Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept

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

LEGRAND, Cyril, BEUGIN, Julie, EL KOURSI, El Miloudi, MARAIS, Juliette, BERBINEAU, Marion, CONRARD, Blaise, 2015, Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept, ESREL 2015 - European safety and reliability conference, Zürich, SUISSE, 2015-09-07, 8p

Approach for evaluating the safety of a satellite-based train localisation system through the extended integrity concept

C. Legrand
Univ Lille Nord de France, F-59000 Lille, France
IFSTTAR, COSYS, ESTAS, F-59650 Villeneuve d'Ascq, France
Institut de Recherche Technologique Railenium, F-59300, Famars, France

J. Beugin, E.-M. El-Koursi
Univ Lille Nord de France, F-59000 Lille, France
IFSTTAR, COSYS, ESTAS, F-59650 Villeneuve d'Ascq, France

J. Marais, M. Berbineau
Univ Lille Nord de France, F-59000 Lille, France
IFSTTAR, COSYS, LEOST, F-59650 Villeneuve d'Ascq, France

B. Conrard
Univ Lille Nord de France, F-59000 Lille, France
CRIStAL, UMR 9189, F-59650 Villeneuve d'Ascq, France

ABSTRACT: The integrity concept, safety quality criterion for satellite-based localisation systems used in aeronautics, is described in terms of levels (protection and alert levels), time (Time To Alarm) and probability (integrity risk). In land transport applications, the requirements in terms of integrity differ from aeronautics in their definition and values. Global Navigation Satellite Systems (GNSS) in railways suffer from additional weaknesses *i.e.* multipath and masking phenomena, which can degrade the localisation integrity. This situation cannot be tolerated in safety-related applications like train control and signalling. To mitigate these weaknesses, GNSS is usually combined with other localisation systems like inertial sensors. However, existing integrity monitoring processes are designed for GNSS integrity evaluation, *i.e.* to estimate the risk allocated to the position given by the GNSS receivers only. Our research work aims, first, to extend the integrity concept to such systems, and, secondly, to demonstrate how to evaluate, with this concept, the safety of a localisation system as expected in railways. The safety of GNSS-Based Localisation System is formalised and quantitatively evaluated.

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS) are now well-spread in air and road transports for non-safety-relevant applications as, as well-known, fleet management, driver assistance or passenger information. In these services, the quality of the localisation information is not a vital parameter regarding the safety (Beugin and Marais 2012) and the performances provided by mass market GNSS-based systems are sufficient, as the one embedded in smartphones.

To guarantee their high level of safety, railways are ruled by standards (especially EN50126 (CENELEC 2007)) that require the degree of confidence, which the user can place in the delivered service through a dependability evaluation. Especially, a safety demonstration is required to put the satellite-based train localisation system into service and has to be delivered in safety documentation required by certification bodies and national safety authorities. GNSS-based positioning systems will have to go through these steps before being generalised. As classical done in robotics or other vehicular applications, some of these railway consortia as 3inSat (Salvatori et al. 2014) developed hybridised GNSS-based multi sensor systems based on different choice of sensors and different strategies to ensure safety but exploiting the advantages and drawbacks of each sensor used. This paper will focus on the safety evaluation of these

kind of systems.

GNSS performance evaluation does not only rely on accuracy when speaking about railway safety. Integrity, linked to a confidence granted to the system, is of prime importance (Le Marchand et al. 2009, Liu et al. 2010, Ochieng et al. 2008). This concept permits us to estimate the risk linked to the position error exceeding an alert limit without being detected called also the integrity risk. However, initially expressed only for GNSS, the integrity must be extended to the positioning systems except GNSS. Thanks to the extended integrity definition and the use of a risk probability related to the railway safety requirements, it is possible to formalise the link between the probability of this risk and the integrity risk.

The paper is organised as follow. In section 2, each part of the considered satellite localisation system hybridised is described in order to make explicit the potential sources of hazard and, finally, the GNSS integrity concept is introduced. In the section 3, the extended integrity of a satellite localisation system hybridised is defined. The section 4 to propose an approach for evaluating the safety using the extended integrity concept thanks to a mathematical formalism of the link between integrity and safety. Paper conclusions are given in section 5.

2 RISK IN SATELLITE-BASED TRAIN LOCALISATION SYSTEM

In its ERTMS (European Rail Traffic Management System) Memorandum of Understanding, the European Railway Agency indicates that GNSS particularly the future Galileo (associated with the satellite augmentation system) can play a major role in the rail sector, both for fleet management and rail safety (signalling and train control) (European Railway Agency 2012). ERTMS, particularly, the ETCS (for European Train Control System) is a new train control system and signalling designed to replace the 27 existing systems in Europe, which generate interoperability problems. In an ERTMS context, satellite technologies can contribute to reducing the costs of the infrastructure (for example, the balise) and enhancing the performances of the ETCS odometer in new trains without impact on equipped lines.

