# Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications

Julie Beugin, A. Filip, Juliette Marais, M. Bernibeau

# Galileo for railway operations: question about the positioning performances analogy with the RAMS requirements allocated to safety applications

Julie Beugin[a,*], Aleš Filip[b], Juliette Marais[a], Marion Berbineau[a]

[a] *Univ Lille Nord de France-F-59000 Lille, INRETS, LEOST, 20 rue Elisée Reclus, BP 317, 59650 Villeneuve d'Ascq, FRANCE*

[b] *RAILWAY INFRASTRUCTURE ADMINISTRATION, TÚDC, LIS, Hlavacova 2801, 530 02 Pardubice, CZECH REPUBLIC*

Tel.: +33-3-20-43-85-05

Fax: +33-3-20-43-83-97

E-mail addressees: julie.beugin@inrets.fr ; ales.filip@tudc.cz ; juliette.marais@inrets.fr ; marion.berbineau@inrets.fr

Abstract: GNSS is penetrating, surely but certainly, the railway market. Introduction is performed through non safety oriented applications such as fleet management or passenger information. However, a huge panel of safety applications could take advantage of this technology. Galileo will soon complement the navigation satellite offer, monopolized today by GPS. Some issues have to be studied before safety uses: performance requirements have to be expressed, cost benefit analysis has to prove advantages compared to installed equipment… But one of the main issues concerns safety proofs that have to be in accordance with European railway standards. Today, Galileo is not yet deployed but specifications are available. However, such specifications have been mainly driven by aeronautics and the transposition of such specifications into classical RAMS standards is not obvious. This paper presents these issues and a methodology proposed to answer the specific RAMS question.

*Keywords: Satellite-based localization, railway transportation system, RAMS analysis*

## Introduction

Contrary to what the general public may think, railways are part of the technological race of transportation systems. In particular, if Galileo has been essentially driven by aeronautical actors, railways demonstrate their interest for this localization technology. Some applications are already ongoing. They rely for the moment on GPS (American), which is the only fully operational system, while Galileo (European) is under development and Glonass (Russian) under renewal.

Most of them are non-safety-related, such as passenger information or cargo management. However, in the US, where the railway network differs strongly from the European one, some control and command systems are now based on GPS, enhanced by the NDGPS (Nationwide Differential GPS), which is a network of reference stations allowing the receiver to have better performances.

In Europe, developments on the operational network have been slow but, for a few years, European projects like LOCOPROL or GADEROS have highlighted the potential of GNSS (Global Navigation Satellite System) for more constraining applications like safety-related applications.

However, some major issues remain, in particular, whether or not performances provided by GNSS services can meet railway safety requirements. Recent confirmation of the good progress of the Galileo program encourages research teams and the railway industry to pursue their efforts in this direction.

In this paper, we will present both the Galileo offer and railway issues. The main question deals with certification of GNSS solutions for safety-related applications. For this task, railway standards have to prove that, even in case of failures, the system studied is able to guarantee a given level of performances expressed in the railway domain in terms of RAMS attributes (Reliability, Availability, Maintainability and Safety). The second section will analyse the specific errors related to GNSS to show when failures of the positioning service can occur and degrade performances. Finally, the last section gives elements to realize safety assessment and evaluate the RAMS, the results of these two tasks being beyond the scope of this paper. In this section, it is explained how the specifications of the navigation services can be used for conducting such evaluations, especially the Galileo quality criteria that are defined in Galileo specifications.

# 1. Using Galileo for railway operations

Most of the Galileo specifications are defined in (ESA 2002), in terms of services and technical requirements. The goal of this paragraph is to face both Galileo services and railway needs in order to highlight the potential benefits of using GNSS for such transport mode. The first paragraph will recall Galileo services and signals. Then, railway requirements will be summarized even if specifications vary strongly according to the application. Finally, issues will be highlighted and some answers will be given when describing some of the research projects in progress.

## 1.1. The Galileo services

In the common language, a GNSS receiver is today called “a GPS” due to the monopoly of GPS, the only fully operational constellation available today. This constellation, managed by the American Department of Defense (DoD), provides a permanent four-dimensional positioning service (longitude, latitude, height and time) under all weather conditions and in all places.
In the near future, GPS will cohabit with other constellations. Indeed, the Russian Space Agency intends to expand the GLONASS constellation from the current 19 satellites to 30 by 2011. A Chinese competitor called BEIDOU or COMPASS is also believed to be under development. In 2008, BEIDOU is composed of geostationary satellites devoted to augment GPS performances, as EGNOS does in Europe or WAAS in the USA, but, officialy, a global competitor system is announced in the coming years.

For economic, societal, political, as well as technological, issues, Europe decided in the 1990s to develop its own satellite navigation system, called Galileo. This upcoming localization system will provide five different services with different performances and characteristics that will be suitable for different ranges of applications:

- The Galileo Open Service (OS), which will be the elementary service (similar to the SPS service of the GPS).
- The Safety of Life service (SoL), which will provide a guarantee of integrity.
- With the Commercial service (CS) and for a fee, users will benefit from two additional signals to improve accuracy.
- The public regulated Service (PRS) will provide a continuous availability of the signals in the presence of interfering threats. It is especially dedicated to governmental applications.
- The Search and Rescue service (SAR) will be a contribution to the existing COSPAS/SARSAT for emergency distress messages detection.

