Safety concept of railway signalling based on Galileo Safety-of-Life Service

A. Filip[1], J. Beugin[2], J. Marais[2] & H. Mocek[1]
[1]*Czech Railways, Laboratory of Intelligent Systems, Czech Republic*
[2]*INRETS, LEOST, Villeneuve d'Ascq, France*

Abstract

The Safety-of-Life (SoL) Service - Level A of the satellite navigation system Galileo has great application potential for both aviation and railway safety-related systems with view to reduce operational, investment and maintenance cost. In aviation sector, radio navigation has been widely used for safety applications for several decades. That's why main quality requirements regarding the Galileo Signal-In-Space (SIS) SoL service - Level A, such as accuracy, integrity, continuity and availability, were taken from aviation ground radio navigation systems. However, different safety philosophies used in aviation domain and in railway signalling complicate direct employment of the Galileo quality measures to railway safety applications.

The objective of this paper is to show, what are fundamental differences between aeronautical and railway safety philosophies from view point of Global Navigational Satellite System (GNSS) applications, how the Galileo SIS quality measures were derived, what is their practical meaning and how it is possible to employ them for practical design of a safe Train Position Locator (TPL).The safety assessment starts from classification of Galileo SIS integrity and continuity risks by failure modes. It is shown how integrity and continuity risks influence railway safety and what impact these risks have on dependability of a safety-related system. The interpretation of the Galileo quality measures in terms of RAMS (Reliability, Availability, Maintainability and Safety) according to the standard EN 50126 is proposed. Finally, the practical application of the Galileo quality measures for safety assessment of a TPL is demonstrated.

Keywords: GPS, GNSS, LAAS, RAMS, Galileo Safety-of-Life Service, continuity risk, integrity risk, satellite navigation, railway safety, signalling, train control.

WIT Transactions on The Built Environment, Vol 103, © 2008 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR080111

1 Motivation

The satellite navigation system Galileo is planned to be used in railway signalling to improve efficiency of railway operations. The basic idea is simple - to replace track side equipment (e.g. track circuits, axle counters, balises) performing safe train position determination function by means of an on-board system based on Galileo. In this case RAMS parameters (EN 50126) of this new function must be quantified. Evaluation of RAMS is performed by means of a dependability analysis that examines the different failures in the system that realizes this location function and/or the different failure modes of the system (possible failure states of the system). To conduct such a study, the failure modes of the Galileo SIS have to be examined and the existing SIS quality measures defined in aeronautical domain have to be taken into account.

2 Aeronautical target level of safety vs. railway RAMS

Since the needs for the GNSS Signal-In-Space were mainly driven by civil aviation, we have to put the following question: "What is common for Galileo applications in aeronautical and railway domains?" Undoubtedly it is the Galileo satellite system including ground infrastructure, Galileo SoL service - Level A, and Galileo SoL standard receiver.

And what is different? Safety philosophies used in aviation and on railways. Further, requirements for Galileo SoL service - railways have not quantitative requirements for Galileo SoL service up to now. As it will be shown latter, the quality measures describing Galileo SoL service also differ from the railway RAMS (EN 50126). And finally, very different is railway environment from viewpoint of SIS reception (SIS shadowing objects along track, landscape profile, etc.). This paper will further deal with topics described in this paragraph.

In 1993, the ICAO Air Navigation Commission requested the All Weather Operations Panel 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. It was proposed to include the following GNSS quality measures: a) accuracy, b) integrity, c) continuity, and d) availability.

Requirements for integrity and continuity risks were derived from the high-level TLS [1]. The TLS in aviation is expressed in the units of hull losses per aircraft flight hour. The TLS is derived from the ICAO historical statistical data of commercial airplane accidents in a given period of time. The average hull loss per mission has been expressed as 431 hull loss accidents / 230 million flights = 1.87×10^{-6}/1 flight. After the TLS improvement (e.g. due to air traffic increasing), the value of 1.5×10^{-7} per mission (i.e. per 1.5 hour) was set. Finally, the risk of hull loss for individual operations was allocated in terms of probability per duration operation. For example, the risk (probability) of 1×10^{-8} was allocated from the total TLS to final approach with the average duration of 150 s [1].