2.1 *Global Navigation Satellite System risk and risk mitigation*

GNSS technology is based on the trilateration concept, which defines the process of determining absolute position by measurement of distances, called pseudoranges using spheres. Typically, these pseudoranges are the distances between a user receiver and satellites. For a single satellite signal, a user can be located on the surface of a sphere of a radius $\boldsymbol{r}$ centred on that satellite. With two signals, the user position can be located on the intersection of two spheres of radii $\boldsymbol{r_1}$ and $\boldsymbol{r_2}$. It is necessary to use an additional signal (a third satellite is requested) in order to limit the user position to two points. For terrestrial applications, one of these two points is possible (the other point is in space). However, the user receiver and the satellite clocks are not exactly synchronised due to relativist effects and lower quality of the receiver clock compared to the satellites' clock. In the three-equations system, the synchronisation issue adds a fourth unknown variable, the clock offset.

GNSS standalone receiver is particularly efficient in terms of availability and safety in open sky areas and precise in the long term (Lu and Schnieder 2014). However, it suffers from multiple weaknesses, such as multipath effect, signals blocked by environmental items (trees, buildings, terrain relief). These signals are also disrupted by RF interference. Several mechanisms on board (use of very precise receivers, map-matching method, *etc*...), on the ground (relay masts, ground-based augmentation system, *etc*...) and at the level of satellites (use of multi-constellation of satellites (GPS (American) + Glonass (Russian) + Galileo (European)), satellite-based augmentation system, *etc*...) exist to mitigate these weaknesses. Besides, techniques for detecting and correcting faults can be implemented in a localisation system (integrity monitoring - integrity concept is described in subsection 2.2).

This last solution is the only one on which railway stakeholders can act on, so it is chosen in this paper. Subsection 2.1.2 deals with the different kind of integration. Before explaining this, the inertial systems that can be hybridised to GNSS are introduced, especially their errors.

2.1.1 *Dead reckoning and risk*

Dead reckoning is a computation process of the current position by using a previously determined position. The Inertial Navigation Systems (INS) and odometer are examples of navigation systems using dead reckoning. First, a INS (Woodman 2007) are commonly used in air, road transport and railways. These systems are composed of two hardware and software parts and provide a navigation solution *i.e.* position, speed and acceleration. The acceleration is determined by the measurement of the specific force and angular rate in body frame (roll, pitch and yaw). The hardware part corresponds to the sensor part called Inertial Measurement Unit (IMU), which is composed of three accelerometers providing an acceleration measurement and three gyroscopes providing a rotation (angular position) measurement (one for each axis in a inertial frame). The software part corresponds to a computer unit, which resolves

inertial equations in order to give a navigation solution. At this level, the measurements coming from accelerometers and gyroscopes are merged. Second, a odometer is a device fitted on the bogie axles, which provides a distance travelled by a vehicle. Classically, it is composed of an incremental encoder, which measures elementary motions of the vehicle.

These systems suffer from slipping phenomena (odometer) and gyroscope bias and initial pitch error (INS), which lead to cumulative errors at each time. Further, these errors are called Slowly Growing Errors showing the slow and insidious nature of his errors. At their occurrence, Slowly Growing Errors are not enough significant to be detected. Without calibration means (note that, in railway context, this calibration is performed by balises, device regularly placed on a railway), these Slowly Growing Errors become too high to be tolerated for all the duration of a mission.

2.1.2 *GNSS/INS integration and risk*

A standalone GNSS receiver associated with an augmentation system does not meet railway safety requirements (Rispoli et al. 2013). The strategy of hybridisation appears as a realistic solution in difficult environments (Gioia and Borio 2015). The hybridisation is a combination of different technologies of localisation (odometry, inertial system, *etc.*), which provides additional navigation signals. Different kinds of hybridisation exist (loosely, tightly, deeply coupled architecture) according to the input data chosen (Groves 2013). These integration architectures will not be fully developed in this paper. It is important to know that the more the input data will be taken upstream of the GNSS subsystem, the more the architecture will be tightly coupled. In this case, these input data are the pseudoranges and not a navigation solution computed by a software part. The main advantage of the INS/GNSS architecture is that each part of the system mitigates the weaknesses others'. Indeed, a proprioceptive localisation technique associated with an exteroceptive one is particularly efficient in several aspects (accuracy, availability, safety, *etc.*). The use of two identical localisation techniques is less judicious: they suffer from the same phenomena and they can mitigate their effects. In the case of inertial/GNSS integration, the GNSS accuracy in the long term mitigates the Slowly Growing Errors affecting the inertial system. So, in order to keep the capacity for excluding a localisation source at the occurrence of failure(s), a loose architecture is not an optimal solution. In that case, if a failure is detected on the GNSS side, the navigation solution, which it provides, is entirely excluded and the train continues to operate with only INS, a situation to avoid in the long term (cf subsection 2.1.1). In consequence, a tightly coupled GNSS/INS is more resilient to failures. Instead of excluding all the GNSS navigation solution in the failure case, it is possible to exclude only one pseudorange on the condition that the number of satellite is higher than 4, the minimum to determine a navigation solution (cf subsection 2.1). Knowing that more than four satellites are in view at any point of earth, GNSS receiver is capable of computation a navigation solution in spite of failures.

