Efficient use of multi-constellation EGNOS for the European Train Control System

Aleš Filip
Faculty of Electrical Engineering and Informatics
University of Pardubice
Pardubice, Czech Republic
Ales.Filip@upce.cz

Abstract— **Exploitation of GPS based EGNOS and Galileo for safe train position determination within the modernised European Train Control System (ETCS) belongs currently among main priorities of the European joint GNSS and rail R&D. It is obvious that only the effective use of the aviation EGNOS SoL service according to CENELEC railway safety standards has the potential to replace costly ETCS track-side balises with much efficient Virtual Balises. This paper deals with optimization and justification of the ETCS Virtual Balise (VB) safety requirements for GNSS with the intention to meet them preferably by means of existing single-constellation EGNOS V2. The optimization has been achieved through the Location Determination System (LDS) with the reactive fail-safety architecture. The applicability of EGNOS V2 for the ETCS LDS with a single-channel structure has been justified by means a so-called Travelling Virtual Balise (TVB). It has been quantitatively demonstrated by means of the TVB that employment of EGNOS V2 together with rapid and independent EGNOS diagnosis based on safe ETCS odometry and other techniques is able to meet SIL 4 requirement for the LDS at a system level. Galileo as a second constellation within future EGNOS V3 can be effectively used for the availability of integrity improvement**.

Keywords—Satellite navigation; GNSS; GPS; EGNOS; ETCS; Galileo; LDS; QZSS; SBAS; SDCM; SIL 4; WAAS; railway signalling; safety-related systems; high-safety integrity; reactive fail-safety; composite fail-safety; travelling virtual balise

I. INTRODUCTION

Nowadays it is generally believed that exploitation of Global Satellite Navigation Satellite System (GNSS) together with advanced mobile communications for signalling and train control will significantly improve safety and efficiency of railway operations. This is especially true for signalling solutions on low traffic lines and also on some long heavy haul lines where previously planned implementations of the European Train Control System (ETCS) with track balises have appeared as economically unrealistic. Moreover, there are currently visions that ETCS solutions based on GNSS will be installed on main corridor and high-speed lines as well.

The very idea of combining satellite navigation and the ETCS for train localization purposes is not new. A mixed train position determination solution by means of ETCS track balises and virtual GPS ones has been already described in the nineties of the last century [1]. Before that, a series of tests focused on train position determination using GPS and DGPS had been performed mainly in the United States and Europe.

On the 2nd March 2011, the European Geostationary Navigation Overlay Service (EGNOS) with its Safety-of-Life (SoL) Service was officially declared available for safety operations in aviation. EGNOS belongs to the family of wide-area Satellite Based Augmentation Systems (SBAS), similarly as US WAAS [2], Japanese MSAT/QZSS, Russian SDCM. In spite of fact that SBAS with its SoL service was originally developed and certified for safety operations in aviation, it also represents a strategic infrastructure for safety-related systems in other modes of land transport [3], [4].

Safe train Location Determination System based on GNSS and intended for the European Train Control System belongs among them. It is mainly due to fact that high investment and operational costs of the ETCS track balises used for safe train position determination discourage from further ETCS expanding not only in Europe, but also worldwide. Therefore, at present, the European Commission, institutions and railway industry strongly support replacement of physical balises with virtual ones based on EGNOS and Galileo. This intention is practically realised within several international ESA and H2020 projects, and also within numerous national R&D activities in the individual EU member states.

However, only the efficient exploitation of EGNOS for railway signalling according to specific ETCS safety requirements, TSI, railway CENELEC safety standards [3]-[9], etc. can bring applicable solutions. A clear LDS safety concept fully exploiting characteristic GNSS features within the virtual balise (VB) concept, such as provision of abundant train positions in time, is the basis for derivation of the realistic ETCS safety requirements for the EGNOS SoL service. It is evident that rapid and independent diagnosis of excessive EGNOS errors significantly contributes to achievement of the required Tolerable Hazard Rate (THR) for the ETCS virtual balises and also for the GNSS LDS.

Basic safety requirements for the train location determination function based on GNSS were specified within the ESA 3InSat project (2012-2015) [10], [12]. It was found

This work was supported from the European H2020 research and innovation programme within the RHINOS project (2016-2017).

that THR for Signal-In-Space (SIS) should meet 1e-8/ 1 hour (SIL 4) and the maximal Confidence Interval in the position domain should not exceed 14 m for the most demanding ETCS operational scenarios. In order to meet the specified safety requirements, the dual-constellation EGNOS-R / SBAS-R interface for EGNOS V3 has been proposed [11], [12].