Therefore, the GNSS integrity and continuity risks, which were derived from the risks for individual flight operations, were also expressed in terms of

probability per operation [1]. The only difference is that the integrity risk (latent/ undetected failure) covers the whole operation while the continuity risk (detected failure) covers the most critical part of the safety operation. Thus for the above mentioned final approach the integrity risk is defined per 150 s and the continuity risk per 15 s (last 15 s before a decision height is the most critical part of the operation since pilot must make decision if to continue in landing or to initiate missed approach).

The main objective of aeronautical safety philosophy is to achieve very high dependability while primarily goal in railway signalling is to achieve very high safety [2, 3]. Dependability in aviation is related to mean of transport, i.e. airplane, while safety of railway signalling is focused on signalling system itself. These fundamental differences have to be taken into account in interpretation of the Galileo SIS quality measures for railway signalling.

3 GNSS Signal-In-Space quality measures

3.1 GNSS integrity

GNSS integrity is the ability of a system to provide timely and valid warnings to the user when the system fails to meet desired margins of accuracy. Thus integrity is dependent on accuracy. Integrity is often specified by its complement, called integrity risk. GNSS Integrity Risk is defined as the probability that an error might result in a computed position error exceeding a maximum allowed value (*AL*), and the user not to be informed within the specific TTA [1]. Integrity risk is defined per duration of the entire operation.

3.2 GNSS continuity

The purpose of continuity is to guarantee, that a service of navigation system or position determination function will not be interrupted when it is really needed. Therefore, the continuity requirement is defined for the most critical phase (very short time interval, e.g. 15 s) of a safety operation. Continuity *C(t)* approximately means reliability that a system works within specifications (desired accuracy and integrity is provided) within stated period of time interval (0, *t*). It is different from integrity, which means correctness of information.

3.3 GNSS integrity and continuity risks as failure modes

The position is correct when position error (*PE*) is maintained within a user defined alert limit (*AL*), i.e. $PE \leq AL$. Reliability of position determination *R(t)* is a measure of success and is a function of operation time interval (*0, t*).

If failure modes are considered, unreliability of position determination function $F(t)$ can be expressed as $F(t)= \{PF_D\ (t) + PF_S\ (t)\}$ and reliability as $R(t) = 1 - \{PF_D\ (t) + PF_S\ (t)\}$. Probability of failing dangerously $PF_D\ (t)$ represents the probability in time interval (*0, t*) that position error PE exceeds the alert limit *AL*, i.e. $PE > AL$. Probability of failing safely $PF_S\ (t)$ represents the probability that $PE \leq AL$. In this case the output position from GNSS system

doesn't influence the safety of the entire system. Nevertheless, there is a failure in diagnostics of GNSS system or/and in position determination, which should be considered in dependability analysis.

Implementation of failure detection mechanisms can improve both safety and reliability. Subsequent refinement of failure modes will help to clarify exact meaning of GNSS integrity and continuity risks, and it will help to find a way how to describe them by means of railway RAMS terms according to EN 50126.

Probability of failing safely detected PF_{SD} (t) represents a probability that $PE \leq AL$ and that an alert is raised due to a failure of diagnostics. False alert is then announced. It is the first part of the continuity risk $CR(t)$. Probability of failing safely undetected PF_{SU} (t) represents the probability of a non-critical failure when $PE \leq AL$, but no failure is announced by built-in diagnostics. In this case, a safe failure in the system exists but user doesn't know about it. It can be revealed by independent diagnostic based on physically diverse sensors, but it is out of scope of this paper.

If PE exceeds AL and this state is hazardous detected, then it is a dangerous detected failure (true alert) and is represented by the probability of failing dangerously detected PF_{DD} (t). It is second part of the continuity risk $CR(t)$, as it will be shown below. Dangerous detected failure mode can be converted to the fail-safe state.

If PE exceeds AL without detection, it is a dangerous undetected failure, so called integrity risk, and it is described by the probability of failing dangerously undetected PF_{DU} (t). This state is the most feared failure in the system.

