# Interpretation of the Galileo Safety-of-Life Service by Means of Railway RAMS Terminology

A. Filip* & J. Beugin & J. Marais
*INRETS, Villeneuve d'Ascq, France*
** Corresponding author: ales.filip@tucd.cz*

H. Mocek
*Czech Railways, TÚČD – Laboratory of Intelligent Systems, Pardubice, Czech Republic*

ABSTRACT: The Galileo Safety of Life (SoL) - Level A service has been designed mainly to support aeronautical operations ranging from en-route up to approach with vertical guidance (APV II). This is why the Galileo SoL Service has been specified by means of quality criteria coming from ICAO's (International Civil Aviation Organization) Required Navigation Performance (RNP) concept, i.e., in terms of accuracy, integrity, continuity, and availability. However, Galileo SoL – Level A service is also intended for railway signalling which is based on a different safety philosophy. The objective of this paper is to describe links among the Galileo quality criteria and the quality attributes of railway signalling systems (RAMS), according to the CENELEC standards EN 50126, EN 50129 and EN IEC 61508. This paper provides a basic theory and methodology for the employment of the GNSS quality attributes for practical design, validation and verification of railway safety systems based on GNSS. It has been shown that, in spite of the different safety philosophies used in aviation and railway safety systems, the Galileo SoL – Level A service can be described by means of RAMS terminology according to railway standards.

KEY WORDS: Galileo, RAMS, satellite navigation, safety, railway signalling.

## 1 MOTIVATION

Quality of railway signalling systems is described by dependability attributes such as reliability, availability, maintainability and safety (RAMS). A relationship among them is stated in CENELEC standards EN 50126 and EN 50129. In these standards a process for their specification and demonstration is also defined, which for "classical" signalling is quite clear. However, the situation becomes more complicated if a satellite navigation system is considered for railway signalling applications. A fixed ground infrastructure, which is usually distributed along the track and is the responsibility of a railway infrastructure manager, should be replaced by moving satellites with extensive ground infrastructure placed on more continents - all the responsibility of a multi-national operator. Moreover, the "core" of the signalling system, which provides safe train position determination, should be replaced by a system, which has not been primarily designed for railway signalling, but mainl for the aviation sector, where different safety principles are used.

The existing safety requirements for Signal-In-Space (SIS) of Global Navigation Satellite System (GNSS) were mainly driven by the needs of civil aviation. In 1993, the ICAO's Air Navigation Commission requested the All Weather Operations Panel (AWOP) to examine the possibility of an extension of 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 main GNSS quality criteria: a) accuracy, b) integrity, c) continuity, and d) availability.

A mutual relation among the GNSS quality measures and railway RAMS attributes was briefly outlined and explained in (Filip, 2006). From today's point of view, this brief explanation is insufficient, since preparation of railway applications requires a more comprehensive view. The aim of this paper is to provide a consistent background on which railway safety applications based on GNSS can be built. The work presented in this paper starts from the reliability of position determination and accuracy guarantee considerations. It is followed by a classification of GNSS failure modes that result from the GNSS quality measures definitions. Finally, the use of the GNSS failure modes within railway RAMS is described. The emphasis is not only focused on the significance of GNSS safety, but also on the analysis of GNSS availability and its impacts, which is important for the feasibility assessment of future GNSS based railway safety applications.

## 2 RELIABILITY OF POSITION DETERMINATION VERSUS SAFETY

Reliability R(t) of correct position determination by GNSS, including the correct function of its diagnostics, is outlined in Fig. 1(a) by means of Venn diagram. The position is correct when position error (PE) is maintained within a user defined alert limit (AL), i.e. PE ≤ AL.