To put into service this kind of system, it is necessary to perform a dependability evaluation through reliability, availability, maintainability and safety (RAMS). However, GNSS performances are evaluated in terms of another class of attributes: accuracy, availability, continuity and integrity (Beugin and Marais 2012). In the next part, we propose to focus on the integrity attribute because, in the aeronautic domain, the integrity is well defined and several data processing systems to evaluate it, exist (For example, the RAIM (Receiver Automonious Integrity Monitoring) algorithms (Liu et al. 2010)). In railways, dependability methods are few (Lu and Schnieder 2014) for RAMS assessment of GNSS and we propose to counterbalance this observation by revision of integrity (definition and mechanisms) in order to evaluate the safety of these systems.

2.2 *GNSS integrity concept*

The integrity concept for GNSS is derived from aeronautical recommendations. It defines "the measurement of the degree of confidence that can be placed in the correctness of the navigation information". It includes "the ability of a localisation system to provide timely warnings to the user when the system should not be used for navigation" (Peters et al. 2008). Aeronautics rules GNSS localisation systems by aeronautical standards (ICAO 2006) especially in terms of integrity according to the following requirements:

- Alert Limit (AL): the maximum allowable position error beyond which the localisation system should be declared unavailable for the intended application
- Time To Alert (TTA): the maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the equipment enunciates the alert
- Integrity Risk: risk related to the position error exceeding the alert limit without the user being informed under TTA period of time

Integrity requirements are given for each application/operation/mission. However, to verify their achievement, the position error has to be known and is function of the true position, an unobservable quantity for the user. In consequence, it is necessary to use

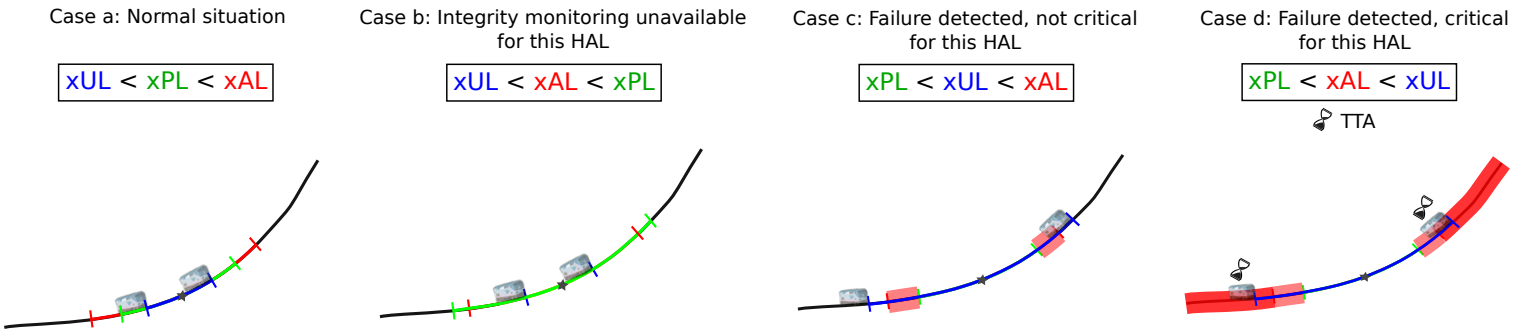


Figure 1: Relations between xUL, xPL and xAL in different cases in railway domain

other metrics including (the different levels are shown in figure 1):

- Protection Level (PL): information guaranteed to the user. It is a variable quantity and computed online from measurement estimations (cf subsection 3.2)
- Uncertainty Level (UL): interval around true position. The uncertainty level is a variable depending on current measurements.

To apply the concept to railways, the effort shall be put on adaptation to the terrestrial transport specificities and to railway rules. In this objective, some automotive (Le Marchand 2010) and railway (Jonas 2014) publications attempted to enhance integrity of position solution but it is always centred on GNSS. In a hybridised GNSS, the other positioning systems other than satellite-based ones are considered failure-free.

Looking at the integrity definition, this concept is compatible with other transport modes other than aeronautics except for the specific parameters UL, PL and the triplets of requirements (AL, TTA and integrity risk). In one hand, vertical error components of AL/UL/PL are less significant and can be neglected for rail and road applications. On the other hand, the integrity requirements depend on the application and the phase of a mission obviously very different according to the transport domain. In addition, these parameters do not consider the Slowly Growing Errors and the errors related to the masking or multipath effects on satellite signals due to varied environments encountered by trains. These considerations permit us to propose a transposition of integrity criteria inspired by the Along the Track Protection Interval method (Nikiforov and Choquette 2003) that are more adapted to the railway domain.

2.3 *Reminders about Safety, attribute of RAMS*

By definition, integrity is an attribute close to safety for a particular event occurring on a navigation solution. At this point, it is necessary to recall the safety definition as described in the standards (especially in EN 50126). Safety is defined by the "absence of unacceptable risk" linked to a probability of safety related failures, $f_S(t)$ (cf Appendice C in (CENELEC 2007)).