GPS and Galileo systems will be interoperable. Compatible receivers will therefore benefit from greater service volume, availability and accuracy.
The Open Service will have close characteristics with the public service of GPS. Using integrity added-values, the SoL service will give guarantees for safety applications and is the most able to convince railway users (the paragraph 2.2 of this article explains in details integrity concepts).

After this brief Galileo presentation, railway issues will be described in order to identify convergences.

### 1.2. Current railway needs

The objective of this paragraph is to present the reasons for making GNSS penetrate the railway systems. These reasons mainly emanate from the localization constraints the railway users are faced with.

The first reason is cost-driven as shown in these three situations:

- New technologies make possible the introduction of intelligent and communicating trains and wagons on the railway network. The new services offered enhance attractivity and impose a strong competitive position. This can considerably improve service quality by informing and localising wagons and corresponding materials or to verify available equipment etc.
- With separation of infrastructures and operation, railway users pay the infrastructure owner for the circulation of trains and energy consumption. GNSS-based positioning information contributes to energy tolling for developing an adapted toll for railways.
- High costs relative to the installation of signalling equipment on track and their maintenance are not compensated for traffic revenues, especially in the case of low traffic density lines. This is critical because some of the European networks are threatened with closure for economic reasons. We can mention as an example, the German case where more than 5,000 km of lines have been closed in the past 16 years, i.e. 10%. Even if the investment costs will not be negligible to equip each locomotive with GNSS receivers, the maintenance costs are expected to be much lower.

The second reason is technological. Historically and technically, each country has developed its own railway networks. The consequences are that the amount of equipment is as large as the number of countries. This is the case for infrastructure, energy (electrification at 25, 15, 3 and 1.5 KV, + 750V), rolling stock, maintenance and exploitation rules, as well as signalling systems. Now that trains are running over borders, Europe has developed a system called ERTMS to harmonize equipment and signalling rules. The possibility of using GNSS is envisaged in ERTMS level 3 scenario for ensuring localization functions of the ERTMS/ETCS signalling system. GNSS are global systems that will not only contribute to answer interoperability needs but also to increase capacity of lines. Indeed, GNSS will permit trains to localize autonomously and with ERTMS/ETCS, positions obtained on board trains can be transmitted to the ground via GSM-R. This will optimize traffic because intervals between trains will be dynamically determined using moving block principle instead of fixed blocks. Modifying the signalling system that controls train traffic will have an impact on the following safety functions, which rely on this system and which are based on localization:

- Controlling that no train exceeds its own speed limit nor the different speed limits assigned to the various track sections,
- Controlling that each train proceeds in the correct direction and remains within a limited authorized zone, called the movement authority,
- Controlling that each train is assigned a zone and each zone contains one and only one train,
- Controlling that each train's movement authority is correctly established, meaning i) that sufficient protections have been set to forbid the entrance of other trains into a zone that has been assigned to a specific train, and ii) that the points of the different switches are blocked in the correct position so that the train moves along its planned itinerary (with signalling and interlocking equipment),
- for railway transportation systems that interact with road traffic, controlling that each level-crossing train barrier is in the correct position to protect people and vehicles during the passage of the train, and,
- Verifying that no object or person is on the track in front of the train.

In the case of technology migration with GNSS-based equipment, all these safety functions have to be performed following high safety requirements. Equipment has also to be designed according to the principles of functional and technical safety described in European railway standards (EN 50126 2000)(EN 50129 1999). In these standards, SILs (Safety Integrity Levels) serve as safety targets. They are discrete indicators on a four-level scale. On this scale, SIL 1 is the weakest safety requirement and SIL 4 is the most restrictive. Signalling functions have mostly to be proved to meet a SIL 4 level. For the moment, GNSS-based standalone solutions, i.e. not enhanced with other sensors, are not developed under safety principles, as is the case for transmission systems mentioned in the 50159 standard (EN 50159 2001). SIL 0 is used to characterize such systems with no safety requirements.

The following paragraphs explain why it is difficult to certify GNSS-based solutions for railway safety-related applications. Before the different solutions that have been explored by the railway community will be described.

### 1.3. European research answers

Before describing some of this research, one should highlight that, contrary to aeronautical or maritime domains, railways do not have common rules and therefore, common requirements. If the UIC's (International Union of Railways) role is to facilitate the sharing of best practices among members, there is no equivalent to ICAO (International Civil Aviation Organization) or IMO (International Maritime Organisation). Such organizations have defined precise technical requirements for most of their function. In the railway community, there is no specifications table shared by the entire community, in particular for the localisation function. Each of the following projects has brought its own requirements.