3.4 GNSS quality measures and railway RAMS

Availability according to railway standard EN 50126 [2] is a combination of reliability and maintainability. Trust of the provided accuracy is assessed separately from availability by means of integrity requirement. In relation to railway safety related systems, we usually talk about availability (or dependability) and safety.

On the other hand, GNSS safety requirements (i.e. integrity and continuity) are directly involved in GNSS availability [1, 7]. GNSS system is available if also (among others) safety integrity requirement is assured.

The use of the GNSS quality criteria within RAMS [2] is proposed in Fig. 1. It results from analysis of GNSS integrity and continuity risks performed in [7]. Continuity risk $CR(t)$ includes both detected failure modes $PF_{DD}(t)$ and $PF_{SD}(t)$ and has impact on safety of the system (but can be converted to fail-safe state).

Availability $A(t|M(t))$ [2] depends on correct position determination, correct function of diagnostics and maintainability of GNSS system. $A(t|M(t))$ can be evaluated by means of probability of incorrect operations $U(t|M(t))$ under condition that maintainability $M(t)$ is provided. As $U(t|M(t)) = PF_{DU}(t) + PF_{DD}(t) + PF_{SD}(t)$, *p*robability of incorrect operations of GNSS system can be determined from given integrity risk $IR(t) = PF_{DU}(t)$ and continuity risk $CR(t) = PF_{DD}(t) + PF_{SD}(t)$. The remaining probability of safe undetected failure mode $PF_{SU}(t)$ is added to the reliability segment $R(t)$ due to sake of simplicity. This simplification can be done since correct position is provided. Then availability

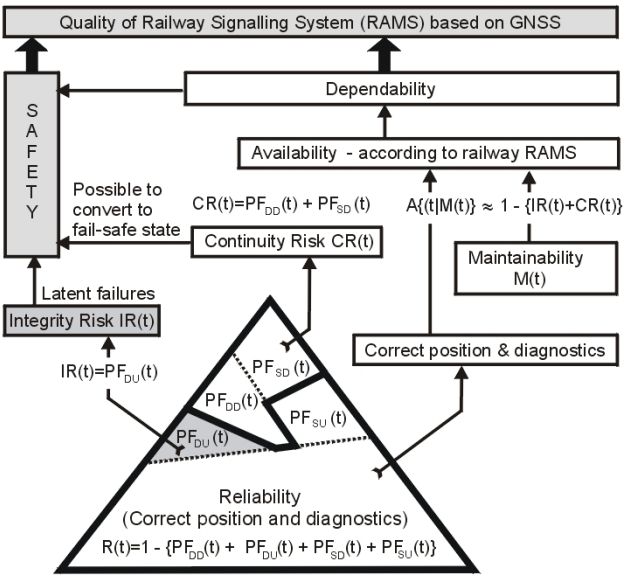

Figure 1: Quality attributes of railway signalling GNSS based.

$A(t|M(t))$ can be expressed as

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

It is obvious, that GNSS service performance is defined by means of notions that came from aviation sector. Railway sector can employ them with respect of their specific meaning according to railway standards.

4 Meaning of SIS integrity and continuity risks for signalling

4.1 Galileo integrity risk as failure rate

In railway safety systems, a failure rate per hour shall be used instead of a probability per duration of operation for purpose of a quantitative safety analysis. A value of the integrity risk for the Galileo SIS SoL – Level A is defined as the probability of dangerous undetected failure of $P_f = 2\ x10^{-7}$ in any interval Δt = 150 s, i.e.

$$IR_{SIS} = \frac{P_f}{\Delta t} = 2x10^{-7}/150\ s \quad (2)$$

The probability of failure during the specified time interval Δt can be expressed as the probability density of failure $f(t)$ as

$$f(t) = \frac{F(t+\Delta t) - F(t)}{\Delta t} \approx F'(t) = -R'(t) \quad (3)$$

where $F(t)$ is the probability of failure up to time t (unreliability). Then Integrity Risk IR_{SIS} corresponds to probability density of failure $f(t)$. The cumulative probability of dangerous failure $F(t)$ in time interval $(0,T)$ is

$$F(0,T) = \int_0^T f(t)dt \tag{4}$$

According to Equations (2), (3) and (4) the probability of dangerous failure per hour *PFH* [6] is

$$PFH(T = 1\,hour) \approx \frac{1 - R(T)}{T} = \frac{1}{T}\int_0^T f(t)dt = \frac{1}{T}\int_0^T \frac{P_f}{\Delta t}dt = \frac{P_f}{T}\int_0^T \frac{1}{150\,s}dt =$$

$$= \frac{P_f}{1\,hour}\frac{3600\,s}{150\,s} = 24P_f\,/1\,hour = 4.8\,x10^{-6}\,/1\,hour\,. \tag{5}$$