We considered as a "safety related failures" in a GNSS-based localisation system the following event: "the position error PE exceeds an alert limit AL, without being detected at the t_i, time of the position i". This paper does not present the failure modes leading to this catastrophic event. However, a complete list of them for a GNSS/INS system can be found in (Bhatti and Ochieng 2007). The probability of this event is linked to integrity risk mentioned in subsection 2.2. Only the considered interval of time is not the same. With the integrity definition, a temporal criterion, TTA has been introduced as a particular condition of the failure detection (TTA period of time).

In the IEC 61508-4 standard, Safety Integrity Level (SIL) is also defined as a quantified objective to reach related to the safety. Be careful, "Integrity" in SIL acronym does not have the same meaning of the integrity seen in this paper. The safety integrity concept is associated to the ability of a safety-related system satisfactorily performing the required safety functions in all specified conditions within a stated period of time. It is a general definition and the integrity point of view is considered for a specific safety related function: the localisation. A Tolerable Hazard Rate (THR) is also indicated in safety standards. In a safety-related systems evaluation context, these systems are often represented by configurations composed of channels. The GNSS/INS system performing the localisation function considered in the paper is a "1-out-of-1 with diagnosis" (1oo1D) voting where GNSS and INS represent a channel and the diagnostic is typically the monitoring integrity (cf figure 3).

3 EXTENDED INTEGRITY CONCEPT FOR A GNSS/INS LOCALISATION TRAIN SYSTEM

In order to give a justified confidence in the localisation system, the integrity concept must be defined, not only for the GNSS part, but also for the other parts, which constitute the localisation system (Here,

the INS part). The extended integrity on a navigation solution provided by the GNSS/INS system depends on the integrity of the navigation solutions provided by the GNSS and the INS system parts. The integrity monitoring already exists in the hybridised systems (GNSS receiver and inertial system) but the main objective is only to evaluate the GNSS integrity. In this case, the other systems provide additional information to GNSS. In the paper, GNSS is coupled with an Inertial Navigation System. Inertial measurements permit us to ameliorate GNSS signal acquisition when the satellite signals are not available. In the integrity monitoring of GNSS/INS, the INS measurements' validity are not discussed and are supposed to be internally guaranteed. However, the assumption about guaranteed validity is not conceivable in the case of a lack of compensation of the INS drifts. In consequence, this validity can be determined through the integrity for other systems other than GNSS. This leads to an extended integrity concept.

3.1 *State representation of GNSS/INS localisation system*

Before introducing the modification especially on $\boldsymbol{PL}$ computation, it is necessary to lay down some equations especially the considered state representation given by the Equation 2.

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{F}(t)\boldsymbol{x}(t) + \boldsymbol{G}(t)\boldsymbol{w}_s(t) \\ \boldsymbol{z}(t) &= \boldsymbol{H}(t)\boldsymbol{x}(t) + \boldsymbol{w}_m(t) \end{aligned} \quad (1)$$

with, $\boldsymbol{F}(t)$ is the $(\boldsymbol{n} \times \boldsymbol{n})$ state matrix of system where the eigenvalues correspond to the poles of the system, $\boldsymbol{x}(t)$ is the $(\boldsymbol{n} \times \mathbf{1})$ state vector representing the system state at time $\boldsymbol{t}$ and its derivative $\dot{\boldsymbol{x}}(t)$, $\boldsymbol{G}(t)$ is the $(\boldsymbol{n} \times \mathbf{1})$ continuous system noise distribution matrix, $\boldsymbol{w}_s(t)$ and $\boldsymbol{w}_m(t)$ are, respectively, the system and measurement noise considered as white Gaussians with zero mean, $\boldsymbol{z}(t)$ is the $(\boldsymbol{m} \times \mathbf{1})$ measurement vector corresponding to measurements received by the sensors at time $\boldsymbol{t}$, $\boldsymbol{H}(t)$ is the $(\boldsymbol{m} \times \boldsymbol{n})$ measurement matrix determined by known properties of the system such as kinematics user and GNSS satellite geometry.

For the sake of brevity, the different matrix and vectors are not developed in this paper (In simulation, $\boldsymbol{n} = \mathbf{17}$ and $\boldsymbol{m} \geq \mathbf{17}$ - it depends on the number of pseudoranges *i.e.* viewed satellites -). The evolution of the $\boldsymbol{m} - \boldsymbol{n}$ difference is important to supervise for integrity monitoring especially in computation of the failure detecting threshold.

3.2 *Extended integrity criteria determination for GNSS-based localisation systems*

The important point here is that the error covariance matrix $\boldsymbol{P}$ of the system and the innovation vector $\boldsymbol{\delta z}$ are computed in a Kalman filter. An error covariance matrix is a measurement of the estimated accuracy of the estimated state. An innovation vector shows the difference between the observation of the system state and the estimated state (cf Equation 2). These two quantities are useful respectively for $\boldsymbol{PL}$ and minimum detectable bias, $\boldsymbol{MDB}$ determination.

$$\boldsymbol{\delta z}(t) = \boldsymbol{z}(t) - \boldsymbol{h}(\hat{\boldsymbol{x}}(t)) \quad (2)$$