Some of years ago, the European Commission started to support research on GNSS in railway transportations. With the idea of preparing the arrival of Galileo, the first objective of projects was to experiment and prove that satellites could offer new services to railway users, based on the existing GPS constellation.

APOLO, LOCOPROL or GADEROS were pioneering projects in Europe. They have explored different GNSS-based solutions with different constraints. The three intended to comply with ERTMS/ETCS deployments. However, GADEROS has developed a multisensor solution based on Galileo SoL signals.

In LOCOPROL, a low cost GPS-only based solution was developed, which was aided by EGNOS when available along tracks. In this solution, as GPS does not offer any service guarantee, the chosen solution (patented by Alstom) relies, not on a typical GNSS computation, but on the use of independent pairs of GPS signals, in order to reach a required safety target (Nikiforov and al. 2003). Thus, a TDOA (Time Difference of Arrival) technique has been applied (Marais and al. 2003). The performances of the LOCOPROL positioning algorithm have been studied in the LOCOLOC project (LOCOLOC. 2004). Fault trees taking into account classical GNSS measurement errors but also signal perturbations and trainborne equipment, have shown that positions, obtained with the 1D hyperbolic algorithm, met a SIL 4 objective (probability of failure lower than $10^{-11}$/h).

The EGNOS COntrolled RAILway equipment (ECORAIL) project, finished in 2005, focused on accuracy. Indeed, it aimed at providing an on-board unit that was able to determine the position of a train on the track with sufficient accuracy and reliability to be used for railway control purposes.

The GRAIL consortium funded by the 6th Framework Program attempted to achieve common specifications (agreed by users and industry) for the GNSS subsystem dedicated to the odometry function (GRAIL 2007). The objective was to examine how GNSS can complement an odometry system.

New issues appeared during these projects: standardization of interfaces and specifications, and mainly, the difficulty of proving safety for GNSS-based solutions for certification.

## 1.4. Issues related to RAMS evaluation, safety proofs and certification

With the integrity added-value delivered by the Galileo SoL service, more possibilities will be provided to the safety-related GNSS-based applications, especially the possibility to detect positioning failures when biases occur in signals. But problems provoked by reception environment are not resolved.

Furthermore, Galileo specifications have been essentially driven by aeronautic users (cf. paragraph 2.3). They have no equivalent in the railway domain where definitions of specifications are different and expressed in terms of RAMS.

Another issue concerns certification. Indeed, as railway equipment has to be certified by a notified body before being installed on tracks or embedded into trains, GNSS infrastructures will also have to be certified as well as the receivers based on its services. One main difference is that GNSS is not at all under railway control. A certification process is ongoing at the European level. The GALCERT program has been funded to support it, taking into account the diversity of the different transport modes. Its role is to ensure that the components of the system are certified, and, in particular the SIS (Signals In Space). One of the railway tasks is to take part in it in order to understand and accept it (Barbu 2008).

Before closing this paragraph, one should also mention the acceptance issue. Indeed, migration from track-circuit technology, providing discrete positioning, to GNSS technology, providing continuous positioning, represents a big break. Instead of controlling the complete equipment, GNSS will constrain the railway community to be confident in a completely external process… This will remain an important point in the coming years. Such issues will rely on the capacity of projects and first demonstrators to convince, i.e. to prove that the system will be as good, safe, cheap, and reliable as the previous ones.

Thus, several tasks are fundamental:

- define GNSS performances into an acceptable railway language,
- develop methods and tools able to perform evaluation in an operational railway context. Experimental solutions are in progress (Poliak *et al.* 2008),
- evaluate RAMS of the trainborne GNSS solution according to railway safety standards.

The second section of this article describes how to perform a RAMS analysis for solutions based on Galileo (the third point). To conduct such an analysis, the specifications defined in Galileo documentation are examined and their equivalence with railway specifications is explained (the first point).

# 2. About RAMS analysis on a Galileo-based solution

## 2.1. RAMS analysis of GNSS-based equipment under design

Before including new equipment or functions in a railway safety-related system, the RAMS attributes of these equipment or functions need to be quantified at the design level of the life cycle, as demanded in the EN 50126 standard (2000). The objective is to measure the confidence that can be placed in the new system, especially when it is dedicated to safety operations. A RAMS analysis examines firstly all known failure causes and failure modes of the system (possible failure states of the system) by means of dependability methods like the fault tree method, FMECA (Failure Mode, Effects, and Criticality Analysis), reliability block diagram… Particular attention is paid to the different failure combinations that can lead to the failure of the studied system or the loss of the final output. The analysis can then use the failure rates and the logical combination of each part of the system to achieve the RAMS attributes evaluation.

The system studied, in this article, is the satellite-based positioning solution using the Galileo SoL service and performed by equipment that could be integrated in a railway signalling system. If the quantification of the RAMS attributes of the positioning function shows that the railway positioning requirements are not fulfilled, the Galileo SoL service cannot be the only means of localization in the railway safety application. We explain below why the RAMS analysis realized on a satellite-based positioning function is special compared to classical analyses.