Since $PFH \approx HR(T = 1\ hour) = \lambda_{DU}^{SIS}(T = 1\ hour)$ then Galileo SIS Integrity Risk of $2\ x\ 10^{-7}/\ 150\ s$ corresponds to Hazard Rate $\lambda_{DU}^{SIS} \cong 4.8\ x\ 10^{-6}\ /\ 1\ hour$.

It is known that the Galileo SIS integrity risk is determined by the number of independent integrity feared events that could occur during critical operation, i.e. during interval of 150 s. Correlation time (i.e. time interval between independent feared events) is higher than 150 s for most of non integrity feared events defined in Galileo. It is mainly due to satellite hardware failures, ground segment algorithm failures and excessive troposphere delays. Note that feared event is an event which leads to a degradation of the accuracy of the position solution computed by the user receiver.

Therefore only one independent integrity check is considered for the interval of 150 s for Galileo. It is sufficient for precision approach with average duration of 150 s because there is no problem with one independent integrity check there. What is behind of the interval of 150 s is not too much interesting for this kind of application. Galileo SoL Level A was designed mainly for this kind of application.

Galileo Sensor Stations (GSS) collect measurements every 1 s or 0.5 seconds and Galileo system can provide Integrity Flag every 1 second. But we cannot say that we have complete (End-to-End) integrity check every 1 second. Due the above reasons the cumulative principle of probability of failure (time dependence) was used in (5).

It should be noted that the derived hazard rate of 4.8 x10^{-6} / 1 hour by means of the cumulative probability principle can be considered to be rather conservative estimation. Utilization of the Galileo SIS integrity risk for railway safety applications will be also subject of our future work.

4.2 Galileo signal-in-space continuity risk as a failure rate

Continuity $C(t)$ approximately corresponds to reliability and can be expressed as follows

$$C \cong e^{-\frac{T}{MTBF}} \tag{6}$$

where *MTBF* is Mean Time Between Failure, and *T* is the continuity time interval. If *T* << *MTBF*, then

$$C \approx 1 - \frac{T}{MTBF} \tag{7}$$

Continuity Risk *CR*(*t*) is the probability that the system will be unintentionally interrupted and will not provide location determination function over intended period of time. Loss of continuity *CR*(*t*) is related to unscheduled GNSS service interruptions. The continuity risk is one complement of *C*(*t*) as follows

$$CR = \frac{T}{MTBF} \tag{8}$$

The Equation (8) yields corresponding *MTBF* = 520.8 hours. Signal-In-Space Continuity risk CR_{SIS} can be conservatively considered as the dangerous detected failures (true alert). Following this presumption the continuity risk for the Galileo SIS SoL - Level A of 8 x 10^{-6} in any 15 s can be expressed as

$$CR_{SIS} = \lambda_{DD}^{SIS}(CR) + \lambda_{SD}^{SIS}(CR) \cong \lambda_{DD}^{SIS}(CR) = 1/MTBF = 1.92 \times 10^{-3}/1\ hour. \tag{9}$$

Continuity determines the cost of the navigation system. Loss of SIS continuity happens when the system has already started a safety function (i.e. system was available) but the safety function must be unexpectedly interrupted.

As it is evident from the railway safety standards [2, 3] no continuity requirement is needed for railway safety system since railway operation can't be specified by means of the most critical phase and duration of the operation as it is done in aviation. However, it is not desirable to loose function of GNSS (train position determination) due to its unpredictable outages. Train stopping is an extreme solution. In case of loss of GNSS function, position and speed can be continuously provided by means of complementary positioning sensors. In this case the system works in a degraded mode which is able to ensure a safe state if the required safety functions are performed with the required integrity for the required period of time. It is obvious that railway signalling can profit from high continuity of Galileo by increasing of availability. This quality measure should be taken into account during design of signalling system.