The computation of $\boldsymbol{PL}$ related to GNSS measurements does not change. However, the contribution of other positioning systems must be taken into account in $\boldsymbol{PL}$. In the hybridized systems, a positioning system like the inertial one makes corrections of GNSS measurements possible. In consequence, we do not see, in current $\boldsymbol{PL}$, the error contribution of inertial measurements as they are considered fault-free. By extension, we do not fully evaluate the global integrity. Equation 3 represents the $\boldsymbol{PL}$ guaranteed by GNSS measurements (Le Marchand 2010).

$$\begin{aligned} \boldsymbol{PL_{GNSS}} &= \sqrt{\boldsymbol{MAX}(\boldsymbol{H}(1,i)^2 + \boldsymbol{H}(2,i)^2)} \\ &\times \boldsymbol{MDB_{GNSS}} \end{aligned} \quad (3)$$

with, $\boldsymbol{MDB_{GNSS}}$ is the minimum detectable bias and $\boldsymbol{H}(1,i)$ and $\boldsymbol{H}(2,i)$ are linked to horizontal coordinates ($\boldsymbol{x}$ and $\boldsymbol{y}$) of the $\boldsymbol{i}$-th measurement given by the GNSS part only.

For an inertial system, the $\boldsymbol{PL}$ computation is not immediate (cf Equation 4). Indeed, the information of the inertial system do not appear in $\boldsymbol{H}$ matrix because these data are used to correct GNSS measurements and then they are merged. To find inertial measurements, pseudoranges $\boldsymbol{\rho}$ and pseudorange rates $\boldsymbol{\delta\rho}$ must be subtracted from the residuals. $\boldsymbol{MDB_{INS}}$ is a minimum detectable bias for INS part. These $\boldsymbol{MDB}$s depend on the performances of bias detection methods *i.e.* the probability that a bias is detected on GNSS or INS part. In this paper, $\boldsymbol{MDB_{GNSS}} = \mathbf{5.49}$ (meters) based on $\boldsymbol{MDB}$ calculation in (Le Marchand 2010) and $\boldsymbol{MDB_{INS}} = \mathbf{0.05}$ (meters) based on the performances of a Slowly Growing Errors detection (Ochieng et al. 2008).

$$\begin{aligned} &\boldsymbol{PL_{INS}} = \\ &\sqrt{\boldsymbol{MAX}((\boldsymbol{\delta z}(1,i) - \boldsymbol{\rho}(1,i) - \boldsymbol{\delta\rho}(1,i))^2} \\ &\overline{+(\boldsymbol{\delta z}(2,i) - \boldsymbol{\rho}(2,i) - \boldsymbol{\delta\rho}(2,i))^2} \\ &\times \boldsymbol{MDB_{INS}} \end{aligned} \quad (4)$$

Finally, a single measurement of $\boldsymbol{PL}$ must be considered. For safety reasons, the $\boldsymbol{PL}$ chosen is simply the maximum between $\boldsymbol{PL_{GNSS}}$ and $\boldsymbol{PL_{INS}}$ (cf Equation 5).

$$\boldsymbol{PL_{System}} = \boldsymbol{MAX}(\boldsymbol{PL_{GNSS}}, \boldsymbol{PL_{INS}}) \quad (5)$$

It remains the time to alert ($\boldsymbol{TTA}$) and integrity risk criteria for us to define. They are constant

quantities and represent integrity requirements (recommended values given in the subsection 4.2.1).

4 INTEGRITY APPROACH FOR EVALUATING SAFETY

In subsection 2.3, some similarities exist between integrity and safety attributes according to the safety related failure. This failure is linked to the integrity risk criterion, defined in subsection 2.2. The $\boldsymbol{TTA}$ period of time is also defined in this part and can be seen as an occurrence condition of the event specified as catastrophic. That is why the integrity risk is considered as a conditional probability and the Bayes theorem can be used.

4.1 *Demonstration and formalism of the link between integrity and safety*

To determine the link between integrity and safety for a localisation system, let consider the following events:

- $\boldsymbol{A_{t_i}}$, the event that $\boldsymbol{UL(t_i) > AL}$ with $\boldsymbol{UL(t_i)}$, observable quantity reflecting the current position error $\boldsymbol{PE}$ at $\boldsymbol{t_i}$ (cf subsection 2.2).
- $\boldsymbol{B_{t_i}}$ is the undetection at $\boldsymbol{t_i}$, an unsafe situation linked to the integrity risk.
- $\boldsymbol{B_{[t_i;t_i+TTA]}}$ is the undetection on $\boldsymbol{[t_i; t_i + TTA]}$ interval, it is the $\boldsymbol{B_{t_i}}$ event associated with the $\boldsymbol{TTA}$ period of time

As we can see in subsection 2.3, the safety attribute for a localisation system can be characterised by the probability of "$\boldsymbol{PE}$ exceeds $\boldsymbol{AL}$, without being detected at $\boldsymbol{t_i}$" event. In consequence, this probability can be expressed by Equation 6 and, for a given mission of a $\boldsymbol{Tm}$ duration in seconds and $\boldsymbol{Te}$, a sample time, by Equation 7.