## 2.2. Particularities of the RAMS analysis

### *2.2.1. Failure cause analysis of the positioning function*

The function that will provide position for railway applications is here analysed to show how it can fail. A failure occurs when the difference between the position calculated by the user and its true position is greater than a threshold defined in the application. As the receivers are not able to calculate this error, it remains unknown for the user.

The position failure is a feared event for the user, i.e. an hazard for the safety-related railway application. It may result from software or hardware failures that occur in any of the three GNSS segments (ground control, satellite and user segments). It can also be the result of specific causes that are not common in RAMS evaluation methods (Beugin & Marais 2008): errors that affect satellite signals (or SIS). We classify these errors in two categories:

- Errors due to perturbations in signal propagation. Indeed, pseudo-ranges (estimation of the satellites/receiver distances by the receiver) used to calculate a position rely on propagation time measurements. As seen in the first section, the close environment of the receiver has an impact on signal propagation. It induces delays and multipath that can degrade the measurement of pseudo-ranges.
- Errors in signal data (navigation message). These data (ephemeris, satellite clock correction), used for satellite location can be corrupted.

Thus, additionally to the common software and hardware failures present in ground, satellite and receiver equipment, the RAMS evaluation has to consider the specific errors that are present in signals and that lead to a position outside the user accuracy requirements (a position failure).

Later on in this article, software and hardware failures will be supposed to be controlled by operators in charge of the different respective infrastructures. Indeed, as mentioned in paragraph 1.4, GNSS infrastructures are not under railway control. Thus, we focus on the main research issue: the RAMS evaluation given SIS errors and existing GNSS specifications.

### *2.2.2. Diagnostic mechanism to detect a position failure*

Within the Galileo SoL service, each SIS will be associated to an integrity message. With this message, receivers will be able to detect a position failure. However, the entire diagnostic mechanism of the Galileo system (diagnostic algorithm in receiver, integrity data in the navigation message, monitoring at ground segment level) is not fault-free, given the following causes:

- at user level, the receivers can use a failing signal (which includes data noise or bias) in the position computation without detecting it;
- integrity data can be corrupted through degraded uplink between ground and satellite segments;

- integrity data can be incorrect through independent and common cause failures stemming from the monitoring system at the ground segment.

Therefore, diagnostic failures must also be taken into account in the global analysis.

Consequently, we distinguish two generic cause events leading to position failure:

- Integrity events: these events occur when a failure exists and has not been detected by the diagnostic mechanism,
- Continuity events: these events occur when the positioning function is interrupted because of signal generation and propagation problems, poor receiver-user geometry, etc. It includes events that have been detected by the diagnostic mechanism.

Accuracy, integrity, continuity and availability concepts are in fact the quality criteria commonly used for describing the performances provided by a GNSS. Expected performances of on-board Galileo-based equipment have been defined in the Galileo specification documents (ESA 2002). They can be used to describe the RAMS attributes associated to the Galileo positioning function. We explain below how this is done. We will show why the analogy between the two classes of quality criteria is not immediate but possible. It requires the background of the GNSS quality criteria to be explained. This will be presented in the last section of this article with a methodology to prove the analogy.

### 2.3. Why are Galileo performance requirements different from RAMS objectives but also analogous?

The specifications of the Galileo SoL service in terms of accuracy, integrity, continuity and availability are presented in table 1. No equivalent specifications are defined in railway domain to characterise what users expect from localization, so no comparison is possible.

Table 1 shows the three categories of requirements that have been identified according to the needs set forth by different applications. They especially cover the diverse safety constraints the users' community meet (ESA 2005). In the case of the railway community, the needs for safety applications are expected to be covered by the level associated to the more constrained requirements: level A.

Table 1: Performance requirements for the Galileo SoL service

| | Level A requirements | Level B requirements | Level C requirements |
|---|---|---|---|
| **SIS integrity risk** | 2.0 $e^{-7}$ in any 150 sec | 1.0$e^{-7}$/ 1 h | 1.0$e^{-5}$/ 3 h |
| **Continuity risk** | 8.0$e^{-6}$ in any 15 sec | 1.0$e^{-4}$ to 1.0$e^{-8}$ / 1h | 3.0$e^{-4}$ / 3 h |
| **Availability of service** | 99.5 % | 99.5 % | 99.5 % |
| **Time to alarm** | 6 sec | 10 sec | 10 sec |
| **Accuracy (95%) H / V** | 4 m / 8 m | 220 m / NA | 10 m / NA |
| **HAL / VAL*** | 40 m / 20 m | 556 m / NA | 25 m / NA |

*Horizontal and vertical alarm limits

However, these requirements have mainly been proposed to support aeronautical operations (ranging from en-route phase to approach operation with vertical guidance, called APV II). In fact, continuity requirements were introduced for the first time in aviation in the late 1960s to define precise approach requirements for a radio navigation system, called the Instrument Landing System (ILS). The purpose was to describe the quality of service during a most critical phase of operation (e.g. 15s for the precise approach phase of an aeroplane before landing, duration in which service interruption is dangerous). Continuity requirement was derived by means of a risk allocation from the Target Level of Safety (TLS), whereas TLS results from statistical analysis of historical accident data of aeroplanes for a given period. In 1993, the ICAO's Air Navigation Commission requested All Weather Operations Panel (AWOP) to examine the possibility of extending the Required Navigation Performance (RNP) concept, which was originally intended for en-route operations, to include approach, landing and departure operations. At that time, it was proposed to use the accuracy, integrity, continuity, and availability quality criteria that were later retained for GNSS.

