Simulation-based evaluation of dependability and safety properties of satellite technologies for railway localization — **Source link** ⌇

Julie Beugin, Juliette Marais

Institutions: university of lille

Related papers:

- Performance Evaluation of GNSS for Train Localization

- Recent progress in application of GNSS and advanced communications for railway signaling

- Formalizing a subset of ERTMS/ETCS specifications for verification purposes

- RAMS evaluation of GNSS for railway localisation

- Vision based rail track and switch recognition for self-localization of trains in a rail network

Simulation-based Evaluation of Dependability and Safety Properties of Satellite Technologies for Railway Localization

Julie Beugin, Juliette Marais

Simulation-based Evaluation of Dependability and Safety Properties of Satellite Technologies for Railway Localization

Julie Beugin[a,*], Juliette Marais[b]

a *Univ Lille Nord de France, IFSTTAR, ESTAS, 20 rue Elisée Reclus, BP 70317, 59666 Villeneuve d'Ascq, France*
b *Univ Lille Nord de France, IFSTTAR, LEOST, 20 rue Elisée Reclus, BP 70317, 59666 Villeneuve d'Ascq, France*

Abstract: Satellite-based localization technologies are strategic opportunities in railway applications because they offer new possibilities of service and have advantages that current technologies relying mainly on infrastructures deployed along tracks cannot equal. GNSS (Global Navigation Satellite Systems) can, in particular, offer localization services in ERTMS (European Rail Traffic Management System), the system developed within the European railway community to harmonize, at European scale, railway signalling and control/command systems. However, using GNSS in such safety applications is slowed down when trying to comply with railway standards. Indeed, demonstrations of RAMS properties (Reliability, Availability, Maintainability, Safety) are required on new solutions embedded in trains. They aim at verifying if all dependability (RAM) and safety aspects are controlled over the lifecycle of the solutions before using them operationally. No RAMS evaluation technique exists for systems based on signal propagation and subject to failures provoked by environment effects. The major challenge is so to develop proof methods that will give means to fulfil the railway certification process. In this article, we propose a procedure to work in that direction after having presented the advantages, the possibilities and the challenges to use GNSS in rail transportation. The procedure is based on experiments for the evaluation of RAMS properties related to satellite-based localisation units. We apply the method to different position measurements obtained in several typical railway environments. The obtained results are discussed according to the dependability and safety points of view.

Keywords: GNSS-based localization, Railway application, Certification, RAMS

---

*Corresponding Author. Tel.: +33-3-20-43-83-90 fax: +33-3-20-43-83-98
E-mail address: julie.beugin@ifsttar.fr

Introduction

Revitalising the railways is one of the priorities defined by the European Commission in the White Paper on

Transport (EC 2001). Satellite localization technologies have an important role to play in this context,

because they can help railway actors to provide a more competitive and quality transportation service for

customers. Several applications based on GPS have already been developed for tracking freight goods or

informing passengers and have shown the advantages and the possibilities of GNSS (Global Navigation

Satellite Systems). A promising possibility is the development of railway applications that ensure safe

operations. This idea is consolidated by the arrival of the future European GNSS Galileo that will provide

new services with different localization performances.

Including a new device into the railway system for realizing safety operations requires the application of a

management process, based mainly, in Europe, on the EN 50126, EN 50128, EN 50129 standards. These

activities are difficult to accomplish for satellite-based navigation technologies. On the one hand, railway

suppliers are looking for standardized methods, which can help them to demonstrate the safety of the

advanced GNSS products. On the other hand, railway operators cannot precisely describe what proofs they

can expect from suppliers, i.e. elements making them confident to accept the products and be sure that they

will be authorized by safety authorities.

There are various opportunities to develop train localization units based on GNSS: the architecture may

only include a GNSS receiver or it can be composed of a combination of a GNSS receiver with other

technologies. In this article, we will focus on what can bring GNSS alone for railway safety applications

given constraining railway environments for signal reception. The objective is to give evaluation means for

such systems that are in agreement with railway certification processes and that will enable the railways to

accept GNSS. For that, we propose a procedure that aims at analysing the localization service provided by a

GNSS receiver. Each position measured by the receiver relies on a signal processing chain going from the

signal transmitted by the satellites to the pseudo-range estimated by a positioning module. Everything that

may create failures or perturbations before the signal reception is, in this article, supposed to be controlled.

Thus we concentrate on the point of view of railway users, who only want to know the quality of the

localization on an entire railway network.

The paper will be organized as follows. The first part will present what the satellite technologies can bring to the railway sector and how they can be used. The second part will detail why the acceptance of GNSS solutions embedded in trains is a challenge. The issues concern the understanding of requirements and the evaluation of the technology according railway standardized practices, especially the RAMS evaluation. The third part will detail the procedure based on experiments we proposed for the evaluation of RAMS properties. The final part will present the results we have obtained in different railway contexts.

1. Satellite technologies for railway localization

The different railway applications presented hereafter show the advantages and the possibilities of GNSS for rail transportation. Some of them based on GPS are already in operation, some other are prototypes that have been tested.

1.1. Current or tested railway applications

1.1.1. Non-safety-relevant applications

GNSS utilization in railway transportation is today helpful to track or trace trains, i.e. to determine respectively current locations (in real time) or past locations (in delayed time) of trains. The existing applications are largely achieved with GPS and concern passenger information or cargo management. In France, for example, all freight locomotives (about 2000) have been equipped with GPS to better track freight trains and inform clients. Such also is the case for all express regional trains (TER) whose associated positions and scheduled times can be displayed on smartphones. The utilization of satellite technologies in the railway sector is, today in Europe, limited to non-safety-related applications. Indeed, having very low risks, these applications are easier accepted and put into service than those having an impact on the safety of individuals and goods. In this case, the execution of the risk management process raises many questions as we will see in section 2.

The aeronautical mode is ahead of the railway mode concerning the safety issues of GNSS utilization given that GPS localization is already in use for air navigation. Although there is still some reticence to use GNSS for railway safety applications, some groups of researchers and industrialists have proposed test systems on

the last ten years, in order to take an active part of the ERTMS standard that concerns the European harmonization of railway signalling (UIC 2005).

1.1.2. Safety-relevant applications

To harmonize progressively all train control/command systems with the ERTMS (European Rail Traffic Management System), the migration strategy encompasses several technological levels. The concept of "intelligent train" characterizes the last level (the third) in the sense that vehicles will be able to perform several functions autonomously. In particular, their capacity to localize themselves with intra-vehicle equipment is expected. All trains can then transmit their absolute position to a radio-block centre, which can then dynamically determine the intervals between trains. By so doing, it is possible to optimize and reduce the spacing distances until a minimal safety interval is obtained, i.e. the train braking distance. Today, this moving block principle is not achievable because the localization function is realized by beacons, track circuits and other trackside equipment, which maintain the trains separated using the fixed block principle, i.e. one train lies one track section.

The satellite technologies bring an efficient and interoperable answer to fill the gap between the ERTMS concept of self-sustaining vehicle localization and its implementation. They will then contribute to improve railway network capacity. Moreover, as they can complement or replace the localization equipment massively deployed along tracks, they can reduce infrastructure costs and simplify the installations. These reasons explain why the projects working on safe train operations by means of GNSS-based localization technologies have been mainly focused on the development and the deployment of ERTMS. Some of them are presented in table 1.

Table 1. List of research projects linked to the GNSS utilization for train control/command

Project name	Period	Funding	Use of GNSS in the projects	Reference
APOLO	1998-2001	EC	Train location system using GNSS and other sensors to facilitate improvements in supervision systems for dispatchers and to support signalling systems for low density lines.	(Filip 2001)
GADEROS	2002-2004	EC-5th framework program	Demonstration of the use of GNSS integrity and Safety Of Life characteristics for defining a satellite-based system to perform train location for safe railway applications.	(Bustamante et al. 2003)
INTEGRAIL	2005-2009	EC-6th framework program	EGNOS in ERTMS.	(Gu 2005)
LOCOPROL /LOCOLOC	2001-2005	ESA-EC	Definition of a low-cost satellite-based train location solution for low density traffic lines.	(Simsky et al.2004)
ECORAIL	2001-2005	ESA	Safe use of EGNOS for level crossing control.	(Thevenot et al. 2003)
RUNE	2001-2006	ESA	EGNOS is used as part of an integrated system to improve train driver's awareness. The system is capable to enhance train position and speed estimation.	(Marradi Albanese, et al.2008)
DemoOrt	2004-2007	Germany	Development with high performances and according safety principles of a platform for self-sustaining vehicle navigation based on GNSS and other navigation systems.	(Hartwig et al. 2006)
GRAIL	2005-2007	EC-6th framework program /GJU	Achieve a common specification (agreed by users and industries) for the GNSS subsystem dedicated to the odometry function (mainly focused on ERTMS/ETCS standard).	(Ballesteros 2006)

In these projects, two different approaches have been considered for the localization solution: either GNSS is the main part of the solution or is used in combination with additional technologies (e.g. inertial platform, digital information on track topography, train-communication network). The design strategy has been oriented towards the standalone or hybrid GNSS solution according to the intended goal, principally: reduce costs of development / material / installation / maintenance or improve the accuracy / availability / continuity / integrity performances. For example, a low cost solution is privileged for the train operation on rural railway lines that are often unprofitable because of the low density traffic, in contrast with high speed lines for which high performances are demanded.

