Significance of the Galileo Signal-in-Space Integrity and Continuity for Railway Signalling and Train Control

A. Filip, H. Mocek and J. Suchanek
Czech Railways, Pardubice, Czech Republic

Abstract

One of the main difficulties complicating consistent evaluation of the Galileo Safety of Life (SoL) service applicability for railway safety related systems is absence of a clear methodology for interpretation of the existing Galileo Signal-In-Space (SIS) quality measures (i.e. accuracy, integrity, continuity, availability and related metrics) to the railway dependability and safety attributes according to the railway safety standards EN 50126, EN 50129, etc. Therefore, the main objective of this paper is to respond to some fundamental questions concerning utilization of the Galileo SoL SIS quality criteria for railway safety related functions and provide assessment, what can railway users expect from the Galileo SoL service.

1 Introduction

The derivation of the already specified Galileo SIS quality measures mainly results from the aeronautical safety philosophy through the Required Navigation Performance (RNP) concept specified by the International Civil Aviation Organization (ICAO). However, the ICAO’s RNP concept doesn’t meet safety and dependability requirements specified in the European railway safety standards EN 50126, EN 50129, etc.

First of all, the derivation of the ICAO’s RNP’s Target Level of Safety (TLS) is briefly described. The TLS results from the statistical data of accidents for a given period of time.

Global Navigation Satellite System (GNSS) SIS safety requirements are expressed from the TLS as the acceptable probabilities of dangerous failures per duration of the specific phase of flight operation and the relation with the Galileo SoL – Level A service performance is shown.

Further, the fundamental railway safety principles according to EN 50126, EN 50129 are briefly outlined in terms of the functional and technical safety. In order to achieve, maintain and guarantee the required level of safety, a systematic methodology, consisting of the Risk Analysis (Railway Authority’s Task) and Hazard Control (Supplier’s Task), must be used according to the EN 50129 standard.

In order to interpret Galileo SIS quality measures to railway safety terms, there is necessary to understand first what is and what is not a failure, and how SIS failures can be classified. Consequently, the SIS integrity risk (IR) and SIS continuity risk (CR) are described by means of the failure modes.

The second part of the paper deals with the interpretation of the Galileo SIS quality measures by means of the railway safety metrics. Their inclusion among the railway dependability and safety attributes, and their influence on the railway safety and dependability measures is discussed.

In contrast to the ICAO’s TLS, the acceptable integrity risk that represents one part of railway safety requirements, shall be expressed by means of the Tolerable Hazard Rate per hour (THR). Since the aeronautical integrity risk is expressed as the probability of dangerous failure per duration of flight operation, the difference between terms of the probability of dangerous failure per time interval and the hazard rate is investigated.

It is explained how to numerically convert Galileo SIS integrity risk to the hazard rate on hour basis and how to describe the continuity risk in terms of unreliability. There is also described a meaning of loss of the continuity for railway safety functions and its impacts on railway safety and dependability.
2 Derivation of Galileo Signal-In-Space quality measures

The existing safety requirements for GNSS SIS were driven mainly by the needs of civil aviation. 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 [5] as evident in Fig. 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 x 10^(-5) / 1 flight. After the TLS improvement (e.g. due to air traffic increasing), the value of 1.5 x 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 x 10^(-8) was allocated from the total TLS to final approach with the average duration of 150 s [5].

Therefore, the integrity and continuity risks, which were derived from the risks for individual flight operations, were also expressed in terms of probability per operation [5]. The only difference is that the integrity risk (latent 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).

![Fig 1: Target Level of Safety for GNSS in Aviation.](image)