As GNSS requirements are driven by aeronautical needs, the railway community encounters difficulties to adapt them for train positioning purposes. For example, no phases of operation can be distinguished when trains are running; requirements are only defined at the sub-system or function level. In safety applications, as mentioned previously, requirements are expressed differently using RAMS attributes and a process for their specification and demonstration is exposed in CENELEC standards (EN 50126 2000)(EN 50129 1999). So, the safety philosophies in railway and aeronautical domains are different and the quality criteria are not interchangeable, considering they are not defined with the same objective.

In spite of this, a mutual relation among Galileo quality criteria and RAMS attributes exists because both criteria are associated to probabilities, which show the confidence we can have in the system, and the risks the system can generate. Dependences are felt *a priori*.

The next section presents how to demonstrate the dependences between the two classes of quality criteria in order to allocate RAMS objectives to the Galileo-based positioning receiver. The demonstration is based on identification of the failure modes of the Galileo output function and on the probability associated to each of them.

# 3. Methodology to demonstrate the relation between the Galileo SoL performances and the railway RAMS attributes

In this part, GNSS quality criteria will be explicitly linked up to the reliability and availability attributes of the RAMS ones. Links exiting between these attributes and the maintainability and safety of GNSS will be presented given that railway RAMS are inter-linked as it is described in the EN 50126 standard.

## 3.1. Failure modes analysis and corresponding probabilities

The position error PE is the difference in meters between the estimated and exact positions. Users consider that an estimated position is correct or accurate as long as PE, which value is variable in time, is maintained within a user defined alert limit AL, i.e. $PE \leq AL$. On the contrary, as long as a position is such as $PE>AL$ (the duration of this condition is unpredictable), the safety of the entire transportation system is degraded.

Some railway requirements have been defined during Rail Advisory Forum (Wiss and al. 2000). An extract concerning AL threshold, especially defined according to the horizontal component (because train run is considered in 2D), is illustrated in table 2. Different types of operating conditions have been considered inside.

Table 2: Rail Advisory Forum requirements on AL

| Safety-related applications | | |
|---|---|---|
| **Operating conditions** | **Examples** | **Horizontal Alert Limit –HAL** |
| I. High density lines | Train control on I / station / parallel track | 2,5 m |
| II. Middle density lines | Train control on II | 20 m |
| III. Low density lines | Train control on III | 50 m |

The following failure modes can then be distinguished given that a failure detection mechanism is used:

- the safe detected failure modes. Probability $PF_{SD}(t)$ represents a probability that PE≤AL, and that an alert is raised due to a failure of diagnostics. False alert is then announced.
- the safe undetected failure modes. Probability $PF_{SU}(t)$ represents the probability of a non-critical failure when PE≤AL, but no failure is announced by built-in diagnostics. In this case, a safe failure in the system exists but the user does not know about it. It can be revealed by an independent diagnostics based on physically diverse sensors, but it is beyond the scope of this paper.
- the dangerous detected failure modes. Probability $PF_{DD}(t)$ represents the probability that PE exceeds AL and this state is detected as hazardous. Then, it is a dangerous detected failure (true alert).
- the dangerous undetected failure modes. Probability $PF_{DU}(t)$ represents the probability that PE exceeds AL without detection. This dangerous undetected failure is the most feared failure of the system.

All possible sequences of failures are represented using the consequence diagram in figure 1.

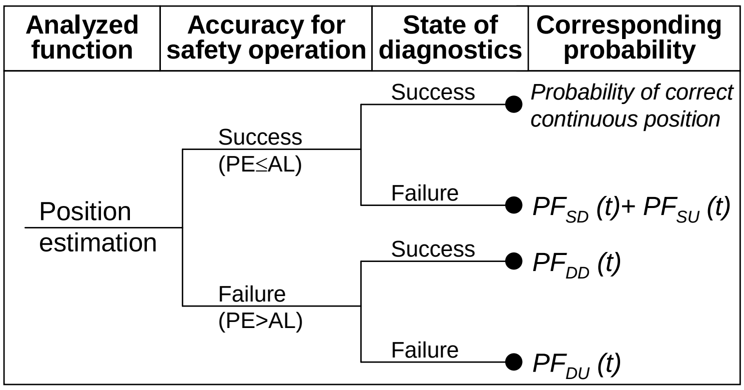


Figure 1: Consequences diagram of the Galileo positioning function

How the defined probabilities of failure modes are associated to the Galileo quality criteria probabilities is detailed below.