1.2. Railway applications in the future

The past conclusive experiments have shown the possibilities with GNSS in the railway domain and their advantages appear now as an opportunity for multiple applications. The improvement of operating performances is sought for applications dealing with train regularity, capacity of lines, safety activities or train energy consumption. Other possible applications constitute added services such as track survey, passenger information on the position of "its" train directly with the expected time of arrival or a waiting time (Gallaud & Catry 2009).

Promising possibilities for European countries are, in the near future, the development of applications based on the Galileo system. In particular, railway signalling systems can benefit of Galileo to realize several safety tasks such as:

− train detection / positioning ,

− spacing out of trains along the lines ,

− control of points at junctions or intersections,

− automatic train protection (ATP system) ,

− automatic train control (ATC system) including driver assistance with the interface in train cabin.

Indeed Galileo will provide new signal properties and new functionalities, especially the guarantee of broadcast information with the *Safety-of-Life* service. The very last goal is then to enhance the train odometry by a Galileo-based device coupled with a minimum of sensors to optimize both performances and costs of the final solution.

Even if experiments have shown the applicability of GNSS in the railway domain, the utilization of the different existing or future satellite systems cannot be taken for granted in the applications dedicated to safety. Indeed, they require some railway safety practices in all the development of the GNSS solution. These practices are described below. They lead to several issues that will be detailed in the next section.

1.3. GNSS and railway safety practices

In railways, the approval of new devices and especially those dedicated to safety operations relies on activities that aim at satisfying RAMS requirements (Reliability, Availability, Maintainability, Safety). These activities strive to ensure the quality of the service delivered by the equipment and integrate a standardized process based on the V-model, a common representation of the systems' development lifecycle (cf. the European / international railway standards, resp.: EN 50126 / IEC 62278, EN 50128 / IEC 62279 and EN 50129 / IEC 62425). At each stage of the process, demonstrations of compliance with RAMS requirements are provided using recommended techniques and methods (such as Failure Mode Effects and Criticality Analysis, Preliminary Risk Analysis, Fault Trees, Reliability Block Diagrams, SIL allocation, Markov Analysis). Thus, proofs of safety are traced and documented as well as proofs of dependability (RAM), i.e. the ability that all conditions to maintain safe operations along the whole lifecycle of the system are applied. Figure 1 represents the V-model with in blue the steps for the development of a GNSS-based solution.
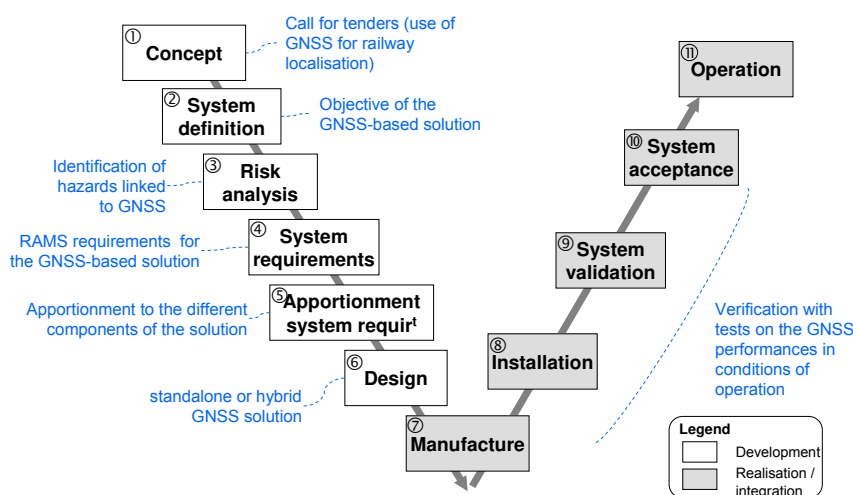

Figure 1. The V-model steps for the development of a GNSS solution

A fail-safe-based approach or a risk-based approach are usually employed to design railway safety-related system. They rely on system engineering principles, which facilitate the management of the RAMS specifications (EN 50126-1 2000) (EN 50126-2 2007) (ERA 2009a).

A system designed according to the fail-safe approach is a system able to enter or to remain in a safe state when a failure occurs (the stop of a train for example). Thus the risk is null. The fail-safe concept is often appropriate for basic components with known failure modes (relays for example). For the more complex systems, where the number of potential failure combinations is large, the risk-based approach is employed. In this case, the system can operate with tolerable risk and safety margins. According to the risks the user can accept, technical and organisational means are planned out and implemented either to detect the occurrence of a failure or to control the propagation of such an event to avoid harmful consequences. This approach is more pertinent for GNSS-based solutions for railway safety applications given that GNSS service can be disturbed with random errors (cf. §2.2.2) and are moreover specified using the risk on integrity and the risk on continuity concepts.

For a system designed with fail-safe principles or with a high level of safety when a risk-based approach is used, we commonly talk about a development realized "in safety". A high level of safety is required when the risk refers to catastrophic events (deaths or severe material damages). In the French Tr@in-MD project, a system aiming at protecting the transport of hazardous goods, the first objective was not to develop a safety-related system "in safety" but to obtain a high reliability of its parts (Minary 2008): a geo-localization and a detection parts that examine wagons and their goods. New GNSS-based systems intended to play a role in the control and command of trains have to be realized "in safety" as it is the case for the today existing infrastructures. This consideration refers to the GAME risk principle described in the EN 50126 standard, which requires that new systems fulfil the same safety requirements as those attained by an equivalent existing system. As we will explain later (see §2.1), SIL (Safety Integrity Levels) serve as safety requirements in the railway domain (EN50129 2003).

This section has shown how satellite technologies can bring benefits for railway transportation in particular for railway applications of control/command ensuring safe traffic of trains. Presently, industries need to know what to do in terms of standardization and certification of GNSS equipment to guarantee the approval in rail sector. They are faced with the challenges presented in the second section.

2. Challenges for the approval of GNSS-based solutions in railway safety applications

2.1. Localization requirements

This part presents the challenge to obtain, at European level, common railway requirements for the localization function and the problem of compatibility between the definitions of GNSS and railway requirements.

2.1.1. Existing requirements

RAMS requirements are specified at the fourth phase of the development process of a railway system (cf. figure 1). SIL (Safety Integrity Levels) are especially used for railway safety-related systems. A SIL is an indicator on a four-level scale allocated to the different safety functions of a system for specifying the measures to take against the functions failures, especially against the dangerous mode of these failures. These latter constitute hazardous events that can potentially lead to a risky situation (e.g. an accident) and are specified, in the railway domain, with a limit value of probability of occurrence per operating hours called THR – Tolerable Hazard Rate. The THR intervals and their associated SIL are presented in table 2 (EN 50129 2003).

Table 2. SIL table

SIL	Tolerable hazard rate (/hour)
4	$10^{-9} \leq THR < 10^{-8}$
3	$10^{-8} \leq THR < 10^{-7}$
2	$10^{-7} \leq THR < 10^{-6}$
1	$10^{-6} \leq THR < 10^{-5}$

A function that participates in the traffic safety, like the localization function, can potentially lead to a catastrophic consequence if a failure occurs. According to (ERA 2009b), the hazard rate requirement in this case "does not have to be reduced further if the rate of that failure is less than or equal to 10^{-9} per operating hour". This target corresponds to the highest level of safety: SIL 4. But no specification tables are really shared by the entire railway community for the localization function. In ERTMS, some performance

requirements have been specified as the accuracy level and the safety level as shown in the first line of table

3. However, these figures do not constitute a reference. The projects presented before have brought their own

requirements for each specific solution developed based on GNSS, as can attest the figures found in GRAIL

and LOCOPROL documents presented in table 3.