GNSS SIS integrity and continuity risks requirements were derived accordingly to the fault tree analysis from allocated risk for a given operation [5]. The following considerations are related to final approach and start from risk of 1 x 10^(-8) / 150 s, as evident from diagram in Fig. 1. The fact that not every hazardous event will lead to an accident gives the reduction of the initial TLS with ratio of 1:10. The corresponding risk value of 1 x 10^(-7) / approach is equally sub-allocated among the total system integrity and continuity risks. The integrity and continuity risks are subsequently reduced by the pilot [5]. Finally the loss of integrity of 3.5 x 10^(-7) / 150 s is sub-allocated among the SIS integrity risk IRSIS = 2 x 10^(-7) / 150 s, the integrity risk of GNSS receiver on airplane IRREC = 5 x 10^(-8) / 150 s and the database integrity risk IRDBS = 1 x 10^(-7) / 150 s. Similarly, the loss of continuity CR = 1 x 10^(-5) / 15 s is sub-allocated among the SIS continuity risk CRSIS = 8 x 10^(-6) / 15 s and the continuity risk of onboard GNSS receiver CRREC = 2 x 10^(-6) / 15 s.
The Galileo SIS SoL - Level A service performance requirements (see Table 1) originate from the IRSIS and the CRSIS. The Level A service shall cover operations requiring guidance with short exposure time and with very stringent dynamic conditions, for example, in the aviation domain approach operations with vertical guidance (APV II).

<table>
<thead>
<tr>
<th>SIS Integrity Risk (IR_{SIS})</th>
<th>2 x 10^{-7} in any 150 s</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIS Continuity Risk (CR_{SIS})</td>
<td>8 x 10^{-6} in any 15 s</td>
</tr>
<tr>
<td>Availability of Service</td>
<td>99.50 %</td>
</tr>
<tr>
<td>Time-to-Alarm (TTA)</td>
<td>6 s</td>
</tr>
<tr>
<td>Accuracy (95%) H / V</td>
<td>4 m / 8 m</td>
</tr>
<tr>
<td>HAL / VAL</td>
<td>40 m / 20 m</td>
</tr>
<tr>
<td>Dual Frequency (E5+L1 or E5b+L1)</td>
<td>YES</td>
</tr>
<tr>
<td>Single Frequency (L1 or E5b)</td>
<td>NO</td>
</tr>
<tr>
<td>Coverage</td>
<td>Global</td>
</tr>
</tbody>
</table>

Table 1: Galileo SoL - Level A service (critical requirements) [7].

Although Galileo SoL - Level A is mainly intended for aeronautical operations, it is expected it will be also used for signalling and train control [7]. However, the problem is that the mission Level A requirements are specified by means of quality measures covering aerial operations only and doesn’t include railway RAMS attributes (Reliability, Availability, Maintainability and Safety). Since railway safety requirements for SIS are missing, following procedure should be done: 1) analyze the aeronautical SoL Level A requirements, 2) transfer the Galileo SIS quality measures to railway terms of safety and dependability, 3) propose how to use the Galileo SIS quality measures within railway RAMS with respect to the functional and technical safety [1, 2, 3], and 4) evaluate how much the Galileo SoL – Level A service meets railway needs for signalling and train control.

3 Railway requirements for train position locator GNSS based

European railway user community specified basic requirements for GNSS Train Position Locator (TPL) within GNSS Rail Advisory Forum in 2000 [8]. The requirements are summarized in Table 2. In order to employ Galileo SoL for railway applications including safety related functions, it is necessary to specify, which quality criteria should Galileo achieved and guaranteed. However, in this early development phase would be at least desirable to propose a way how exactly use the specified Galileo SoL Level A service for railway safety applications in terms of railway RAMS [1] and according to railway safety principles [2].

TPL based on GNSS performs safe train position determination function, if TPL position error is within user defined Alert Limit (AL) as illustrated in Fig. 2(a). Example of hazardous failure of TPL is depicted in Fig. 2(b). In that case the TPL position error exceeds the AL due to the dangerous SIS failure. Figure 2(c) shows this example of hazardous head of train determination for AL = 2.5 m (ATC on high density lines/ Station/ Parallel track) in horizontal plane.

<table>
<thead>
<tr>
<th>Application/ Lines</th>
<th>Horizontal Accuracy [m]</th>
<th>Integrity Alert Limit - HAL [m]</th>
<th>Integrity TTA [s]</th>
<th>Continuity of Service [%]</th>
<th>Interruption of Service [s]</th>
<th>Availability of Service [% of time]</th>
<th>Fix Rate [s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATC Corridors Station tracks</td>
<td>1</td>
<td>2.5</td>
<td>&lt; 1.0</td>
<td>&gt; 99.98</td>
<td>&lt; 5</td>
<td>&gt; 99.98</td>
<td>1</td>
</tr>
<tr>
<td>Middle density</td>
<td>10</td>
<td>20</td>
<td>&lt; 1.0</td>
<td>&gt; 99.98</td>
<td>&lt; 5</td>
<td>&gt; 99.98</td>
<td>1</td>
</tr>
<tr>
<td>Low density</td>
<td>25</td>
<td>50</td>
<td>&lt; 1.0</td>
<td>&gt; 99.98</td>
<td>&lt; 5</td>
<td>&gt; 99.98</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Table 2: Railway requirements for GNSS train position locator [8].
4 Railway safety concept