(a) (b)

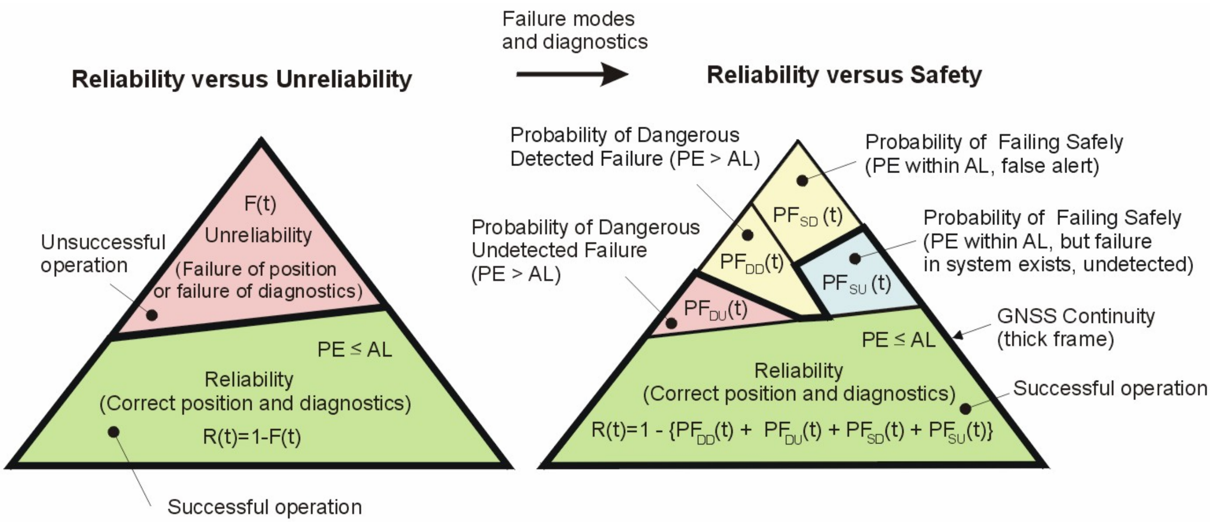



**Figure 1: The relation between reliability and safety of position determination: (a) Reliability vs. unreliability, (b) Reliability vs. safety when diagnostics is implemented.**

Reliability of position determination R(t) is a measure of success and it is a function of operation time interval (0, t). Unreliability F(t) of provided service or function is a measure of failure in time interval (0, t). It represents PE exceeding AL or/and a diagnostic failure. Unreliability F(t) is one complement of R(t).2.1 Failure modes

### 2.1 Failure modes

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 ≤ AL. In this case, the output position from GNSS system does not influence the safety of the entire system. Nevertheless, there is a failure in diagnostics of the GNSS system or/and in position determination, which should be considered in dependability analysis.

### 2.2 Failure detection

Implementation of failure detection mechanisms can improve both safety and reliability. Subsequent refinement of failure modes will help to clarify the exact meaning of GNSS integrity and continuity risks, and it will help to find a way to describe them by means of railway RAMS terms, according to EN 50126. A relation among the reliability of position determination R(t) and the probabilities of failure modes is outlined in Fig. 1(b).

Probability of failing safely detected $PF_{SD}$ (t) represents a probability that PE ≤ AL and that an alert is raised due to a failure of diagnostics. A false alert is then announced. The probability of failing safely undetected $PF_{SU}$ (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 this is outside the scope of this paper.

If PE exceeds AL and this hazardous state is 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 a part of the GNSS continuity risk CR(t), as will be shown below. The dangerous detected failure mode can be converted to the fail-safe state.

If PE exceeds AL without detection, it is a dangerous undetected failure, the so-called GNSS 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 CONTINUITY

The purpose of continuity is to guarantee that the service of a 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 (a very short time interval, e.g. 15s) of a safety operation. Continuity C(t) approximately means reliability that a system works within the specifications (desired accuracy and integrity is provided) within a stated period of time interval (0, t). It is different from integrity, which means correctness of information. Loss of Signal-In-Space (SIS) continuity is caused by unscheduled interruptions due to internal fault detection mechanisms, and not by shadowing objects along track, which are well predictable. The exact difference between reliability and continuity is explained in the following paragraph.

### 3.1 Probabilistic description of continuity

The probability of correct continuous position determination (PE ≤ AL) by GNSS system under absence of any failure is described by reliability R(t) and is represented by the base segment in the pyramid diagram of Fig. 1(b). Unreliable position (unacceptable PE or/and failure in diagnostics) is described by failure modes which are represented by probability segments $PF_{SD}$ (t), $PF_{SU}$ (t), $PF_{DD}$ (t), $PF_{DU}$ (t) at the top of the pyramid.