However, multi-constellation/ multi-frequency EGNOS V3 is expected to be available as lately as in 2022 and the current pressure for signalling and train control solutions based on GNSS is continually growing. Moreover, there is still a will to employ existing EGNOS V2, which has been once certified for aviation, for railway signalling as well. That's why new ways and methods enabling efficient exploitation of single-constellation EGNOS V2 in railway sector are still investigated.

This paper deals with the harmonization of the ETCS and aviation safety integrity requirements for the GNSS SoL service with the intention to meet the safety requirements using a single-constellation SBAS. In contrast to the recently applied composite fail-safety principle within the multi-constellation EGNOS-R railway interface for EGNOS V3, here in this paper the main attention is focused on the utilization of reactive fail-safety, which can be implemented using rapid and independent diagnosis of the provided EGNOS PVT solutions. It has been assessed that reactive fail-safety would enable to increase the required ETCS THR for EGNOS SIS from 1e-8/ 1 hour to about 1e-7/ 1 hour or even less. The increase in THR for SIS corresponds to the change in Safety Integrity Level (SIL) from SIL 4 to SIL 3.

Safe train position determination within the ETCS is outlined in Section II. Basic fail-safe principles applicable in railway safety-related systems compliant with SIL 3 and SIL 4 and their relation to the mono/multi-constellation LDS solutions are described in Section III. Section IV. outlines the apportionment of Tolerable Hazard Rate for the ETCS virtual balise. The applicability of EGNOS V2 for the ETCS LDS reactive fail-safety architecture is justified by means a so-called Travelling Virtual Balise (TVB) in Section V. The SBAS THR apportionment within the LDS with the reactive fail-safety architecture is outlined in Section VI. Section VII. summarises basic features and benefits of the TVB. Finally, a promising method for detection and identification of excessive errors due to local effects by means 3-dimensional (3D) track map is outlined in Section VIII.

II. Safe Train Position Determination For ETCS

In order to demonstrate the positive impact of the GNSS diagnosis on the ETCS safety integrity, a train position determination function within the ETCS using classical track balise groups and virtual balises is outlined first.

The classical ETCS track balise group, also called Information Point (IP), which shall be compliant with SIL 4 (λ_{IP} of 1e-9/1 hour) [5], determines together with the ETCS on-board balise reader, a so-called Balise Transmission Module (BTM), the absolute position of train. The ETCS odometry (SIL 4) provides the instant speed of train and the relative distance from the Last Relevant Balise Group (LRBG) including its Confidence Interval (CI). The train position, velocity and other data are reported via radio (GSM-R) to the track-side Radio Block Centre (RBC). One of the important odometry functions is called linking of balises via the relative distance measurement. It is in fact the independent diagnosis of balises and on-board unit (ONB) because it enables detection of a deleted (missing) balise, incorrectly inserted balise or an ONB fault.

In case of the virtual balise concept the absolute position of train is determined using the LDS based on GNSS. The instant position of the train is compared with the position of virtual balises whose coordinates stored in the on-board European Vital Computer (EVC) and in RBC. If the actual GNSS train position together with the relevant Confidence Interval (CI) match with a virtual balise stored in the database, then the VB is considered as the Last Relevant Virtual Balise (LRVB). The odometry together with the track database perform two following functions: 1) diagnosis of the consecutive virtual balises using linking with its direct positive impact on the desirable reduction of the safety integrity requirement for the