Railway safety concept is especially determined by means of CENELEC standards [1, 2, 3]. Railway signalling systems are characterized by the RAMS quality attributes as stated in the railway standard EN 50126. The normal metrics of reliability, availability, and MTTF only suggest a measure success. The reliability goal is to reduce the probability of operational failures, whereas safety is focused on reduction of the probability of critical (dangerous, hazardous) failures.

Safety and risks are mainly based on knowledge of all safety related functions, safety related failure modes (safe, unsafe, …) in specified applications and environment, all possible hazards and their frequency of occurrence, rate of occurrence of safety related failure modes, consequences of hazardous events, etc. It is necessary to consider both the quantitative and qualitative safety assessment.

Safety requirements of railway safety systems are composed of: 1) Functional safety requirements [2, 3], and 2) Technical safety requirements [2]. Functional safety means proper performance of all required safety functions in expected working environment, while technical safety means what is the prediscribed behaviour of the system in case of failure(s).

Safety function is a keystone of functional safety. If the safety function is performed, the dangerous event will not take place. The safety function is determined from the hazard analysis. Safety function determines which action has to be done to achieve or maintain a safe state of the safety related systems.

The quality of safety function, which is referred as the safety integrity, is determined from the risk assessment. The technical safety of railway signalling systems is related to the safe construction of signalling equipment and it includes requirements for integrity against systematic and random failures.

Main principles of the technical safety include:

1. No failure can endanger ride of train.
2. Any failure must be detected in fast enough manner.
3. If (2) is impossible, one must presuppose any other failure, which must be detected together with the first one.
4. If dependent failures can arise, all their combinations must be considered.
5. System/subsystem should enter in a safe state after detection of a failure.
6. If system is in a safe state, any other failure must not restore its function.

Note: It is assumed that only one failure can arise in one instant of time.

In order to define safety requirements, Risk Analysis and Hazard Control (System Design Analysis) have to be carried out. A systematic methodology to achieve railway safety is well described in [2]. Risk Analysis that is the task of Railway Authority investigates consequences of potential dangerous states. Quantitative risk analysis determines the level of protection from the random failures, which can be defined by THR. THR shows the tolerable frequency of the given hazard. THR is one of the inputs for the consecutive Hazard Control. Hazard Control which is the task of a supplier includes management relating to realization of required THR and associated safety functions.
5 Classification of GNSS failure modes

In order to utilize GNSS system for railway safety relevant functions, the reliability and safety of position determination based on GNSS has to be performed. If a failure is considered then the significant increase in user Position Error (PE) can occur. The PE refers to the difference between a measured or estimated position and the true position. This failure is considered as dangerous when the PE exceeds Alert Limit (AL) defined by user, i.e. $\text{PE} > \text{AL}$. The AL is the maximum allowable error in the user’s position solution before alarm is alerted within the specified TTA. The failure is considered as safe if the PE is bounded within the AL, i.e. $\text{PE} \leq \text{AL}$. Reliability is provided during normal operation that involves SIS failure free cases, proper function of GNSS diagnostics, and correct position determination, i.e. $\text{PE} \leq \text{AL}$.

The following GNSS failure modes with consideration of diagnostics can be obtained, see Table 3: 1) Safe Detected (SD) – False Alert, 2) Dangerous Detected (DD) – True Alert, 3) Safe System (SS) failure, 4) Dangerous System (DS) failure, 5) Safe Undetected (SU), 6) Dangerous Undetected (DU) – Loss of integrity, and 7) Dangerous Detected Failure Free (DDFF) mode. Integrity Flag (IF) is part of the GNSS integrity messages.