5 Galileo availability for railway signalling

Availability of GNSS is an indication of ability of the total system (satellites and ground infrastructure and user receiver) to provide service, (position determination), within the specified coverage area. GNSS availability includes: 1) availability of service, i.e. quality of transmitted SIS in terms of accuracy, integrity, continuity and availability, 2) availability of SIS in the service volume, and 3) availability of user receiver.

According to the Galileo SoL service - Level A specification [5] SIS should be available at 99.5% of time. It means that SIS for SoL Level A may not be available 43.8 hours per year. Note that possible SIS interruptions due to objects along track and landscape profile are not included in this specification of

availability. In some cases, due to SIS shadowing mainly on urban or mountain lines, conditions for utilization of the Galileo service can be much worse. A guarantee of EGNOS SIS service is much worse: it is not available at 5% of time, i.e. 438 hours per year, i.e. approximately 18 days.

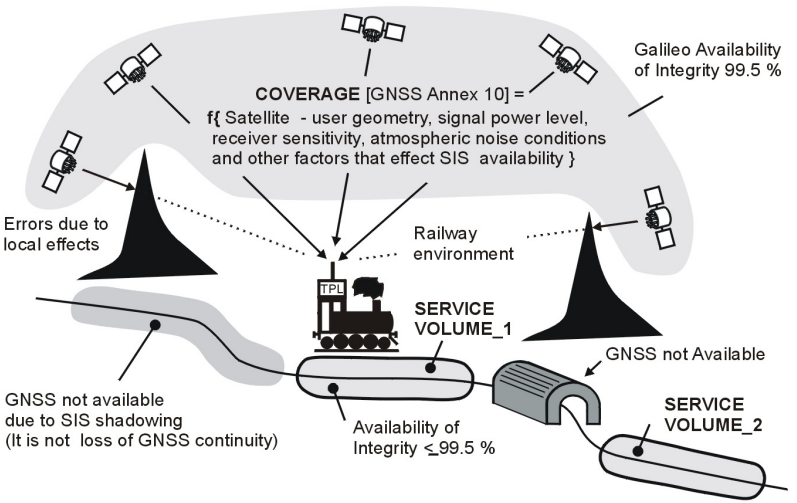

Figure 2: GNSS coverage and service volume.

5.1 Railway requirements for availability of position determination

Availability requirements for signalling equipment results from safety and operational requirements for entire railway transport system. For example if a system based on GNSS should replace ERTMS/ ETCS odometry, then unavailability less then 10^{-7} is required. It means downtime for odometry subsystem should be less than 3.15 seconds per year. One can imagine how much augmentation of GNSS by additional sensors is needed to achieve this very high availability target.

5.2 Determination of Galileo service volume for signalling system

Availability of GNSS is defined in so called coverage area (volume). The coverage is a function of system-user geometry (PDOP), signal power level, receiver sensitivity, atmospheric noise conditions and other factors that affect signal availability. For example the coverage in case of GPS, Galileo or GLONASS is global and in case of GBAS (Ground Based Augmentation System) is just in a vicinity of airport. It is clear that due to local effects (shadowing objects, EMI, etc.) the coverage is limited and therefore from view point of application it is necessary to define so called service volume. Service volume is the region within which the GNSS system is required to meet accuracy, integrity, continuity and availability. Therefore loss of SIS due to

shadowing outside service volume is not loss of continuity since loss of continuity is related to unscheduled service interruptions. Design of the service volume for signalling will be part of signalling system design. It is evident that responsible for design of service volume will be signalling system supplier. Excepting a GNSS SIS track measurements system, a certified simulator of GNSS service volume will be also needed.