$$\boldsymbol{f_S(t_i) = p(A_{t_i}|B_{t_i})} \tag{6}$$

$$\boldsymbol{PFH = \frac{3600}{Tm} \times \sum_{i=0}^{int(\frac{Tm}{Te})} f_S(t_i)} \tag{7}$$

$\boldsymbol{PFH}$ represents the probability of dangerous failure per hour. This notation, coming from IEC 61508, permits us to allocate a Safety Integrity Level (cf 4.2.2) to the localisation system. The $\boldsymbol{int(x)}$ function for any number $\boldsymbol{x}$ is the integer part of $\boldsymbol{x}$. Indeed, $\boldsymbol{Tm}$ can not be necessary a multiple of $\boldsymbol{Te}$ (same observation with $\boldsymbol{TTA}$ in relation to $\boldsymbol{Te}$ in Equation 6). Now, to express the probability linked to the integrity risk (further, this probability is written by $\boldsymbol{p(IR)}$),

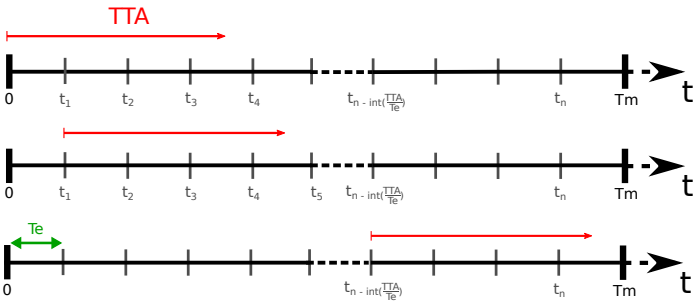


Figure 2: $\boldsymbol{TTA}$ period of time seen as a floating windows

$\boldsymbol{TTA}$ period of time must be taken into account (cf Equation 8).

$$\boldsymbol{p(IR(t_i)) = p(A_{[t_i;t_i+TTA]}|B_{[t_i;t_i+TTA]})} \tag{8}$$

Thanks to Equation 6, $\boldsymbol{f_S(t_i)}$ can be linked with $\boldsymbol{p(IR(t_i))}$ (cf Equation 9). $\boldsymbol{TTA}$, $\boldsymbol{t_i}$ and $\boldsymbol{Te}$ are expressed in seconds.

$$\boldsymbol{p(IR(t_i)) = \sum_{j=i}^{i+int(\frac{TTA}{Te})} f_S(t_j)} \tag{9}$$

All along a mission, $\boldsymbol{TTA}$ period of time is seen as a floating windows (cf figure 2). It permits us to make explicit a limit case occurring at $\boldsymbol{t_n}$, previous time before end of mission $\boldsymbol{Tm}$. In consequence, $\boldsymbol{t_n \leq Tm < t_{n+1}}$.

$$\boldsymbol{f_S(t_i) = \frac{1}{int(\frac{TTA}{Te})} \times p(IR(t_i))} \tag{10}$$

Equation 10 permits to express the safety attribute (characterised by $\boldsymbol{f_S(t_i)}$) throughout the integrity (characterised by $\boldsymbol{p(IR(t_i))}$ assuming that $\boldsymbol{f_S(t_i), ..., f_S(t_i + int(\frac{TTA}{Te}))}$ are equiprobables. Finally, thanks to Equation 7, a $\boldsymbol{PFH}$ can be computed.

4.2 *Safety quantitative analysis with integrity results*

Thanks to the extended integrity concept and the link between safety and integrity, it is possible to make a quantitative analysis of safety. Before introducing these results, the experimental protocol must be posed.

4.2.1 *Experimental protocol*

In order to generate integrity results, a simulated GNSS/INS localisation system is necessary. Its architecture is given in the figure 3 taken from (Groves 2013). To evaluate its integrity performances, some requirements must be followed: alert limit, time to alarm and risk integrity. These requirements come from GNSS rail user forum (Wiss et al. 2000) and

Table 1: Integrity recommendations for safety related railways applications (Wiss et al. 2000)

Applications	Integrity requirements		
	AL (m)	TTA (s)	Integrity risk (10^{-x}/h)
ATC on high density lines / Station / Parallel track	2.5	<1	1×10^{-7}
Train Control on medium density lines	20	<1	1×10^{-7}
Train Control on low density lines	50	<1	4.8×10^{-6}