Table 3. Some requirements for the localization function (Odometry)

System	Accuracy	Safety level	References
ERTMS	+/- 5 m + 5 % s*	Risk < $0,67.10^{-9}$/h	(UNISIG 2005) (UNISIG 2009)
GRAIL	+/- 5 m + 2 % s*	Risk < 10.10^{-10}/h	(GRAIL 2007)
LOCOPROL	Not defined (linked to the calculation of confidence intervals with the 1D-algorithm)	Risk < 6.10^{-11}/h	(LOCOPROL 2001)

* s is the distance travelled from the last calibration of the odometric device

The GNSS Rail Advisory Forum has proposed some possible common requirements for different safety- and

non-safety-related applications (see table 4) (Wiss et al. 2000). But, as we will see in the next paragraph, the

way in which the performances are described is not easily understandable by the railway actors and raises a

lot of questions.

Table 4. GNSS requirements for rail excerpt from the GNSS Rail Advisory Forum document (Wiss et al. 2000)

Applications	Horizontal accuracy (m)	Integrity		Availability (% of mission time)	Interruption of service (s)	Continuity of service (%)
		Alert limit (m)	Time to alarm (s)			
Safety related applications						
ATC on high density lines/station/parallel track	1	2.5	<1.0	>99.98	<5	>99.98
Train Control on medium density lines	10	20	<1.0	>99.98	<5	>99.98
Train Control on low density lines	25	50	<1.0	>99.98	<5	>99.98
Mass commercial /information and management – operational applications						
Tracing & Tracking of vehicles	50	125	<10	99.9	N/A	N/A
Cargo monitoring	100	250	<30	99.5	N/A	N/A
Dispatching	50	125	<5	99.9	N/A	N/A
Passenger information	100	250	<30	99.5	N/A	N/A
Infrastructures & civil engineering, professional applications						
Positioning of machines	1 cm	N/A	<5	99.5	N/A	N/A
Infrastructure survey	1 cm	0.1 cm	<10	99	N/A	N/A
Fix point applications	5 mm	N/A	<30	99	N/A	N/A

The UIC (*Union Internationale des Chemins de fer* – International Union of Railways) has nevertheless established a framework to facilitate the sharing of best practices among railway members by creating an expert group "Galileo applications for rail" (UIC 2005) (Barbu 2007). It aims at preparing the entrance of the Galileo-based solutions in the railway domain. For the moment, GNSS-based standalone solutions are not developed under safety principles, as is the case for transmission systems mentioned in the 50159 standard (EN 50159 2001).

The following paragraph focuses on the problem of dissimilar definition of requirements in railway and GNSS applications.

2.1.2. Railway requirements versus GNSS requirements

The RAMS techniques mentioned previously help in preserving the initial requirements along the development process of the railway system by controlling all sources of failures (either organizational or technical) and by verifying the satisfaction of requirements with the evaluation of quantitative properties related to the reliability, availability, maintainability and safety (e.g. probabilities of system operation on a given time, failure rate, mean time to failure, safety integrity level etc.) (IEC 60050-191 2011).

GNSS possess specific requirements characterizing the expected localization performances in terms of accuracy, availability, continuity and integrity. Such quality criteria have been initially introduced in aeronautic to describe performances associated to different phases of operation (e.g. airplane approach phase before landing). GNSS requirements are consistently well intelligible in aeronautical community. In the railway domain, the different actors (suppliers/operators) encounter difficulties to adapt these requirements to answer to their proper needs and standards, in particular safety philosophies in both domains are not treated in the same manner (Hänsel et al. 2006)(Manz et al. 2009)(Poliak et al. 2008). For example, failure rates are defined to characterize GNSS requirements with time scales of 15, 30 or 150 seconds, which mostly correspond to different operational phases of flight (ESA 2002), whereas, in railway domain, failure rates used to describe RAMS requirements are defined on 1 hour (cf. the SIL in table 2) to describe periodical

failures of components or functions of a system. On the one side, requirements are led by operational constraints, on the other side they are led by functional constraints.

So it is necessary to map the GNSS requirements into RAMS requirements so that the rail community can understand how GNSS can be used in train localization. In (Filip et al. 2008), we have proposed a methodology that presents the possible analogy between the two classes of quality criteria. Now the challenge remains to convert quantitatively GNSS to RAMS requirements.

If we now assume the RAMS requirements are laid down with defined values, another challenge is to bring the evidences that the GNSS solution designed to meet these requirements really reach the expected performances in operational conditions. At this stage, analysts are faced with difficulties to apply the evaluation techniques recommended by the railway standards to demonstrate that RAMS targets are satisfied.

2.2. The RAMS evaluation challenge

To evaluate the RAMS properties of a GNSS solution, the possible problems (hazards, failures, etc.) that may prevent the user to obtain the expected localization service are analysed beforehand. These problems may result from software or hardware failures undergone by the technical components of the solution and, also, by errors affecting each satellite signal. This latter element raises several questions as detailed below.

2.2.1. A particular railway "component" : the SIS

In the context of railway validation and certification practices, all technical elements contributing to develop, build, operate and maintain the railway safety are fully controlled by the railway industry. So, for the development of a GNSS-based solution, GNSS signals shall be regarded as a manageable constituent for the application, just as the receiver hardware and software components. However, this is not the case: GNSS are not at all under railway control. The GALCERT project (Certification Support for Galileo) aimed at ensuring that the components of GNSS (satellites and ground infrastructures) are certified for different transport modes, and, in particular the SIS (Signals In Space) (Butzmuehlen 2007). One of the railway tasks is to take

part in this certification process in order to understand it and to define legal relations with GNSS service providers (Barbu 2008).

2.2.2. The SIS errors and the railway environment

The errors on SIS can have negative consequences on the position accuracy. They are classified, in this article, in two categories:

- Errors due to perturbations of the signal propagation. Indeed, pseudo-ranges (the satellite/receiver distances estimated by the receiver) used to calculate a position, rely on propagation time measurements. The local environment of the receiver has a major impact on signal propagation. It induces delays and multipath that can degrade the pseudo-range measurement. Multipath occurs when a signal, reflected on obstacles, arrives at the receiver simultaneously with a non-reflected path of the same signal. Delays caused when signals pass through the atmosphere are secondary and can be neglected especially when mathematical models can correct them (Viandier et al. 2008).

- Errors in signal data (navigation message). These data (ephemeris, satellite clock corrections), used for satellite location, can be corrupted.

In the first case, signal propagation depends upon the specific geometry of the environment. In the railway context, the environment is greatly variable because a train encounters different zones during the run (vegetation near railway lines, different configurations of cuttings, etc.). The onboard GNSS receiver is in front of three types of sky visibility:

- 1) a full visibility: the visibility all around the receiver is unobstructed, so the reception of more than four GNSS signals necessary to obtain a position is always guaranteed,

- 2) a poor visibility: many signal deviations and multipath that can greatly degrade the position and provoke failures,

- 3) no visibility: when the environment creates a mask that blocks signal reception and interrupts the service.

No method of RAMS analysis is able to consider the effects of multipath and *a fortiori* their variability. Globally, no method allows the analysis of perturbations affecting signals. This can explain why the railway research projects conducted up to now (cf. table 1) have not evaluated the environment impact on SIS in the development of their satellite-based localization solutions.

This section has shown that taking up the challenge of RAMS evaluation is a necessary step to overcome so that GNSS will be accepted in railway safety applications. It entails:

− making explicit the measurement criteria (what we do in a previous work) (Filip et al. 2008) and,

− developing methods leading to the evaluation of these criteria.

The work presented in the next section refers to the second point. We propose a methodology for conducting tests on technical GNSS prototypes in conditions of operation to provide results in terms of quantitative values, which are meaningful for RAMS activities. The assumptions used to establish such procedure will be detailed beforehand.