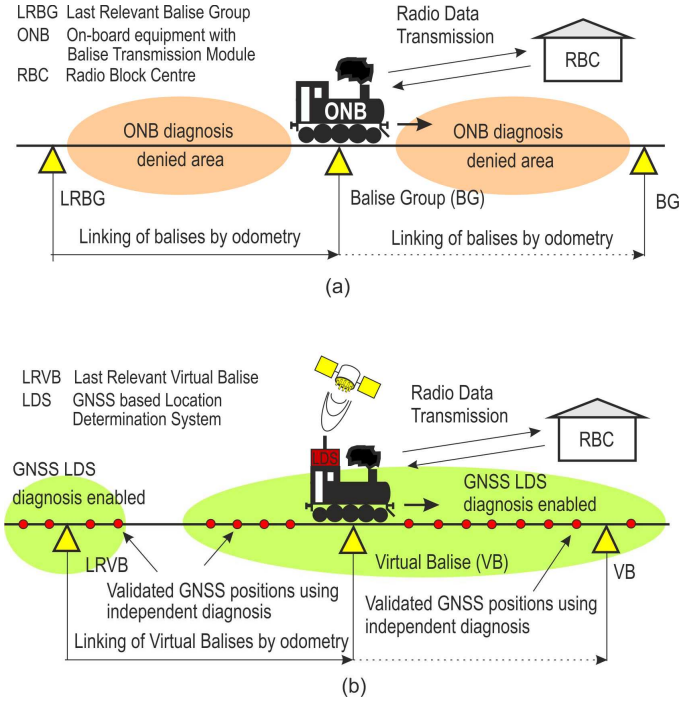

Fig. 1. Safe train position determination using: (a) ETCS track balise groups, and (b) GNSS based Location Determination System.

GNSS LDS – i.e. GNSS THR increasing, and also 2) provision of the relative train position from LRVB if GNSS SIS is temporally unavailable due to SIS service outages or SIS shadowing in a harsh railway environment.

The above described virtual balise concept copies in fact the ETCS train position determination function using track balise groups. Now it should be said how ETCS can profit from GNSS. Let's compare for this purpose the diagnosis of position determination in case of the track balise based ETCS and diagnosis for the ETCS VB concept.

As it is evident from Fig. 1(a), the ETCS on-board unit ONB is able to perform fault diagnosis of physical balise groups (BGs) and also its own diagnosis only in locations of the BGs. It is possible thanks to BG linking because position of next BG with respect to the Last Relevant Balise Group (LRBG) position is known to the ONB and the correct BG detection can be validated using a so-called Expectation Window (ExW). The ExW includes all potential uncertainties due to odometry and BG position errors. However as it is depicted in Fig. 1 (b), GNSS LDS is naturally able to perform its fault diagnosis also in the vicinity of virtual balises or on the whole track section between virtual balises, depending on SIS visibility.

Safe GNSS train position determination also available in locations between VBs is needed for LDS initialization in Staff Responsible (SR) mode. The former THR requirement for GNSS LDS of 3e-8/ 1 hour [12] was derived just for SR mode. However this THR requirement was still quite demanding due to the applied relatively long average time to fault detection (36 s) resulting from the infrastructure model for conventional lines.

The abundant GNSS train positions outside of the VB vicinity are not in fact needed under normal operation (after LDS initialization) for train position reporting to RBC because it is provided by means of the relative distance measurement

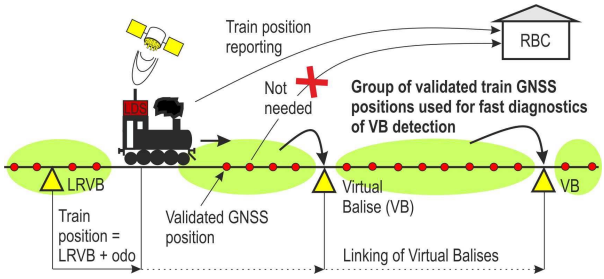

Fig. 2. Exploitation of GNSS train positions within VB concept.

from the Last Relevant Virtual Balise (LRVB) – see Fig. 2. However it is evident that these abundant GNSS positions together with the odometry data can be effectively used for the GNSS diagnosis and it can finally lead to reduction of safety requirements for the GNSS based LDS.

III. Single and Multi-Constellation SBAS for ETCS

Railway safety related systems to be compliant with SIL 3 or SIL 4 must ensure that they will remain safe in the event of any kind of single random HW fault. This principle is known as fail-safety and can be achieved by means of the following techniques [9]: inherent fail-safety, composite fail-safety or reactive fail-safety. It is evident that implementation of these techniques not only determines which level of LDS safety will be achieved, but also how efficiently GNSS will be used within the LDS. The applicability of the individual fail-safety techniques within the GNSS LDS is analysed below.

The inherent fail-safety technique allows a safety-related function to be performed by a single channel, provided that all the credible failure modes of the channel are not hazardous. It would be very difficult or impossible to make such evidence in case of complex SBAS and therefore inherent fail-safety is not further considered for the SBAS based LDS.