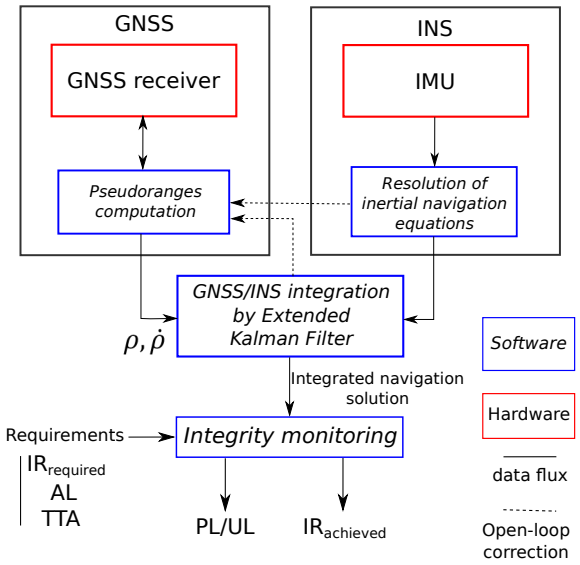


Figure 3: Architecture of GNSS/INS navigation system and integrity monitoring

summarise in table 1 (Note that, for the moment. They are not accepted requirements in railways just recommended). However, these values of requirements seem to be difficult to reach, particularly, time to alert, which appear very restrictive. In this paper, other values are proposed to be compatible with the European Railway Traffic Management System (ERTMS). According to the ERTMS performance requirements, $\boldsymbol{TTA}$ criteria such as those considered in Table 1 should be reviewed and sized in realistic way. Figures 4a and 4b propose to quantify the $\boldsymbol{AL}$ and $\boldsymbol{TTA}$ depending on emission ERTMS/ETCS messages delays from train to RBC (Radio Block Center). In consequence, four seconds is chosen for $\boldsymbol{TTA}$. Concerning $\boldsymbol{AL}$, the safety margin ($< \mathbf{20}$ m) constitutes a justified quantification. This margin refers to the reliability of braking system in ETCS system (Note that it should not be mixed up with the reliability of ETCS system) (Hougardy et al. 2012).

At the level of simulation, the probabilities are difficult to obtain. It is preferable to choose the term of occurrence rate, but that is easily linked to probability. Consider an event, $\boldsymbol{E}$, that occurs in some trials but not others. The probability of its occurrence in a trial is given by Equation 11.

$$\boldsymbol{Pb(E)} = \lim_{n \to +\infty} \frac{\boldsymbol{n_E}}{\boldsymbol{n}} \tag{11}$$

With, any $\boldsymbol{E}$ event, $\boldsymbol{n_E}$, the number of trials where event $\boldsymbol{E}$ occurs and $\boldsymbol{n}$, all the possible trials. About the simulation details, it is Matlab® routine simulating a mission with a duration of $\mathbf{8059}$s with a sampling of $\mathbf{0.20}$s.

4.2.2 *Safety quantitative results*

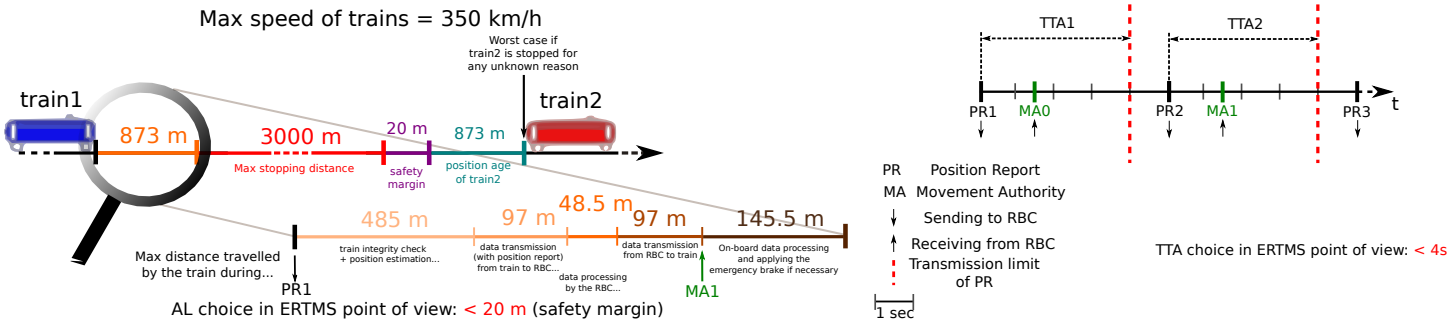
In Table 2, the results useful for $\boldsymbol{p(IR)}$ and, thank to the link described before, for safety (throughout $\boldsymbol{f_S(t_i)}$ are introduced. The different quantities in the table are means values during the simulation. According to this Table, the GNSS/INS localisation system reaches the integrity risk of 9.7214×10^{-5}. Thanks to Equations 7 and 10, the $\boldsymbol{f_S(t)}$ and $\boldsymbol{PFH}$ deduced from $\boldsymbol{p(IR)}$ are estimated respectively at 4.8607×10^{-6} (dimensionless quantity) and 2.1713×10^{-6} failure per hour. The following definitions seen in subsection 2.3, the SIL associated with this $\boldsymbol{PFH}$ is SIL1. However, SIL1 is not a sufficient level. The SIL required must be SIL4 to ensure the system is certified for safety-related railway applications. To achieve a SIL4 without compromising the availability, a 2oo3D (triple redundancy) or 2oo4D (quadruple redundancy) voting with diagnostic and map matching seems to be the best solutions for fault tolerance against dangerous detected or undetected failures (Ding et al. 2014).