3. Procedure based on experiments for the evaluation of RAMS

3.1. Assumptions

From railway users' point of view, only the quality of the localization function provided in output of a GNSS receiver is important. This quality depends on how the GNSS sub-systems (satellites, ground stations and the user receiver) realise their mission. As mentioned previously, specific requirements exist to define the quality level a user can expect from the global satellite system. However they do not encompass the uncontrolled errors in the SIS caused by the local environment of propagation, even if characterizing them is fundamental for safety applications. The work presented hereafter will focus on these local phenomena to investigate the research issue related to the evaluation of the RAMS properties of a train localization unit. Thus, we will assume later on in the article that problems occurring in GNSS equipment placed before the receiver (interruptions or faults in the transmitted data flow) are controlled as well as the software and hardware failures in receiver.

To consider now the influence of the environment along train routes, it is obviously impossible to describe a limited number of representative geometries to cover all situations of signal visibility. The variability of situations is a complex issue that cannot be considered in a generic model of errors. However, with the objective to evaluate RAMS properties, we can focus on two possible conditions of observation:

1) A specific route is followed by a train equipped with a GNSS receiver. The evaluated characteristics are therefore only associated to this train itinerary. RAMS results constitute then average properties characterizing all the environment configurations of the route. In these conditions, they cannot highlight particular places with poor conditions of visibility but they give a global level of RAMS for this railway line.

2) The environment configurations along the train itinerary present identical geometry features. The area around this itinerary constitutes actually a "typical" environment. RAMS results can then give representative characteristics for different typical environments observed. Recommendations for adding GNSS augmentation devices can be provided according to the configuration of the environment. It is also possible to make comparisons between different environment properties.

Our evaluation procedure based on GNSS measurements captured in conditions of operation is now described. How the collected data are managed to determine probabilities or average values is presented after having detailed the states of the localization function we analyze. For the application of the proposed approach in the last section, we will concentrate on conditions of observation highlighting typical environment characteristics (the second point above).

3.2. *The proposed evaluation procedure*

3.2.1. States of the localization function

We identified three states for the output function of the receiver: "to deliver estimated positions". Figure 2 represents them and an illustration of a train associated to a correct and a wrong localization. These three states are:

1)   correctly estimated position, i.e. when the true position, unknown for the receiver, is inside a circle centred on the position calculated by the system. The circle radius is equal to the maximum position error tolerated by the user and corresponds therefore to the accuracy requirement.

2)   incorrectly estimated position, i.e. when the estimated position is outside accuracy boundaries. In this case, the localization service expected by the user is failed. However, as this state is not recognized by the system, this service is still delivered.

3)   the position is not delivered because, at the receiver level, number of signals received are insufficient. In this case, the localization service expected by the user is interrupted.
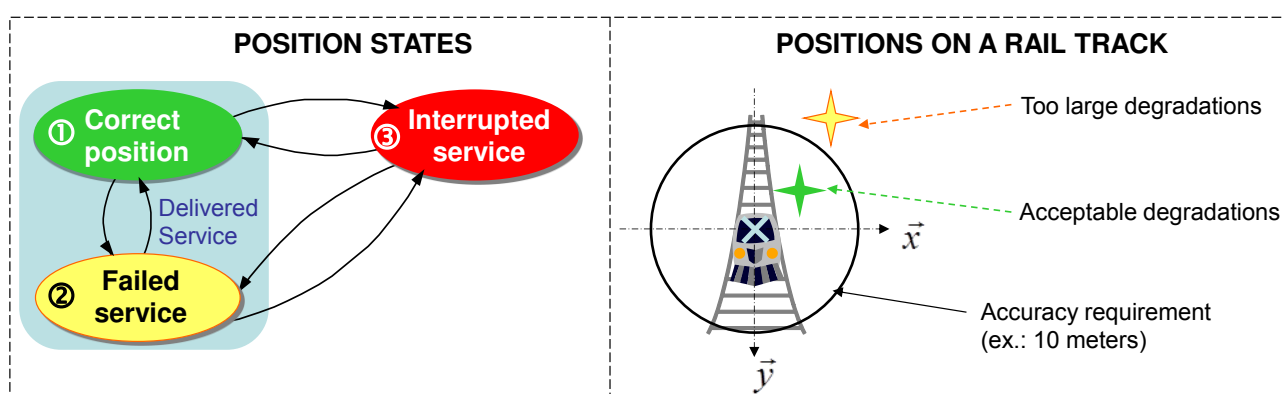

Figure 2. State of the position delivered by the localization function

A hazardous event occurs when the localization function reaches states 2 or 3. A train, which has been wrongly positioned (state 2), can, for instance, make an intrusion into the area reserved to another train without being detected. This situation can lead to an accident. If signal reception is too degraded (state 3), no position can be calculated and sent to the traffic management control centre, the service is therefore interrupted. In this case, the control centre will not be able to determine if the train has stopped or is in movement to correctly protect it against other trains. The RAMS activities on a railway GNSS-based system concentrate on these two states.

3.2.2. Principles of the procedure

We use an Operational Experience Feedback (OEF) methodology to obtain an efficient procedure capable of managing a huge quantity of data in order to evaluate RAMS properties. This approach follows usual steps that we have here adapted to the GNSS localization.

In an OEF analysis, collected data can give information on the system behaviour and its evolution in relation to the period of operation (Lannoy 2002). These data can be facts or events like incidents, failures, degradations, maintenance operations, during the given mission time of the system. They are processed and analysed subsequently.

Data associated to real positioning measurements in railway environments can be recorded to keep trace of the operational behaviour of the GNSS-based solution. What can be collected are data that provide information associated to signals – intrinsic properties or satellite/receiver path characteristics – and also information associated to signal processing leading to position estimations. They could serve to identify a posteriori the occurrence of failure events, what is not possible during measurements. The occurrences of such events determine the instants when the localization function enters in the state 2 of figure 2.

To determine the accuracy of an estimated position, a reference is needed. Existing technical solutions can give very accurate reference (for instance, an odometric platform composed of several sensors embedded in train). Figure 3 illustrates the proposed procedure, which begins with this data collection and continues with several processing steps:

−   In the first step, a selection is carried out from the amount of collected data stemming from receiver output files. Indeed, even if these files are organized according to a given format (in RINEX or NMEA format for instance), the inside data are very heterogeneous. They constitute raw data that are unworkable for a RAMS evaluation. Useful data leading to the position estimation are extracted at each sampling instant.

−   In the second step, the useful data are processed to obtain information related to correct and hazardous states. To determine if there is a failure or not, a position has to be compared with the true position (the reference).

−   Finally, the obtained information leads to quantitative values that can be subsequently analysed statistically in order to get RAMS results.

The results are in relation with the considered accuracy requirement because it serves to determine whether

positions are correct for users or not. This requirement can be very constraining (ex.: 1m) or more supple

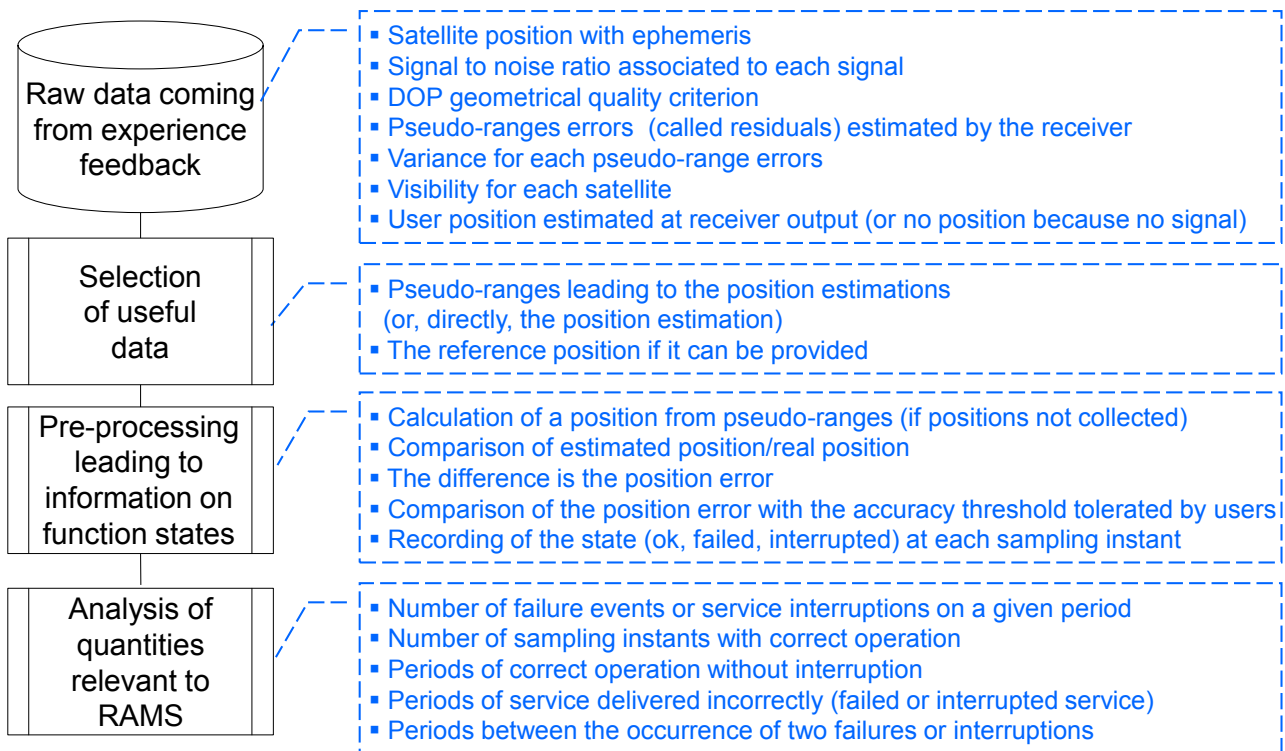(ex.: 100m). So, the procedure can lead to different results that depend on a requirement.