The question is "under what conditions is the continuous provision of accuracy provided by the GNSS system?”. It is evident that it is not in a case of failure detection and notification. Therefore, probability $PF_{SD}$ (t), i.e., probability of false alert, and $PF_{DD}$ (t), i.e., probability of true alert, describe the probability of the interruption of the position determination function and belong to continuity risk (CR), see Fig. 1(b). Both undetected failure modes, represented by probabilities $PF_{DU}$ (t) and $PF_{SU}$ (t), exist during position determination since the user does not know them.

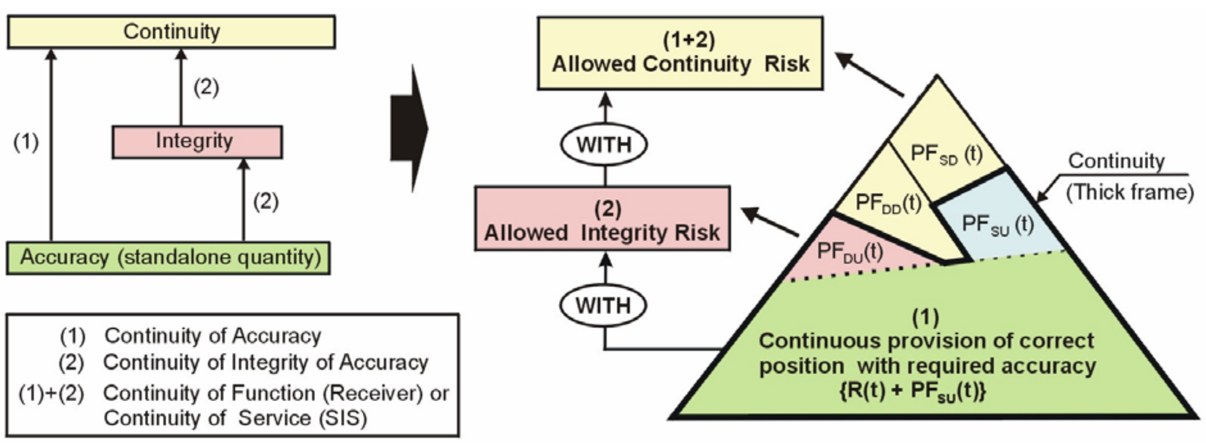
The probability of a hypothetical continuous provision of correct position (PE $\leq$ AL) is equal to R(t) + $PF_{SU}$ (t). The total probability of a continuous provision of position with acceptable integrity risk (possibly incorrect position due to a latent failure) is R(t) + $PF_{SU}$ (t) ++ $PF_{DU}$ (t), see Fig. 1(b). It is obvious that both undetected failures (SU, DU) can be revealed by a diagnostics based on physically diverse sensors.

3.2 Relation between reliability, integrity and continuity risks

Continuity is assured when a GNSS receiver provides, during operation: (1) navigation accuracy, and (2) accuracy guarantee, i.e., integrity. Accuracy is the only standalone parameter. The other GNSS quality criteria are accuracy dependent, as shown in Fig. 2(a). Continuity Risk (CR) is the complement of C(t), i.e., CR(t)=1 - C(t).

However, real systems can stop providing accuracy or integrity independently. In case of dangerous detected failure $PF_{DD}$ (t) accuracy can be lost (PE > AL) while integrity (timely warning) is provided. Alternatively, in case of safe undetected failure $PF_{SU}$ (t) accuracy is provided (PE $\leq$ AL), even if the ability to provide timely warnings is lost. In this case, the user considers that system’s integrity is OK, since he receives integrity flags.

Therefore, it is necessary to distinguish three kinds of continuity: (1) Continuity of Accuracy, (2) Continuity of Integrity of Accuracy, and (1+2) Continuity of Service /Function. In the case of safety applications of GNSS, (1+2) continuity should be considered - see Fig. 2(a). Figure 2(b) outlines a relation among (1+2) continuity risk, reliability of position determination during the desired time interval and other failure modes.




a) (b)