5 CONCLUSION

In this paper, a quantitative safety evaluation of a localisation system based on GNSS has been proposed through the determination of its integrity risk. In a context of railway infrastructure optimisation (reduction of balises), the question of inertial systems performances must be asked as well as GNSS ones. In consequence, the integrity, firstly defined as a GNSS performance attribute, must be extended to inertial systems. After formalising this extended integrity, protection levels and integrity risk are computed about a tightly coupled GNSS/INS architecture. The architecture envisaged today in a lot of railway projects. Thanks to a probabilistic demonstration, a link between safety and integrity is proposed permitting us to eliminate the constraint of safety evaluation for the GNSS based localisation system through the incurred integrity risk.

6 ACKNOWLEDGEMENTS

The authors would like to thank the Technological Research Institute Railenium and the IFSTTAR for their



(a) Spatial justification (AL - Alert Limit) (b) Temporal justification (TTA - Time To Alert)

Figure 4: Integrity requirements proposed in ERTMS point of view

Table 2: Integrity and safety quantitative evaluation

System part	Integrity results				
	PL(part)	PL(system)	$p(IR)$	$f_S(t)$	PFH
GNSS	15.60	15.60	9.7214×10^{-5}	4.8607×10^{-6}	2.1713×10^{-6}
INS	6.61				

support in this work and the International Campus on Safety and Intermodality in Transportation (CISIT) and the European Commission via the European Regional Development Fund (ERDF) for making possible this work. The acknowledgements go also to the GEOLOC team from IFSTTAR-Nantes for GNSS and INS data and their help in using them in the present work.

REFERENCES

Beugin, J. & J. Marais (2012). Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization. *Transportation Research Part C: Emerging Technologies 22*(0), 42 – 57.

Bhatti, U. I. & W. Y. Ochieng (2007). Failure modes and models for integrated gps/ins systems. *Journal of Navigation 60*(02), 327–348.

CENELEC (2007). EN50126: Railway applications - the specification and demonstration of reliability, availability, maintainability and safety (RAMS). Brussels.

Ding, L., H. Wang, K. Kang, & K. Wang (2014). A novel method for SIL verification based on system degradation using reliability block diagram. *Reliability Engineering & System Safety 132*(0), 36 – 45.

European Railway Agency (2012, April). Memorandum of Understanding ERTMS. http://www.era.europa.eu/Document-Register/Pages/Memorandum-of-Understanding-concerning-ERTMS.aspx.

Gioia, C. & D. Borio (2015). Stand-alone and hybrid positioning using asynchronous pseudolites. *Sensors*.

Groves, P. (2013). *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems, Second Edition:*. GNSS/GPS. Artech House.

Hougardy, A., A. Chiappini, & P. Guido (2012). Introduction to ETCS braking curves. Technical report, European Railway Agency.

ICAO (2006). International standards and recommended practices. Technical report, International Civil Aviation Organization.

Jonas, M. (2014, May). Integrity enhancement of the GNSS position solution for the railway applications. In *Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION*, pp. 839–845.

Le Marchand, O. (2010, June). *Autonomous approach for localization and integrity monitoring of a ground vehicle in complex environment*. Theses, Université de Technologie de Compiègne.

Le Marchand, O., P. Bonnifait, J. Ibaez-Guzman, & D. Betaille (2009, Oct). Vehicle localization integrity based on trajectory monitoring. In *Intelligent Robots and Systems, 2009. IROS 2009. IEEE/RSJ International Conference on*, pp. 3453–3458.

Liu, H., G. Zheng, H. Wang, & C. Feng (2010). Research on integrity monitoring for integrated gnss/sins system. In *Proceedings of the IEEE International Conference on Information and Automation*.

Lu, D. & E. Schnieder (2014). Performance evaluation of GNSS for train localization. *Intelligent Transportation Systems, IEEE Transactions on PP*(99), 1–6.

Nikiforov, I. V. & F. Choquette (2003). Integrity equations for safe train positioning using GNSS. In *Proceedings of the European Navigation Conference*.

Ochieng, W. Y., S. Feng, T. Moore, C. Hill, & C. Hide (2008). User level integrity monitoring and quality control for high accuracy positioning using gps/ins measurements. *Journal of Global Positioning Systems 7*(2), 104–114.

Peters, M. E., R. M. Gates, & M. Chertoff (2008). Federal radionavigation plan. Technical report, Departement of Defense and Department of Homeland Security and Department of Transportation.

Rispoli, F., A. Filip, M. Castorina, G. D. Mambro, A. Neri, & F. Senesi (2013). Recent progress in application of GNSS and advanced communications for railway signaling. In *23th Conference Radioelektronika, Pardubice, Czech Republic*.

Salvatori, P., A. Neri, C. Stallo, V. Palma, A. Coluccia, & F. Rispoli (2014, Sept). Augmentation and integrity monitoring network and EGNOS performance comparison for train positioning. In *Signal Processing Conference (EUSIPCO), 2014 Proceedings of the 22nd European*, pp. 186–190.

Wiss, J., G. Barbu, P. Frsig, M. Schrder, C. Edwards, K. Walter, A. Filip, A. Sage, & S. Forsyth (2000). GNSS Rail User Forum: Requirements of Rail Applications. Technical report, European GNSS Secretariat.

Woodman, O. J. (2007). An introduction to inertial navigation. Technical report, University of Cambridge.