Figure 3. Evaluation procedure based on the analysis of OEF data

3.3. The evaluated RAMS properties

The information obtained in the last step of the procedure can lead to average values, probabilities or

distributions that can serve for the RAMS evaluation.

Table 5 presents the characteristics that can be obtained and explains how they can be calculated. The [1)]

refers to the quantities that are used and [2)] refers to the process leading to the specific properties.

Up time and *down time* are concepts that appear in table 5. The *up time* for the localization function is a sub-

part of the whole receiver utilisation time that only includes periods when the function is in correct

operation. The *down time* only includes periods when the function is in down states caused by failures and

service interruptions. By definition, the time between failures is related to the time between the beginnings of

two down time periods. In the case of localization, the down time includes periods of interrupted service. So

for consistency, the time between failures refers here to the time between the occurrence of two failures or

interruptions (not only two failures).

Table 5. RAMS properties obtained after calculation

Average values		
MUT	Mean Up Time	1) Periods of correct operation without interruption 2) Average on all period lengths
MDT	Mean Down Time	1) Periods of service delivered incorrectly (failed or interrupted) 2) Average on all period lengths
MTBF	Mean Time Between Failures	1) Periods between the occurrence of two failures or interruptions 2) Average on all period lengths
Average frequency of incorrect positions		1) Number of failures or service interruptions on a given period 2) Average on the number of all sampling instants
Probabilities		
Instantaneous availability		1) Position state at each sampling instant 2) Average on the number of operational scenarios
Average availability		1) Sampling instant with correct operation 2) Average on the number of all sampling instants
Distributions		
Distribution of unreliability		1) Periods of service delivered incorrectly (failed or interrupted) 2) Distribution of all period lengths
Distribution of reliability		1) Periods of operation without interruption 2) Distribution of all period lengths

To apply the proposed approach, our measurements will be obtained using simulations in artificial

environments rather than using a receiver placed in real operational conditions. This can seem contradictory

to OEF analysis that relies, by definition, on real data. But, in so doing, we first aim at showing the

feasibility of the method and at making possible the comparison of typical environment characteristics.

Moreover, with a simulation, the exact trajectory of the mobile is known. In practice, this information can

only be obtained with the deployment of an expensive solution. The results obtained using different railway

environments are presented below. RAM and Safety are discussed separately as the risk needs to be defined

before evaluating the safety.

4. Application of the approach and results

4.1. Simulation of railway conditions

The Ergospace software is employed for the simulations (Ergospace 2008). This tool uses 3D numerical models of environments (called scenes) in which a mobile can circulate. It provides pseudo-range values associated to each satellite of the GNSS constellation. Signals that can reach the mobile are determined using a 3D ray-tracing principle. Errors due to local propagation phenomena are calculated by applying optical geometrics laws and ray tracing techniques.

The software provides, for every sampling instant (1 second generally), the following elements:

− data related to each signal path (number of reflections, additional delays due to reflection),

− data related to the received signal level (attenuation of signal strength when reflected, and when passing through the atmosphere, etc.),

− satellite coordinates,

− information on the satellite geometry (DOP indicator),

− exact receiver positions at each sampling instant along a predefined route in the 3D scene.
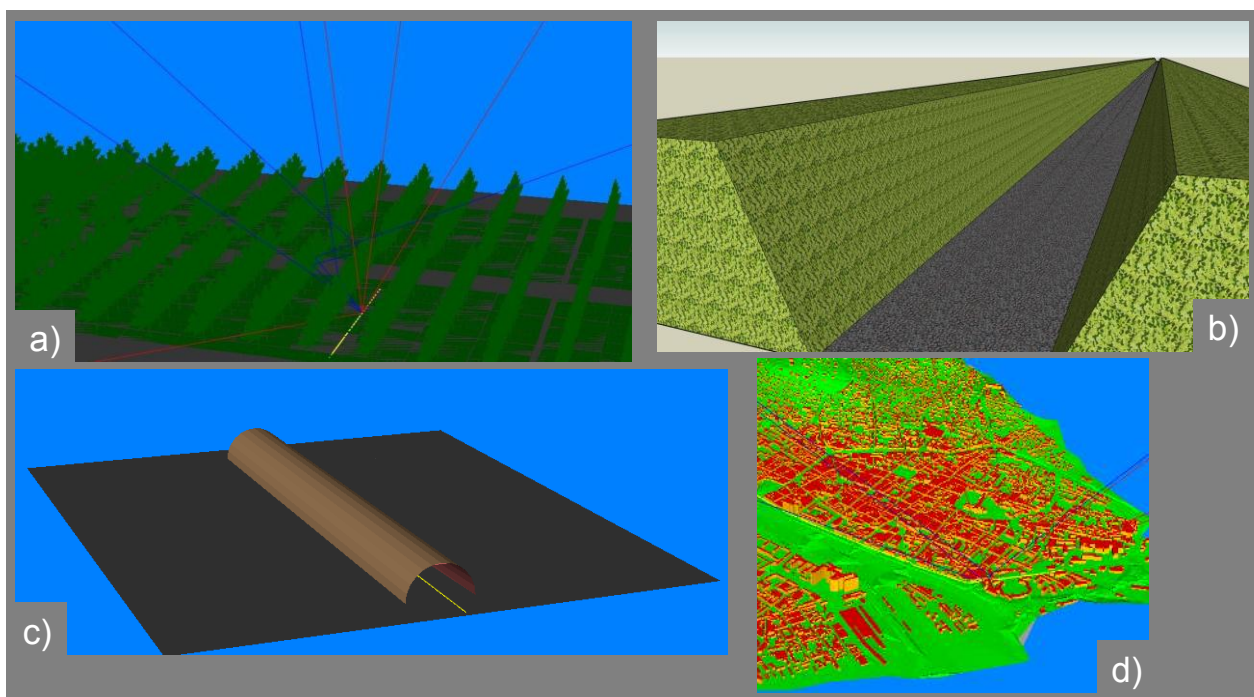

Figure 4. a) Wooded environment - b) Railway cutting environment - c) Tunnel environment - d) Urban environment

We have selected four typical railway environments. The 3D models of these environments are illustrated in figure 4:

- a) the wooded environment. Trees have been regularly placed to facilitate the model construction.

- b) the railway cutting environment. Observed phenomena are in particular masking effects and multipath.

- c) the tunnel environment. A tunnel totally masks the signal reception. The interest is the signal propagation effects at the tunnel entrance and exit.

- d) the urban environment. The model of the city of Rouen is used. It integrates buildings without architectural details.

In a scene linked to a model, the train route appears in yellow, direct rays in red and reflected rays in blue (see sub-figure a).

4.2. Use of scenarios for statistical evaluations

The procedure is based on measurements that are captured in conditions of operation and that are processed statistically. Basically, acquisitions have to be performed during a long period of observation to obtain significant amounts of data. As data come from simulations rather than real measurements, a train itinerary is restricted to the simulation software limits. Consequently, the observation period can only be short. Nevertheless, to apply this approach, we use scenarios. One scenario is a sequence constituted of a succession of states associated to the localization function. Figure 5 illustrates eight possible scenarios in which states are distinguished at each sampling instant using unit steps and colours. As defined previously, the function can be in one among three possible states. This depends whether the position is correctly estimated (in green), whether the function has failed to deliver the service with a correct accuracy (in yellow) or whether the position is not delivered, i.e. the service is interrupted (in red).