<table>
<thead>
<tr>
<th>GNSS Failures</th>
<th>Safe PE $\leq$ AL</th>
<th>Dangerous PE $&gt; \text{AL}$</th>
<th>Integrity Flag (IF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected</td>
<td>SD = False Alert</td>
<td>DD = True Alert</td>
<td>Alert</td>
</tr>
<tr>
<td>System</td>
<td>SS Continuity Risk</td>
<td>DS Continuity Risk</td>
<td>Not Monitored</td>
</tr>
<tr>
<td>Undetected</td>
<td>SU</td>
<td>DU = Loss of integrity</td>
<td>Good</td>
</tr>
<tr>
<td>Without Failures</td>
<td>Normal operation</td>
<td>DDFF = True Alert</td>
<td>Good Alert</td>
</tr>
</tbody>
</table>

Table 3: GNSS failure modes vs. Integrity Flag status.

Failing safely detected (SD) represents cases when accuracy is provided (PE is within AL), but IF being raised (False Alert) due to a failure of diagnostics. Dangerous detected (DD) failures represent states which are hazardous detected. The DD failure mode can be converted to the fail-safe state. Special case of the DD mode represents Dangerous Detected Failure Free (DDFF) mode. The DDFF event occurs during SIS and GNSS diagnostics failure free operation, whereas the IF reports Alert in accordance with the incorrect position determination, i.e. $\text{PE} > \text{AL}$. The DDFF originates from dangerous detected failure due to the inconvenient geometry of the satellite constellation, number of ground reference stations, etc.

In case of SS and DS modes, IF indicates Not Monitored status. Integrity is not properly guaranteed by the system and GNSS losses the ability to provide timely warnings. User can only make a decision by means of alternative information (e.g. local elements utilization). In relation to this fact the SS mode should be considered as the SD one and similarly the DS mode should be supposed as the DD one. Integrity is not affected, whereas Continuity Risk is influenced as outlined in Table 3.

The SD and DD (including SS and DS modes) failures describe interruption of position determination function and belong to the loss of SIS continuity. Since there is not known to user whether SIS true or false alert was reported, the total SIS continuity risk is conservatively considered as the DD failure (see Fig. 3).

Failing safely undetected (SU) represents a non-critical safe failure (PE $\leq$ AL), but no failure is announced by built-in diagnostics. In this case user considers that system integrity is provided since he receives IF = OK. If PE exceeds AL and this state is not detected, it is dangerous undetected failure, so called integrity risk. It is the most feared failure in the system.
6 Interpretation of quality measures of Galileo Signal-in-Space SoL – Level A service

Galileo SoL service quality is defined in terms of accuracy, integrity, continuity, and availability with respect to the predefined alert limit and TTA (see Table 1). The relation among these GNSS terms, i.e. quality criteria, is depicted in Fig. 4. In the following parts of the paper, the interpretation of the GNSS notions within the quality attributes of railway signalling systems (RAMS) is provided.

6.1 Accuracy

Accurate position determination is the main objective of GNSS service. The fundamental quality criteria describing GNSS service is expressed in terms of accuracy that refers to the statistical measure of the positioning error, and is specified by the position error at 95% (2-sigma) confidence level. Accuracy is a standalone quantity with respect to the other GNSS quality criteria (integrity, continuity and availability). All of the other GNSS parameters are dependent on the accuracy. Accuracy represents a basis for apportionment of the other GNSS quality measures as it is illustrated in Fig. 4.

Accuracy is determined by the following major components of the positioning error: 1) Dilution of Precision (DOP), 2) pseudorange measurement accuracy, and 3) GNSS failures. The DOP is a function of the satellite-to-user geometry, while the pseudorange measurement accuracy is determined by the SIS user range error (URE) from each satellite. In case of fault-free conditions, satellite-to-user geometry and the SIS URE statistics can be well predicted. Consequently, all
accuracy and integrity losses can be predicted before the next operation, which can result in pre-
planned availability outages. In case of GNSS failure, the PE can not be properly predicted. Due to a
latent effect of the failure all GNSS quality attributes are influenced.

6.2 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 (see
Fig. 4). Integrity is often specified by its complement, called integrity risk, as outlined in Fig. 3. 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 [6].
Integrity risk is defined per duration of the entire operation.