## 3.2. Probability associated to Galileo quality criteria

### *3.2.1. Integrity quality criterion*

The integrity of service is guaranteed when the GNSS receiver provides correct information. The probability $IR(t)$ is the measure of integrity risk. It refers to the probability of the incorrect position due to the failures mentioned in the cause analysis of section 2. Therefore, the probability of dangerous undetected failures describes the integrity risk, i.e. $IR(t) = PF_{DU}(t)$.

### *3.2.2. Continuity quality criterion*

The continuity of service is guaranteed when the GNSS receiver provides the following during operation: (1) navigation accuracy and (2) accuracy guarantee (i.e. integrity) within a stated period of time [0,t]. Probability $C(t)$ is the measure of continuity. Continuity risk $CR(t)$ is the complement of $C(t)$, i.e. $CR(t) = 1 - C(t)$. Loss of SIS continuity described with $CR(t)$ is caused by unscheduled interruptions due to internal failure in the detection mechanisms and not by shadowing objects along the track, which are easily predictable.

Probability to provide a continuous correct position (PE≤AL) refers directly to the reliability $R(t)$ because the reliability is defined as the probability that an item can perform a required function under given conditions for a given time interval [0,t].
A continuous correct position is obviously not provided by GNSS when a failure is detected and notified. Therefore, probability $PF_{SD}(t)$ i.e. probability of false alert, and $PF_{DD}(t)$ i.e. probability of true alert, that are both related to the interruption of service are such as: $CR(t) = PF_{SD}(t) + PF_{DD}(t)$. Undetected failure modes, represented by probabilities $PF_{DU}(t)$ and $PF_{SU}(t)$, exist during position determination since user does not know them.
Finally, the total probability of continuous provision of position with acceptable integrity of service is $C(t) = R(t) + PF_{SU}(t) + PF_{DU}(t)$. $C(t)$ is not only equal to $R(t)$ as position is also provided when a failure is not revealed by GNSS

diagnostics. It is obvious that undetected failures (DU, SU) can be revealed by additional diagnostics based on physically diverse sensors.

Note that dangerous detected failures (true alert) are not as dangerous as dangerous undetected failures. They can be converted to fail-safe state. For example, a train can be stopped. However, it shall be done only in an extreme case, if no other possibility exists. Relatively frequent interruptions of Galileo Signal-In-Space SoL Level A Service (MTBF=521 hours) can be substituted by a relative position determination, by means of sensors (Filip 2007).

### *3.2.3. GNSS availability quality criterion*

GNSS service is available if the requirements of accuracy, integrity and continuity of the positioning function are met. It deals with the correct operation of the service at a given instant *t* and at a given location. The availability is, therefore, time- and space-dependent.

## 3.3. Positioning performances analogy with the RAMS requirements

### *3.3.1. Reliability of the positioning function*

The reliability $R(t)$ of the positioning function is a measure of success on the operation time interval [0,t]. It can be expressed as $R(t) = 1 - (PF_D(t) + PF_S(t))$. We can define the probability of failing safely: $PF_S(t) = PF_{SD}(t) + PF_{SU}(t)$ that is the probability on the time interval [0,t] that PE≤AL, and the probability of failing dangerously: $PF_D(t) = PF_{DD}(t) + PF_{DU}(t)$ that is the probability on the time interval [0,t] that PE>AL. Given $IR(t) = PF_{DU}(t)$, then $PF_D(t) = PF_{DD}(t) + IR(t)$. The unreliability $F(t) = 1 - R(t)$ is a measure of failure in time interval [0,t]. It represents PE exceeding AL and/or a diagnostic failure. It can be expressed as $F(t) = PF_D(t) + PF_S(t)$. Thus unreliable position is described by the failure modes which are represented by probability $PF_{SD}(t)$, $PF_{SU}(t)$, $PF_{DD}(t)$, $PF_{DU}(t)$ on top of the Venn diagram in figure 2. This figure shows the relation between the failures modes probability of the positioning function and the GNSS quality criteria. It also shows the relation between the failures modes and the reliability and safety attributes.

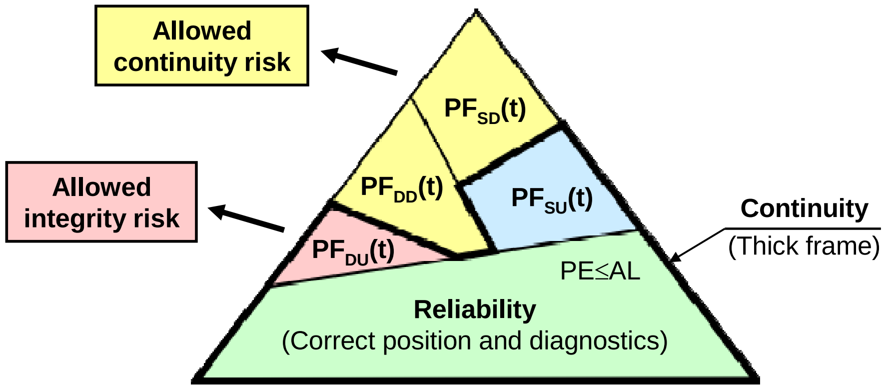


Figure 2: Illustration of the analogy between GNSS criteria and the reliability and the safety of the position