To obtain different scenarios with the Ergospace software, raw data are collected as follows: the run of a train equipped with a GPS receiver is simulated at several moments on a given day in order to consider different configurations of the GPS satellite constellation. The train runs through the same itinerary at the beginning of each hour. The number of scenarios is established knowing that a satellite configuration for a

given place at a given instant will be nearly the same 24 hours later. Thus we consider that one simulation

realized each hour on a given day is sufficient and will lead to 24 distinct scenarios. It is consistent with a

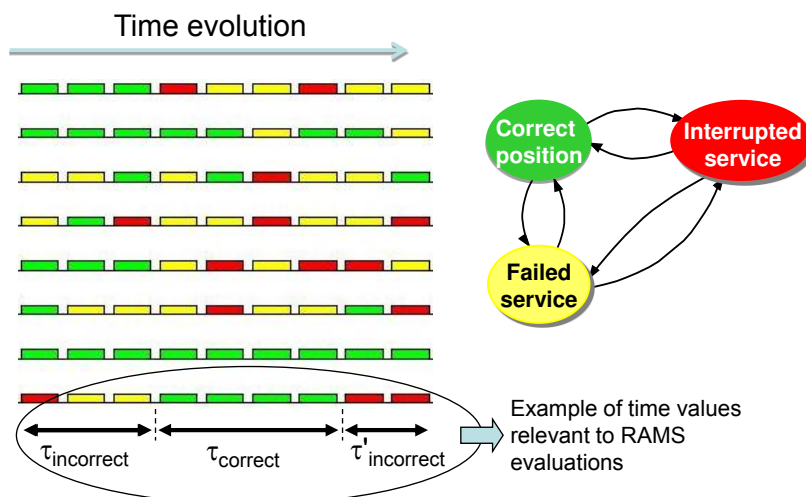train that does several round-trips per day.

Figure 5. Example of 8 scenarios constituted of the successive states reached by the localization function

4.3. Results of the approach

The utilisation of the proposed procedure leads to evaluations associated to a given level of accuracy. Levels

are different from one railway application to another as different localization performances are expected (see

table 4). To cover a wide range of applications, we have tested three levels of accuracy: 50, 10 and 1 meter.

With the same environmental constraints, the application associated to the most tolerant accuracy

requirement will have naturally better results than the others. We can observe this statement in the

evaluations of RAM properties presented in figure 6, 7 and 8. The results have been graphically presented to

allow visual comparisons of properties related to the different environments and the different levels of

accuracy that are analysed.

In figure 6, specific comments concern the urban environment. It has the highest MUT (27 seconds) for an

accuracy requirement of 50m compared to the other environments. The operating periods become very short

as soon as a higher level of accuracy is required (3 to almost 5 seconds). In fact, when a receiver moves in

such area, the satellite visibility varies strongly because of the extremely uneven elevation of the

architectural elements along the route. Masking effects perturb then the reception of the signals and consequently degrade the accuracy and limit the availability of the service. These results prove that, for the urban environment, the localization function enters frequently in down states for high accuracy levels and much less often for low levels.
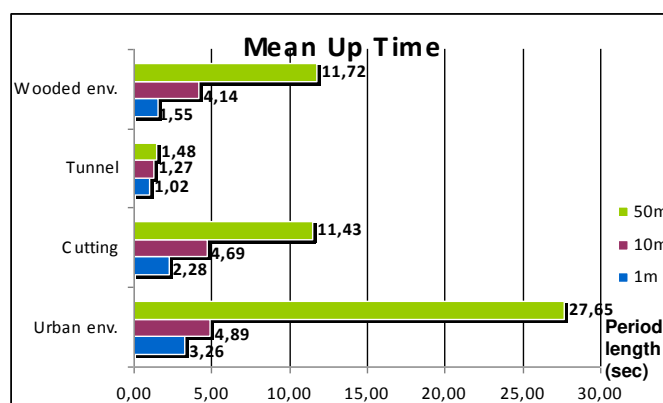

Figure 6. Mean Up Time for 4 environments each associated to 3 different accuracy levels

In figure 7, each horizontal bar is associated to a value of MTBF. As seen previously, the MTBF is the average period between the occurrences of two failures or interruptions. It is equal to the sum of MUT and MDT. In the figure, the fractions of time related to the MUT (dark colours) and MDT (light colours) are represented on each bar. Low MTBF values in tunnel are not significant because they only explicit the absence of signal reception in tunnel.

For the other environments, the MDT values logically increase with the growth of accuracy. For an accuracy requirement of 10 m, the MDT and MUT values are equivalent, and MTBF values are the shortest compared to other requirements. This proves that, for this 10 m level, the transitions between up and down states vary enormously. The up time is larger than the down time for the low accuracy level of 50 m and inversely for the high requirement of 1 m.

In wooded environment, for an accuracy level of 1 m, the MTBF value is the largest. In tunnel environment where the availability is relatively low, the reception is in the mode "all-or-none": either it is available and accurate or totally unavailable.

For the railway cutting, occurrences of down states are frequent as MTBF are short but, when referring to figure 8, availability is high. This proves in fact that state transitions are multiple.
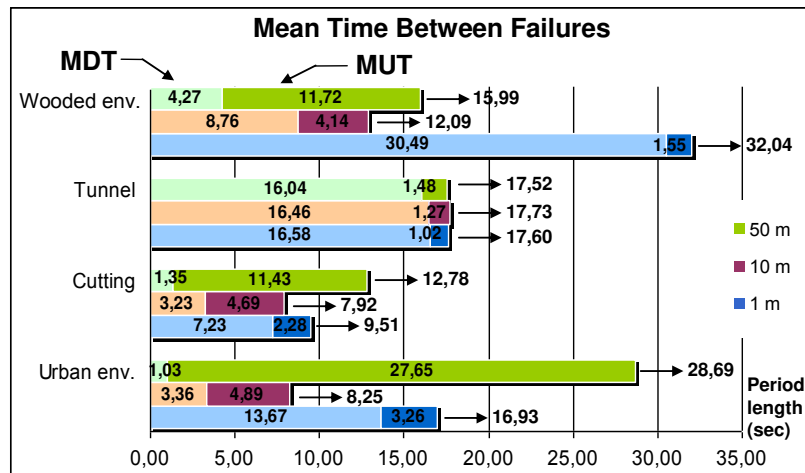
Figure 7. Mean Time Between Failures for 4 environments each associated to 3 different accuracy levels

Average availability results presented in figure 8 are quite intuitive. The greater the accuracy requirement is,

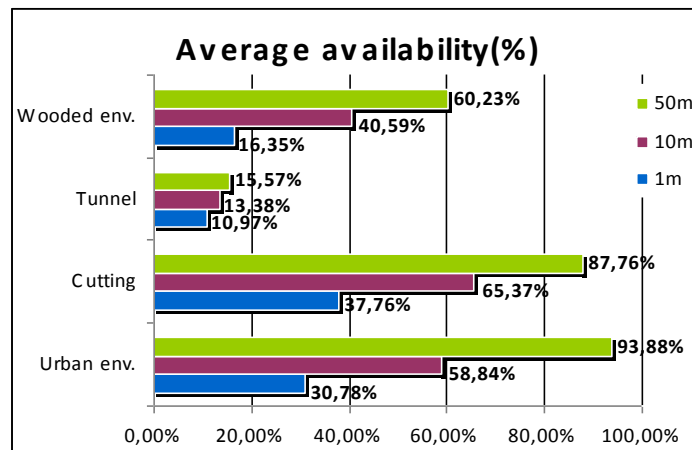the less the availability is, whatever the analysed environment.

Figure 8. Average Availability for 4 environments each associated to 3 different accuracy levels

Figure 9 shows distributions of probabilities that characterise the reliability of the GNSS-based localization

function according to the different examined accuracy levels and environments. Table 6 additionally gives

the values of the probabilities.