A different situation is in the field of a functional safety of electrical/ electronic/ programmable
electronic (E/E/EP) safety-related system operating in continuous or high demand mode, where
according to the standard [3] the quantified safety integrity risk shall be expressed in term of the
Probability (average) of dangerous Failure per Hour (PFH). PFH in matter of fact means failure
intensity [3] as results from Equation (1), if considered time interval $T \rightarrow 0$. Then

$$PFH(t) \approx \frac{P(X_1 < T)}{T} = \frac{1 - R(T)}{T} \rightarrow -\dot{R}(t), \quad (1)$$

where $P(X_1 < T)$ is the probability of dangerous failure in time instant of $X_1$, and $R(T)$ is the reliability
of the system.

In railway safety related systems the quantified safety integrity shall be expressed according to the
standard EN 50129 [2] by means of the Tolerable Hazard Rate (THR). The hazard rate can be
expressed as Equation (2)

$$HR(t) = \dot{\lambda}(t)_{sys} = \frac{R(t) - R(t + \Delta t)}{\Delta t \cdot R(t)} = \frac{-\dot{R}(t)}{R(t)} = \frac{f(t)}{R(t)}, \quad (2)$$

where $HR(t) \cdot \Delta t$ or $\dot{\lambda}(t)_{sys} \cdot \Delta t$ represents probability of failure in the time interval $<t, t+\Delta t>$ given the
system had not failure in the time interval $<0, t>$. In other words, $HR(t)$ or $\dot{\lambda}(t)_{sys}$ is the failure intensity
$f(t)$ conditioned by the reliability $R(t)$. If the system is very reliable, then $R(t) \approx 1$ and

$$\frac{-\dot{R}(t)}{R(t)} \approx -\dot{R}(t). \quad (3)$$

Substituting Equations (1) and (2) into Equation (3) yields

$$PFH(t) \approx HR(t). \quad (4)$$

A value of the integrity risk for the Galileo SIS SoL – Level A (see Table 1) is defined as the
probability of dangerous undetected failure of $P_f = 2 \times 10^{-7}$ in any interval $\Delta t = 150$ s, i.e.

$$IR_{SIS} = \frac{P_f}{\Delta t} = 2 \times 10^{-7} / 150 \text{ s}. \quad (5)$$

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

$$f(t) = \frac{F(t + \Delta t) - F(t)}{\Delta t} \approx F'(t) = -\dot{F}(t), \quad (6)$$

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

$$F(0, T) = \int_0^T f(t) dt \quad (7)$$
According to Equations (1), (5), (6) and (7) the probability of dangerous failure per hour PFH is

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

$$= \frac{P_f}{1 \text{ hour}} \frac{3600 \text{ s}}{150 \text{ s}} = 24P_f/1 \text{ hour} = 4.8 \times 10^{-6} / 1 \text{ hour}.$$ (8)

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

It should be noted that the derived hazard rate of $4.8 \times 10^{-6} / 1 \text{ hour}$ by means of the cumulative probability principle can be considered to be rather conservative estimation. 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 events defined in Galileo. For example, this is the case of feared events due to satellite hardware failures, ground segment algorithm failures and excessive troposphere delays. Due to this reason the cumulative probability principle was used for hazard rate estimation in this paper. Utilization of the Galileo SIS integrity risk for railway safety applications will be also subject of our future research.

Note: Feared event is an event which leads to a degradation of the accuracy of the position solution computed by the user receiver.

6.3 Continuity

Continuous provision of positioning was introduced into GNSS quality measures based on aviation requirements. Continuity is the ability of the system to provide navigation accuracy and integrity throughout the intended operation given that the navigation accuracy and the integrity are provided at the start of the operation. Continuity is a quality measure if the system is functioning when it is really needed. Hence it expresses reliable operation (no failure) of the system during the specific time interval given that the system was operating at the start of the operation. Continuity is not exactly equivalent to reliability since a failure can remain undetected. Continuity is provided not only in case of normal operation, but it also covers both undetected failure modes (safe and dangerous), as evident from Table 3. As it is outlined in Fig. 4, continuity approximately corresponds to reliability that a system works within specifications within stated period of time interval since reliability is mostly influenced by the detected failure modes. Continuity (C) can be expressed as follows

$$C \equiv e^{-\frac{T}{MTBF}},$$ (9)

where $MTBF$ is Mean Time Between Failure, and $T$ is the continuity time interval. If $T \ll MTBF$, then

$$C \approx 1 - \frac{T}{MTBF}.$$ (10)