Note that real systems can stop providing accuracy or integrity independently. In the case of dangerous detected failure $PF_{DD}(t)$, accuracy can be lost (PE>AL) while integrity (timely warning) is provided. Alternatively, in the case of safe undetected failure $PF_{SU}(t)$, accuracy is provided (PE≤AL) even if the ability to provide timely warnings is lost. In this case, the user considers that system integrity is correct since he receives an integrity message without any warning. Therefore, we can distinguish three kinds of continuity: (1) Continuity of Accuracy, (2) Continuity of Integrity of Accuracy, and (1+2) Continuity of Service. In the case of GNSS safety applications, (1+2) should be considered (Filip *et al.* 2008).

### *3.3.2. GNSS availability versus quality of signalling system in terms of the availability and maintainability attributes*

According to a RAMS point of view, service is available if a GNSS system is correctly operating at time *t*. No requirement for successful operation at a specific moment of time is directly involved in GNSS availability. However, a condition of continuous successful operation within a specific time interval [0,t] is involved in a lower rung, in the continuity requirement. A system can also be accurate, have high integrity and continuity, but it can be down e.g. 1 month per year. maintainability must be assured. When maintainability is considered together with other quality criteria, then we talk about availability of continuity, availability of integrity, etc. GNSS availability at user level also implies that GNSS receiver is able to predict accuracy, integrity and continuity performance over the next critical operation period and the predicted values must not exceed the specified values.

The availability $A(t)$ according to EN 50126 is a combination of reliability and maintainability. The safety attribute is not included in the railway availability even if both are dependent. In relation to railway safety-related systems, we usually talk about dependability and safety distinctly. $A(t)$ depends on correct position determination, correct function of diagnostics and maintainability $M(t)$ of GNSS system. It can be written as $A\{t|M(t)\}$. Availability $A\{t|M(t)\}$ can be evaluated by means of the unavailability, the probability of incorrect operations $U\{t|M(t)\}$ under condition that maintainability $M(t)$ is provided ( $\forall t, M(t)=1$).

Probability of incorrect operations of GNSS system can be determined from given integrity risk $IR(t)=PF_{DU}(t)$ and continuity risk $CR(t) = PF_{DD}(t) + PF_{SD}(t)$ as $U\{(t|M(t)\} = IR(t) + CR(t) = PF_{DU}(t) + PF_{DD}(t) + PF_{SD}(t)$. The probability $PF_{SU}(t)$ remains and is considered as being part of the reliability part $R(t)$ . This simplification can be done since correct position is provided. Then availability $A\{t|M(t)\}$ can be expressed as:

$$\begin{aligned} A\{t|M(t)\} &= 1-(PF_D(t)+PF_S(t)) = 1-(PF_{DU}(t)+PF_{DD}(t)+PF_{SD}(t)+PF_{SU}(t)) \\ &= 1-(IR(t)+CR(t)+PF_{SU}(t)) \approx 1-(IR(t)+CR(t)) \end{aligned}$$

### 3.4. Quality attributes of GNSS-based railway signalling

The use of the GNSS quality criteria within railway RAMS is proposed in figure 3. It results from analysis of GNSS integrity and continuity risks performed above.

In railway safety-related systems, a failure rate per hour shall be used, instead of a probability per duration of operation for purpose of a quantitative safety analysis. Indeed, SIL requirements (cf. paragraph 1.2) are quantitatively defined using Tolerable Hazard Rate (THR) and, also, as mentioned above, no phases of operation can be distinguished in railway systems. An approach to convert GNSS integrity risk to THR and so to a SIL has been proposed in (Filip 2007).