For each curve, probabilities are distributed according to 9 periods of time whose length Δt is equal to 2, 5,

10, 15, 20, 25, 30, 35 or 40 seconds. Each probability $P(\Delta t)$ represents a reliability property of the

localization function in the sense that, the localization function, in a correct state at the instant t, will continue to operate correctly until t+Δt with a probability P(Δt). Here the reliability results are expressed in percentages. For example, in the case of the wooded environment with an accuracy level of 50 m, we would say that the localization service is likely to be uninterrupted from t to t+2s (whatever the value of t) with 47 percent chance.

In all cases, except the tunnel case, the different distributions follow a decreasing pattern: the shortest down time are the most frequent. The urban case shows multiple operating periods with short duration. For high level of accuracy, urban and railway cutting environments show similar probabilities.
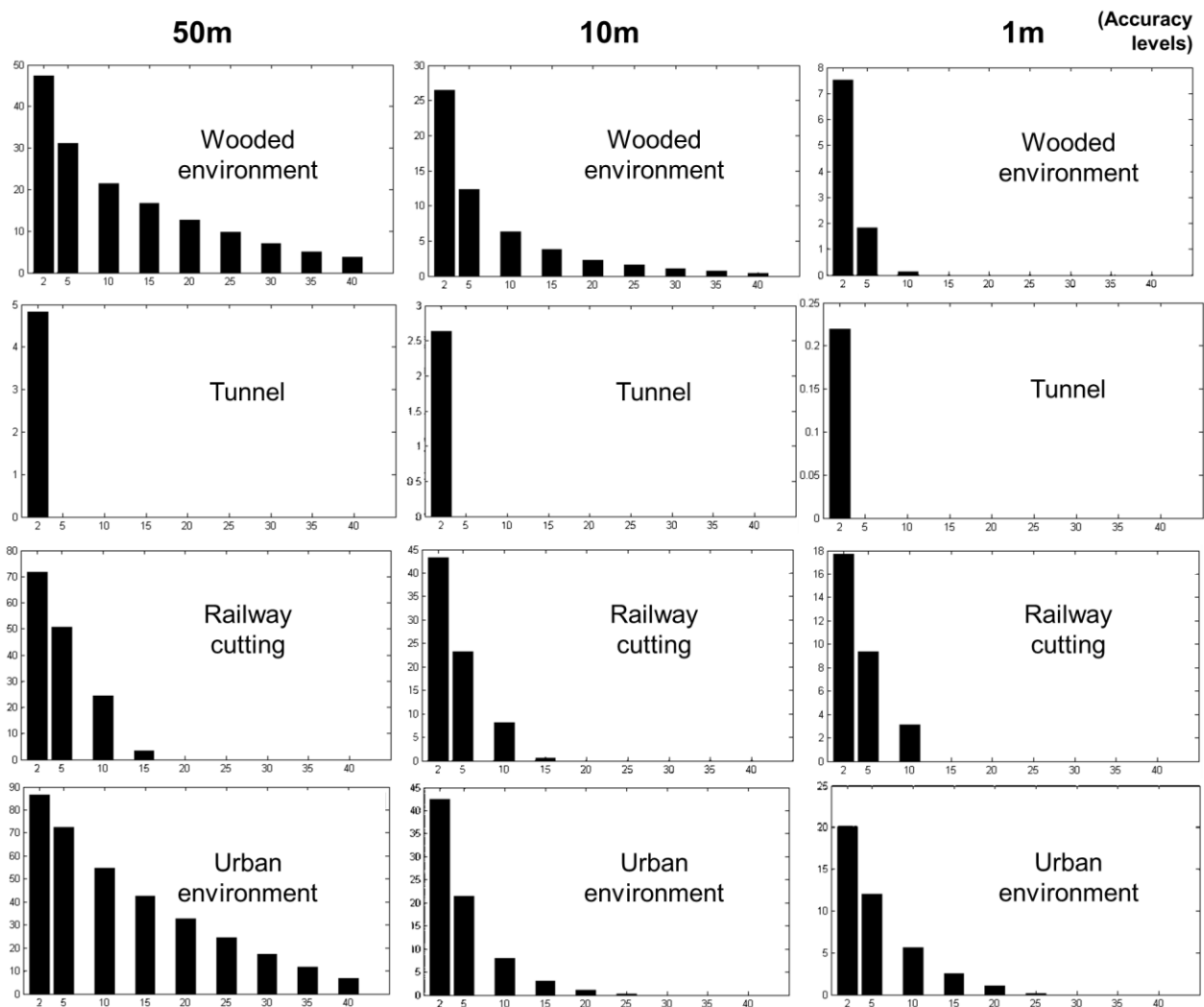

Figure 9. Distributions of reliability of the GNSS-based localization for 4 environments each associated to 3 different accuracy levels

Table 6. Probabilities of reliability of the GNSS-based localization

Environment	Level of accuracy (m)	Period Length of service without interruption (in seconds)								
		2	5	10	15	20	25	30	35	40
Wooded env.	50	47.41	31.44	22.16	17.61	13.95	11.36	8.96	7.01	5.43
	10	26.58	13.26	7.32	4.80	3.47	2.84	2.27	1.96	1.64
	1	7.39	1.83	0.13	0	0	0	0	0	0
Tunnel	50	5.04	0	0	0	0	0	0	0	0
	10	2.85	0	0	0	0	0	0	0	0
	1	0.22	0	0	0	0	0	0	0	0
Railway cutting	50	71.61	50.52	24.48	3.39	0	0	0	0	0
	10	44.01	24.48	9.38	0.78	0	0	0	0	0
	1	17.45	9.38	3.13	0	0	0	0	0	0
Urban env.	50	86.65	72.62	55.02	42.69	32.99	24.40	17.35	11.56	6.89
	10	43.54	21.94	7.91	2.98	1.02	0.17	0	0	0
	1	19.90	11.90	5.61	2.55	1.02	0.17	0	0	0

The next paragraph makes a synthesis of these results about RAM properties, i.e. about dependability. They lead us to other characteristics related to safety.

4.4. Synthesis linked to dependability results

The results emphasize that maximal up times and mean up times (cf. distributions of reliability and histograms of MUT) are greater in environments with varying conditions, like the urban and wooded environments, as opposed to the other environments. However, for these cases, state transitions are multiple due to low MTBF.

The tunnel environment is a specific case. Mean times are not significant because MDT, MTBF or availability values only rely on the tunnel length. Values that characterize the tunnel entrance and exit are the only ones which are meaningful.

In all cases, rapid degradations of quality can be observed when the accuracy requirement increases. Degradations are the greatest for the urban environment.

For a 10 m level, state transitions are most frequent, especially in the railway cutting case.

4.5. The "safety" property linked to the results

The risk, which allows the identification of the level of safety, does not directly appear in the results. To quantify this risk, the probability of occurrence of hazardous events per operating hour has to be evaluated. This is possible using the availability property related to the GNSS-based localization function (see figure 8)

because the complementary property, the unavailability, can lead to such probability. Indeed, for a safety application ensuring safe railway traffic, a hazardous event occurs when the localization function becomes unavailable. So unavailability is a probability of occurrence of hazardous events. In the context of the simulation, this probability is related to a period of operation, whose length depends on the simulation settings (here a scenario lasts at most one hour). In figure 8, several availability values are given. If we place in the best case of performance with the availability of 93.88% related to the urban environment, the SIL 4 requirement mentioned in the paragraph 2.1.1 for the localization function is far to be attained as the associated unavailability value correspond to a probability of 6.10^{-2} over the period of operation (one hour at most). The localization function necessitates therefore to be aided by other functions to reduce the risk engendered. Two possibilities can be envisaged to avoid the occurrence of the hazardous states 2 and 3 exposed in figure 2:

− a function that can assure the localization with other technical means in case of GNSS service interruptions,

− and, when the service is delivered, a function that can detect possible failures, such as a GNSS integrity monitoring function.

The new GNSS-based solution using these means will have to be evaluated in terms of RAMS to be accepted.

5. Conclusion

Global Navigation Satellite Systems are regarded as crucial for revitalizing the railway sector because they are able to make the railway systems more efficient. They are also profitable to improve rail traffic management systems. They will certainly take a significant part in such safety applications. Standards are used to manage the use of innovative systems playing a role in the safety of operations. These standards define processes based on RAMS activities (Reliability, Availability, Maintainability and Safety) that verify, during all the lifecycle of the future system, if all safety measures are correctly planned to guarantee a minimal risk during the operations. Satellite-based localization systems are of course also concerned by these processes.