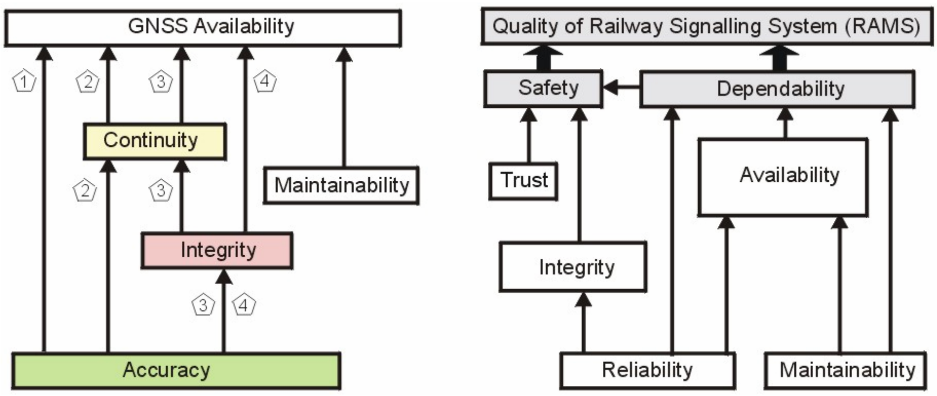
**Figure 2: The relation among: (a) GNSS continuity, integrity, and accuracy, (b) Integrity and continuity risks and probabilities of failure modes.**

Continuity C(t) in this figure includes R(t), $PF_{SU}(t)$ and acceptable GNSS integrity risk $PF_{DU}(t)$. Note that if once a quality of GNSS system is described in terms of failure mode probabilities, then integrity and continuity should be expressed in terms of risks IR(t), CR(t).

Dangerous detected failures (true alert) related to continuity risk are not as dangerous as undetected failures described by GNSS integrity risk. They can be converted to a fail-safe state. For example, a train can be stopped. However, it should be done only in an extreme case, when 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 additional physically diverse sensors (Filip, 2007).

## 4 GNSS AVAILABILITY VERSUS QUALITY OF SIGNALLING SYSTEM

The GNSS system is available if services of the system are within the required limits. That is, the requirements for accuracy, integrity and continuity of service/function are met. The mutual relation among the GNSS quality measures is outlined in Fig. 3(a).

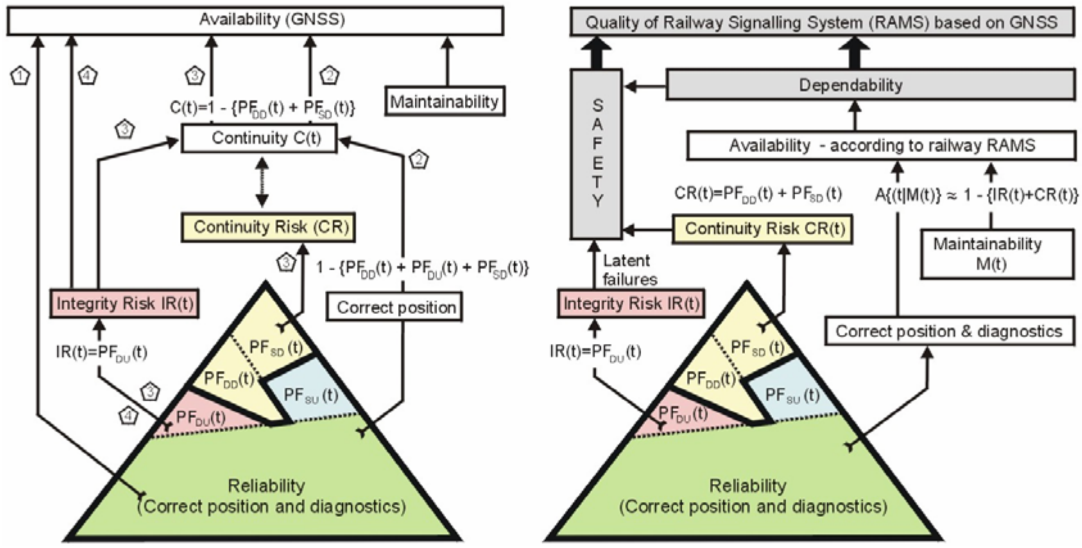



(a) (b)

**Figure 3: The relation among: (a) GNSS availability, continuity, integrity, and accuracy, (b) Quality attributes of railway signalling system.**

Since GNSS continuity and integrity are not standalone quality measures, as they depend on accuracy, then availability is guaranteed if the following conditions are simultaneously satisfied: (1) availability of accuracy, (2) availability of continuity of accuracy, (3) availability of continuity of integrity of accuracy, and (4) availability of integrity of accuracy – see Fig. 3(a). GNSS availability can be described by means of failure modes as shown in Fig. 4(a). Continuity C(t) consists of both unrevealed-by-diagnostics failure modes $PF_{SU}(t)$ and $PF_{DU}(t)$, and reliability R(t).