6 Redundant architecture of TPL

Integration of GNSS receiver together with additional diverse sensors according to principles of functional and technical safety [2] enable to improve both safety integrity of TPL and also availability of position determination. An example of TPL based on GNSS and odometry subsystem is outlined in Fig. 3 (a). Fault tree for this example is depicted in Fig 3 (b). Let's suppose that independent diagnostics under absence of common cause failures exists. The total GNSS integrity risk is $3.5x10^{-7}$/150 s (i.e. IR of GNSS SIS and GNSS receiver) and the

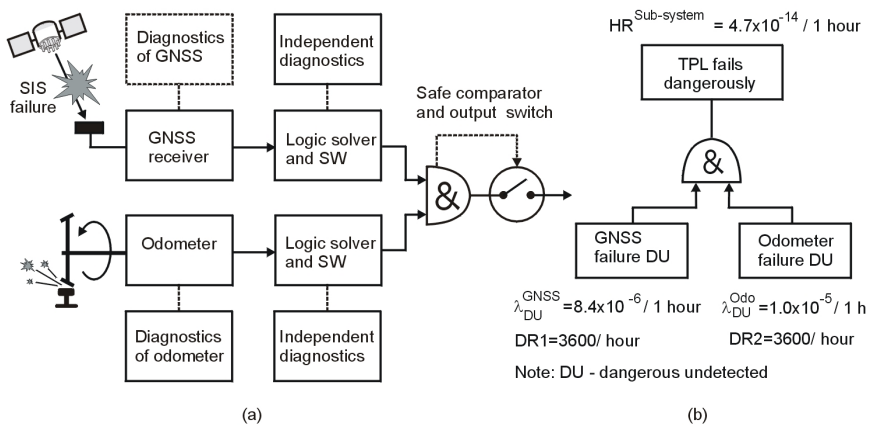

Figure 3: (a) Integration of GNSS with additional sensor, (b) Fault tree.

corresponding failure rate according to (5) is $\lambda_{DU}^{GNSS} = 3.5x10^{-7}x24 = 8.4x10^{-6}/$ *hour*. Further, if failure rate of odometer is $\lambda_{DU}^{Odo} = 1.0x10^{-5}/$ *hour* and detection rates for GNSS receiver and odometer are $DR^{GNSS} = DR^{Odo} = 3600/$ *hour*, than resulting Hazard Rate (*HR*) according to (10) [3]

$$HR^{Sub\_system} \approx \frac{\lambda_{DU}^{GNSS}}{DR^{GNSS}} \times \frac{\lambda_{DU}^{Odo}}{DR^{Odo}} \times (DR^{GNSS} + DR^{Odo}) \qquad (10)$$

is assessed as $HR^{system} = 4.7x10^{-14}/$ *hour*. Note that TPL in Fig. 3(a) is very simplified example. A real TPL usable for signalling will be more complex.

Safety and dependability assessment will be much complicated. Main problem will be to increase availability of Galileo from 99.5% to the required 10^{-7} [4].

7 Conclusion

Knowledge of relations among GNSS quality measures and RAMS (EN 50126) is important for design and verification of railway safety related systems. In this paper we have shown how to employ GNSS quality criteria according to railway RAMS. In spite of different definitions and notions used for description of GNSS quality measures and RAMS, it is possible to find a relationship among them.

Acknowledgements

The work was funded by the INRETS in the period November 2007- April 2008. The work was also supported by the National Science Foundation of the Czech Republic under contract No. 102/06/0052, and the Ministry of Transport of Czech Republic under contract No. CG743-037-520.

References

[1] Manual for Validation of GNSS in Civil Aviation, EC DG Tren, Sept. 2000.
[2] EN 50126, The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS), 2002.
[3] EN 50129, Railway applications: Safety related electronic systems for signalling, 2003.
[4] ERTMS/ETCS RAMS Requirements, Chapter 2 – RAM. Version 6, 30/9/1998.
[5] Galileo Integrity Concept, ESA document ESA-DEUI-NG-TN/01331, 2005.
[6] Filip, A.: *Safety Aspects of GNSS Based Train Position Determination for Railway Signalling*. UIC Galileo for Rail Symposium, Paris, Oct 18-19, 2007.
[7] Filip, A., Beugin, J., Marais, J. and Mocek, H.: *A relation among GNSS quality measures and railway RAMS attributes.* CERGAL '2008, Braunschweig, Germany, 2-3 April, 2008.