However, as an external system relying on wireless signal propagation, their analysis is not usual. The question mainly asked by railway actors refers to how to evaluate the satellite-based system to demonstrate that the RAMS requirements are reached. This question is all the more thorny that the environment along the railway lines can provoke propagation phenomena that degrade the reception of satellite signals and so the information they contain for the position estimation. These phenomena are local and random as they are directly linked to the obstacles around the train. The negative impact the signal degradations have on the localization performances is the main problem to quantify.

This article brought a contribution to this evaluation issue by presenting a complete procedure capable of quantifying RAMS properties. This procedure relies on positioning measurements recorded in conditions of operation and is able to manage a huge quantity of data to obtain statistical results. The application of the proposed method was realized with the simulation of typical railway environments (wooded, railway cutting, tunnel and urban environments) and scenarios that describe the evolution of the states of the localization function. The obtained dependability results (i.e. RAM properties) showed that environments with varying conditions, like the urban and wooded environments, have the greatest maximal and mean operating times. However, for these cases, the transitions between correct and incorrect states of the localization function are multiple. Rapid degradations of quality were observed when the accuracy requirement increased. The tunnel was only examined to quantify the properties at its extremities. The safety property was obtained after having determined the risk probability depending on the unavailability result obtained previously. The result showed that the satellite-based function is not safe and requires risk reduction measures such as the use of redundant systems or the use of systems that detect faults.

Such work aspires to give means to railway actors for analyzing RAMS of satellite-based localization systems. Having understandable and tangible demonstrations will convince them to introduce GNSS technologies, like the future Galileo, in railway safety applications.

References

Ballesteros J.P.(2006). GRAIL project: GNSS introduction in the rail sector. EURNEX-ŽEL 2006, 14th international symposium: Towards the competitive rail systems in Europe, Žilina, Slovakia.

Barbu G. (2007). GALILEO certifies for rail, which safety case ? CERGAL conference - Certification of GNSS Systems & Services, Braunschweig, Germany.

Barbu G. (2008). GNSS / GALILEO certification for rail safety applications, Railway requirements and the strategic position of UIC. The 8th World Congress on Railways Research - WCRR, Seoul, Korea.

Bustamante J., De Miguel S. (2003). GADEROS - A technological approach to GNSS-aided railway traffic monitoring for conventional and low-density traffic lines - Interoperability of GNSS-based location with ERTMS / ETCS on-board. Intelligent Transport Systems and Services, Madrid, Spain.

Butzmuehlen, C. (2007). GALCERT, Support to the Certification of Galileo. CERGAL conference - Certification of GNSS Systems & Services, Braunschweig, Germany.

EC (2001). White paper: European transport policy for 2010: time to decide. European Commision, Brussel, Belgium, http://ec.europa.eu/transport/strategies/doc/2001_white_paper/lb_com_2001_0370_en.pdf

EN 50126-1 (2000). Railway Applications - Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1. CENELEC European standard (European Committee for Electrotechnical Standardization).

EN 50126-2 (2007). Railway Applications - Specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Guide to the application of EN50126-1. CENELEC European technical report (European Committee for Electrotechnical Standardization).

EN 50128 (2001). Railway Applications - Communication, signalling and processing systems - Software for railway control and protection systems. CENELEC European standard (European Committee for Electrotechnical Standardization).

EN 50129 (2003). Railway Applications - Communication, signalling and processing systems - 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).

ERA – European Railway Agency (2009a). Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation. ERA reference: ERA/GUI/02-2008/SAF.

ERA – European Railway Agency (2009b). Regulation on the adoption of a common safety method on risk evaluation and assessment. Commission regulation (EC) No 352/2009 of 24 April 2009. Official Journal of the European Union. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:108:0004:0019:EN:PDF

Ergospace (2008). http://www.ergospace.fr/index_anglais.html

ESA – European Space Agency (2002). Galileo Mission High Level Definition 3.0. Available at http://ec.europa.eu/dgs/energy_transport/galileo/doc/galileo_hld_v3_23_09_02.pdf

Filip A. (2001). Train control via global navigation satellite system : fiction or reality?. ITS International Conference, Brno, Czech Republic.

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): pp 61-68, Czech Transportation Ministry.

Gallaud J., Catry A. (2009). Railway applications of global positioning system (GPS). RGCF Journal - Revue Générale des Chemins de Fer (47): pp 47-56.

GRAIL (2007). Enhanced Odometry FMEA Report. Deliverable of the GRAIL project: GNSS Introduction in the RAIL sector, issue 1.0., project funded by the European GNSS Supervisory Authority, 6th framework program.

Gu X. (2005). Feasibility of GNSS/Galileo-based train location for safety relevant applications. Signal + Draht International 97(1-2): pp29-33.

Hänsel F., Poliak J., Barbu G., Schnieder E. (2006). Safety related usage of satellite based positioning systems in transportation-concept for Certification. CERGAL conference - Certification of GNSS Systems & Services, Braunschweig, Germany.

Hartwig K., Grimm M., Meyer Zu Hörste M., Lemmer K. (2006). Requirements for safety relevant positioning applications in rail traffic - a demonstrator for a train borne navigation platform called "DemoOrt". The 7th World Congress on Railways Research - WCRR, Montreal, Canada.

IEC 62278 (2002) Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS). Geneva, Switzerland (International Electrotechnical Commission).

IEC 62279 (2002) Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems. Geneva, Switzerland, IEC (International Electrotechnical Commission).

IEC 62425 (2007) Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling. Geneva, Switzerland, IEC (International Electrotechnical Commission).

IEC 60050-191 (2011). Dependability and quality of service. IEV (International Electrotechnical Vocabulary) chapter 191, available at www.electropedia.org

Lannoy A. (2002). A survey of methods and tools for reliability evaluation of SSCs. In proceedings of the 3rd International Conference on Mathematical Methods in Reliability (MMR'2002), Trondheim, Norway.

LOCOPROL (2001). System Safety Report. LOCOPROL- Low Cost satellite-based train location system for signalling and train Protection for Low density traffic railway lines, deliverable D5.1.

Manz H., Schnieder, L. (2009). Bridging the gap between railway safety and the specification of satellite based localisation systems. The 9th international conference on Intelligent Transport System-Telecommunication - ITS-T, Lille, France.

Marradi L., Albanese A, Di Raimondo S. (2008). RUNE-railway user navigation equipment, architecture and tests. Chapter in Satellite Communications and Navigation Systems edited by Del Re E. and Ruggieri M., Springer.

Minary B. (2008). TR@IN-MD: the Intelligent Railway Transport for Hazardous Goods. The 8th World Congress on Railways Research (WCRR), Seoul, Korea.

Poliak P., Marais J., Hänsel F., Becker U., Schnieder E. (2008). Methods and Tools for the Certification of GALILEO Localisation for Railway Applications. The 8th World Congress on Railways Research – WCRR, Seoul, Korea.

Simsky A., Wilms F., Franckart J-P. (2004). GNSS-based failsafe train positioning system for low-density traffic lines based on one-dimensional positioning algorithm. NAVITEC 2004, 2nd ESA Workshop on Satellite Navigation User Equipment Technologies, Noordwijk, The Netherlands.

Thevenot V., Bruckmueller T., Doederlein C., Mattos P., Sarfati R., Lechner W., Tossaint M. (2003). ECORAIL: A Step Towards Safe Railway Controlling Systems based on Satellite Positioning. ENC-GNSS 2003 - European Navigation Conference, Graz, Austria.

Viandier N., Nahimana F., Marais J, Duflos E. (2008). GNSS performance enhancement in urban environment based on pseudo-range error model. IEEE/ION PLANS conference (Position Location and Navigation System), Monterey, California, USA.

UIC Working Group "GALILEO Applications for rail". (2005). GALILEO Applications for rail: Roadmap for implementation. Union Internationale des Chemins de fer - International Union of Railways (UIC), Paris.

UNISIG (2005). Performance requirements for interoperability. ERTMS specifications, subset 041 V2.1.0.

UNISIG (2009). Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2. ERTMS specifications subset 091 V2.5.0.

Wiss J.-M., Barbu G., Frøsig P., Schröder M., Edwards C., Walter K., Filip A., Sage A., Forsyth S. (2000). Requirements of rail applications. Produced by the GNSS rail user forum in response to a request from the European GNSS Secretariat (EGS).