If a GNSS system is correctly operating at a time *t*, service is available. No requirement for successful operation during a specific time interval 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 – see Fig. 3(a). Continuity is related to service or function interruptions within a specified (short) time interval. Continuity itself does not say anything about the percentage of time that a system should be in operation. A system can be accurate, have high integrity of accuracy 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 measures, then we talk about the availability of continuity, availability of integrity, etc. GNSS availability at user level also implies that the GNSS receiver is able to predict the accuracy, integrity and continuity performance over the next critical operation period and that the predicted values must not exceed the specified values.




(a) (b)

**Figure 4: Quality attributes of: (a) GNSS system, and (b) Railway signalling based on GNSS.**

4.1 Quality attributes of GNSS based railway signalling

A relationship between the main quality attributes of railway signalling system (RAMS) is outlined in Fig. 3(b). As results from the “railway” definition of availability (EN 50126), a system is available if it is successful at a time *t*. In case of a location determination unit, successful operation means that, for example, a desired accuracy is met (PE $\leq$ AL) and diagnostics work correctly.

Availability (EN 50126) is a combination of reliability and maintainability. Trust of the provided accuracy is described separately from availability by means of integrity requirement - see Fig. 3(b). Safety requirements are not included in railway availability. In relation to railway safety related systems, we usually talk about availability (dependability) and safety.

On the other hand, GNSS safety requirements (i.e., integrity and continuity) are directly involved in GNSS availability as results from Fig. 3(a). GNSS system is available if also (among others) safety integrity requirement is assured.

The use of the GNSS quality criteria within railway RAMS is proposed in Fig. 4(b). It results from the analysis of GNSS integrity and continuity risks performed in the above parts 2 and 3. Instead of the notion of integrity in Fig. 3(b), the term GNSS integrity risk IR (t) is used in Fig. 4(b), which is one complement of integrity and expressed by means of $PF_{DU}$ (t). In railway safety systems, a failure rate per hour shall be used instead of a probability per duration of operation for the purpose of a quantitative safety analysis. An approach to convert GNSS integrity risk to the dangerous failure rate per hour has been proposed in (Filip, 2007). GNSS continuity risk CR(t) includes both detected failure modes $PF_{DD}(t)$ and $PF_{SD}(t)$ as both have an impact on the safety of the system.

Availability A(t) according to EN 50126 depends on the 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 probability of incorrect operations U{t|M(t)} under condition that maintainability M(t) is provided ($\forall$ t, M(t)=1).

The probability of incorrect operations of the GNSS system can be determined from the given integrity risk $IR(t)= PF_{DU}(t)$ and the continuity risk $CR(t)= PF_{DD}(t) + PF_{SD}(t)$ as $U\{(t|M(t)\}= PF_{DU}(t) + PF_{DD}(t) + PF_{SD}(t)$. The remaining probability of safe undetected failure mode $PF_{SU}(t)$ is, for the sake of simplicity, added to the reliability segment R(t). This simplification can be performed, since the correct position is provided. Then availability $A\{t|M(t)\}$ can be expressed as

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

In spite of the fact that GNSS service performance is defined by means of notions that come from the aviation sector, the railway sector can employ them, with respect to their specific meaning according to railway standards (see Fig. 5).