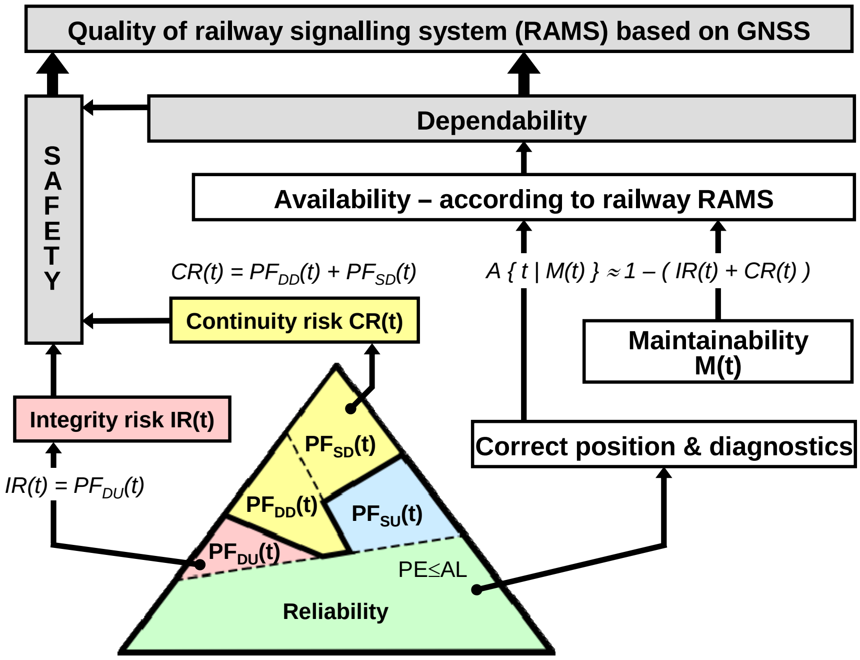


Figure 3: GNSS quality criteria within railway RAMS

# 4. Conclusion and prospects

Up to now, GPS has convinced a lot of users about feasibility and efficiency of non-safety solutions based on satellite navigation for land transportation. However, due to the intended provision of the Galileo SoL service in the coming years, it is expected that the Galileo system (or Galileo together with GPS) will be implemented in European railway safety-related systems rather than standalone GPS. Current development in GNSS technology and existing standards dedicated to safety applications clearly show that main leader in this field is the aeronautical community.

In this paper, we have, in particular, highlighted the question of the safety assessment. Two main axes are concerned. The first deals with the question of the RAMS evaluation of the satellite-based location function delivered to a railway application, as recommended by railway safety standards. The second concerns the relation that can be established between the Galileo specifications, mainly expressed according to aeronautical needs, and the railway RAMS attributes.

The railway community has discovered the great potential of GNSS rather late. Nowadays, railways are no longer in position whether to accept or not a „gift“ from the aeronautical/GNSS industry in the form of the Galileo system with its

SoL service. But the question remains: how to use this gift for railway safety applications according to railway safety standards. Railway operators, infrastructure authorities, railway industry, research institutions and other railway actors support this concept. This paper can be considered as a contribution to this effort.

## References


Barbu G. (2008) GNSS / GALILEO certification for rail safety applications Railway requirements and the strategic position of UIC. Proceedings of WCRR 2008, Seoul, Korea.

Beugin J., Marais J. (2008) Application des principes de la sûreté de fonctionnement à l'évaluation du service de localisation par satellites dans le domaine ferroviaire. Recherche Transports Sécurité n°99, Lavoisier, pp 89-103.

EN 50126 (2000) Railway Applications: The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS). CENELEC European standard (European Committee for Electrotechnical Standardization).

EN 50129 (1999) Railway Applications: Safety related electronic systems for signalling. CENELEC European standard (European Committee for Electrotechnical Standardization).

EN 50159 (2001) Railway Applications: communication, signalling and processing systems: safety-related communications in closed (part 1) and in open (part 2) transmission systems. CENELEC European standard (European Committee for Electrotechnical Standardization).

ERTMS/ETCS RAMS Requirements (1998) Chapter 2 – RAM. Version 6.

European Space Agency (2002) Galileo Mission High Level Definition 3.0, http://ec.europa.eu/dgs/energy_transport/galileo/doc/galileo_hld_v3_23_09_02.pdf, Directorate-General Energy and Transport.

European Space Agency (2005) Galileo Integrity concept. Galileo Project Office Documentation, ESA-DEUING-TN/01331, Issue 1, Revision 2.

Filip A. (2007) Safety Aspects of GNSS Based Train Position Determination for Railway Signalling. UIC GALILEO for Rail Symposium, Paris, France.

Filip A., Beugin J., Marais J., Mocek H. (2008) Interpretation of the Galileo Safety-Of-Life Service by Means of Railway RAMS Terminology. International scientific journal Transactions on Transport Sciences vol. 1-num. 2, Czech Ministry of Transport, pp 61-68.

GRAIL (2007) GNSS introduction in the RAIL sector: GNSS subsystem requirement specification for enhanced ETCS applications. Report, project funded by the Galileo Joint Undertaking, 6th framework program.

LOCOLOC (2004) System Preliminary Safety Case, version 2.1, Restricted report, project funded by ESA, Aug. 2004.

Marais J., Berbineau M., Frimat O., Franckart J.-P. (2003) A New Satellite-Based Fail-Safe Train Control and Command for Low Density Railway Lines. Proceedings of the TILT conference, Lille, France.

Nikiforov I., Choquette F. (2003) Integrity Equations for Safe Train Positioning Using GNSS. ENC-GNSS 2003 - European Navigation Conference, Graz, Austria.

Poliak J., Marais J., Hänsel F., Becker U., Schnieder E. (2008) Methods and Tools for the Certification of GALILEO for Railway Applications. Proceedings of WCRR 2008, Seoul, Korea.

Wiss J.M., Barbu G., Frøsig P., Schröder M., Edwards C., Walter K., Filip A., Sage A., Forsyth S. (2000) GNSS Rail User Forum: Requirements of Rail Applications. Final draft, European GNSS Secretariat, Brussels, Belgium.