Continuity Risk (CR) 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) is related to unscheduled GNSS service interruptions. Loss of SIS due to obstacles along track is not loss of continuity since it can be well predicted according to the profile of surrounding environment along the track. The continuity risk is one complement of C according to Equation (11) as follows

$$CR = \frac{T}{MTBF}.$$ (11)

The Equation (11) yields corresponding $MTBF = 1.875 \times 10^6 \text{s} = 520.8 \text{ hours}$. Continuity risk for the Galileo SIS SoL - Level A of $8 \times 10^{-6}$ in any 15 s can be expressed as

$$CR_{\text{SIS}} = \lambda_{\text{DD}}(CR) + \lambda_{\text{SD}}(CR) \approx \lambda_{\text{DD}}(CR) = 1/MTBF = 1.92 \times 10^{-3} / 1 \text{ hour}.$$ (12)

$CR_{\text{SIS}}$ results from the presumption mentioned above that continuity risk is conservatively considered as the dangerous detected failures (true alert).
Continuity determines the cost of the navigation system. It is different from integrity, which corresponds to the correctness of the determined position. Loss of SIS continuity happens when the system has already started a safety function but the safety function must be unexpectedly interrupted.

As it is evident from the railway standard [1], 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. Moreover, it is not desirable to interrupt performing of the safety function (train position determination) due to potential SIS outages. Restrictions of railway operations or other irregularities due to loss of continuity are not generally desirable since they can negatively influence safety of the entire transportation system. Train stopping is an extreme solution. Position and speed should 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.

6.4 Availability

Availability of the navigation service is the probability that the positioning service and the integrity monitoring service are available and provide the required accuracy, integrity and continuity performances [6]. The expected values of the uptime and downtime in the steady-state condition are known as the mean uptime (MUT) and mean downtime (MDT). According to the Galileo SoL Level A service specification, the availability should be at least $A = 99.5\%$ at the service area (see Table 1). The corresponding mean up time is $\text{MUT}_{\text{SoL,A}} = 8716.2$ hours per year (1 year = 8760 hours). The mean downtime of the Galileo service is $\text{MDT}_{\text{SoL,A}} = 43.8$ hours per year. The MDT can consist of repair time and other delays. If the other delays are neglected, then MDT is proportional to mean time to repair (MTTR).

GNSS availability depends on reliable and safe GNSS positioning and also on maintainability. Quality criteria of positioning service such as accuracy, alert limit, time-to-alarm, and safety requirements (integrity and continuity) influence the resulting GNSS availability.

The quality attributes of railway signalling (RAMS) distinguish safety from availability. Safety (integrity) is not included in railway availability. Railway availability only depends on reliability and maintainability according to [1]. It is the fundamental difference between railway and GNSS availability, because GNSS availability anticipates that safety requirements (integrity and continuity) are also met. A probabilistic description of differences between GNSS availability and railway availability according to [1] has been recently described in [9].

From view point of railway safety applications it is not sufficient to know only a value of the availability (or MUT) provided by GNSS service. Another important criterion of the GNSS availability is MTTR after a SIS discontinuity event happens. A value of MTTR should be provided to railway industry and users.

7 Conclusion

Correct understanding and interpretation of GNSS quality measures is essential for future signalling and other railway safety applications based on GNSS. It creates a basis for design, validation and verification of railway systems based on GNSS according to the railway safety standards EN 50126, 50129, etc. In this paper, the origin of the GNSS quality measures has been outlined. Signal-In-Space integrity and continuity risks have been classified by means of GNSS failure modes and system reliability attributes. The difference between GNSS availability and availability according to the standard EN 50126 has been described. The numerical results illustrate the interpretation of the Galileo SoL Level A service quality measures in terms of RAMS. The presented results contribute to the implementation of satellite navigation to railway operations.

Acknowledgements

The work was 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).

The authors also wish to thank Dr. Lubor Bažant, Václav Maixner and Jan Taufer (all from the ČD – Laboratory of Intelligent Systems) for review of the paper and their comments.
References