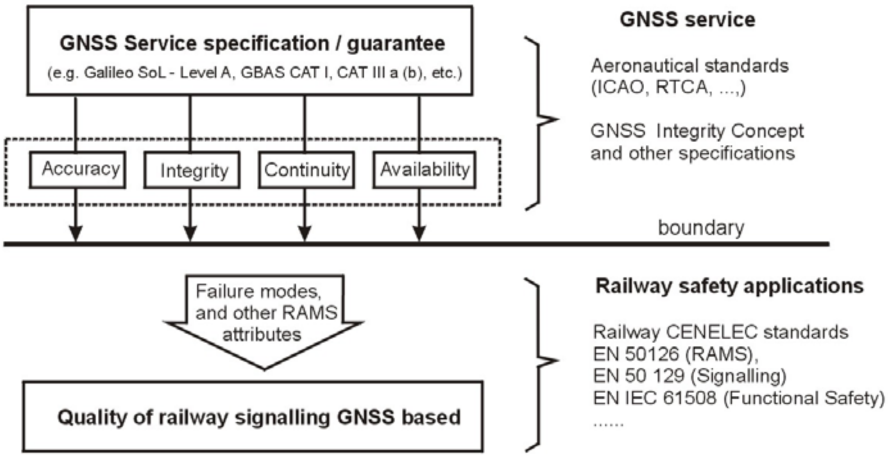



**Figure 5: The relation between GNSS service specification and railway RAMS.**

ICAO's Required Navigation Performance measures (continuity and integrity risks) can be converted to failure modes and used together with other GNSS RAMS (such as availability, MTTR after discontinuity event, etc.) for design and verification of GNSS based railway safety related system according to railway standards EN 50126 and EN 50129.

4.3 Availability for railway signalling

According to the Galileo SoL - Level A service specification (Galileo Integrity Concept, 2005) SIS should be available at 99.5% of time. It means that SIS for SoL Level A may not be available 438 hours per year. Note that possible SIS interruptions due to objects alongside the 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 95% of time, i.e., 438 hours per year, i.e., approximately 18 days.

Availability requirements for signalling equipment result from the safety and operational requirements for the 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 (ERTMS/ETCS RAMS, 1998). 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 would be needed to achieve this very high railway availability target.

## 5 CONCLUSIONS

Knowledge of the exact relationship between GNSS quality measures and railway RAMS is important for the design and verification of railway safety related systems. In this paper, we have shown how to employ GNSS quality criteria according to railway RAMS. Analysis performed in this paper shows that GNSS continuity does not exactly correspond to reliability and what the difference between GNSS and railway availability is according to EN 50126. In spite of the different definitions and notions used for the description of GNSS quality criteria and railway RAMS, it is possible to find a relationship between them.

## 6 ACKNOWLEDGEMENT

This work was funded by the INRETS in the period November 2007 - April 2008. The work was also partially supported by the National Science Foundation of the Czech Republic under contract No. 102/06/0052 (project *GNSS Local Elements for Railway Signalling*), and the Ministry of Transport of Czech Republic under contract No. CG743-037-520 (project *Certification of the Satellite Navigation System Galileo for Railway Telematic Applications*).

## REFERENCES

EN 50126, 2002. *The Specification and Demonstration of Dependability – Reliability, Availability, Maintainability and Safety (RAMS)*.

EN 50129, 2003. *Railway applications: Safety related electronic systems for signalling*.

EN IEC 61508 (1-7), 2002. *Functional Safety of electrical/electronic/ programmable electronic safety-related system.*

*Galileo Integrity Concept*, 2005. ESA document No. ESA-DEUI-NG-TN/01331.

ICAO, 2004. *Aeronautical Telecommunications*, vol. I (Radio Navigation Aids), Amendment 79, pp. B-83, B-84.

RTCA, 2004. *Minimum Aviation System Performance Standards for the Local Area Augmentation System (LAAS)*, RTCA DO-245 A.

*ERTMS/ETCS RAMS Requirements*, 1998, Chapter 2 – RAM. Version 6.

Filip, A., 2006. *Railway Safety Certification Requirements for the Galileo Signal-In-Space*. CERGAL, Braunschweig, 4-6 April.

Filip, A., 2007. *Safety Aspects of GNSS Based Train Position Determination for Railway Signalling*. UIC GALILEO for Rail Symposium, Paris, Oct. 18-19.

Kovach, K., 1998. *Continuity: The Hardest GNSS Requirement of All*. ION GPS-98, Nashville Convention Center, Nashville, Tennessee, Sept. 15-18.

Zahradník, J. et al., 2004. *Bezpečnosť železničných zabezpečovacích systémov*, Žilina.