security" within the FP6 European Rail Research Network of Excellence. Dr. El-Koursi has organized several conferences and workshops on railway issues and is a reviewer for several international journals in the transportation and safety domains.