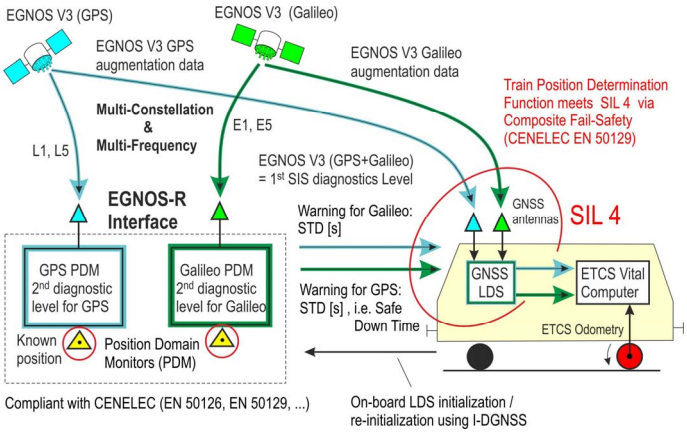

Fig. 3. Principle of LDS based on dual-constellation EGNOS and composite fail-safety.

The composite fail-safety technique allows a safety-related function to be performed by at least two independent channels. Hazardous fault in one channel shall be detected and negated in sufficient time to meet the required THR. The fault is detected by the comparison of the output values of these two or more channels, or also by means of an additional independent diagnosis. This technique has been already employed in case of the above mentioned dual-constellation EGNOS-R interface [11], [12] - see Fig. 3. The EGNOS-R interface (see Fig. 4) was mainly proposed with the intention to meet THR of 1e-8/ 1 hour (SIL 4) for Signal-In-Space and

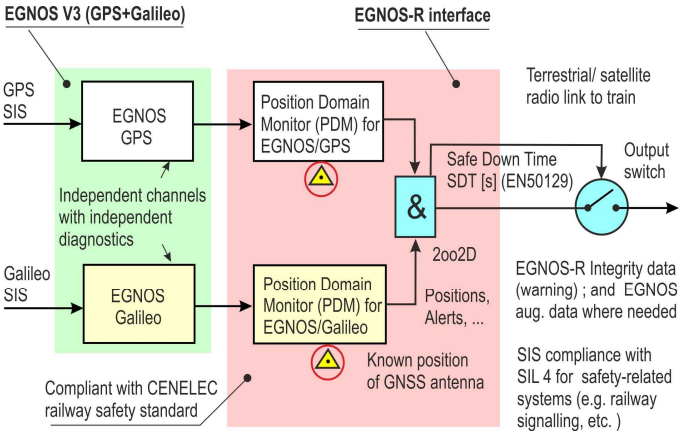

Fig. 4. Dual-constellation EGNOS-R interface for ETCS.

simplify the required safety case and certification according to railway CENELEC safety standards. It was found that introduction of EGNOS-R also enables to reduce the EGNOS Confidence Interval (CI) magnitude in the position domain [11].

Finally, the reactive fail-safety technique allows a safety-related function to be performed by a single channel, provided

its safe operation is assured by fast detection and negation of any dangerous fault. The existing single-constellation SBAS itself can be considered as a system with reactive fail-safety, because the safety function is performed by the GPS and its correctness is checked by the SBAS infrastructure – see Fig. 5. Nevertheless, the standalone SBAS is not yet able to meet the ETCS SIL 4 requirement for train position determination. Excepting this the position determination function must also meet the required integrity level in case of local effects, such as multipath, EMI, spoofing, etc. against which SBAS does not protect. That's why the SBAS fault diagnosis must be

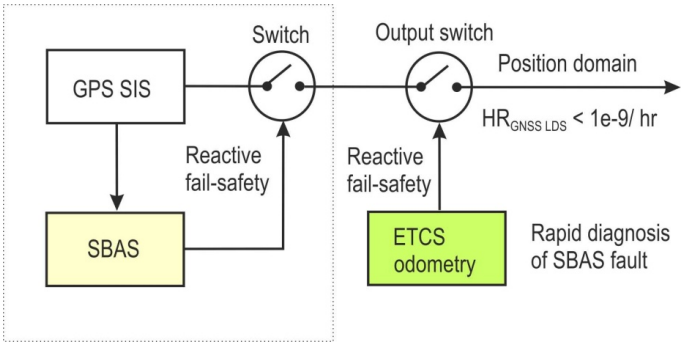

Fig 5. Single-constellation SBAS and odometry as LDS with reactive fail-safety.

completed with an additional independent fault diagnosis realised e.g. using safe ETCS odometry (SIL 4), 3-dimensional track database (SIL 4) and other relevant techniques.

Markov model of the LDS based on single-constellation SBAS and reactive fail-safety is depicted on Fig. 6.

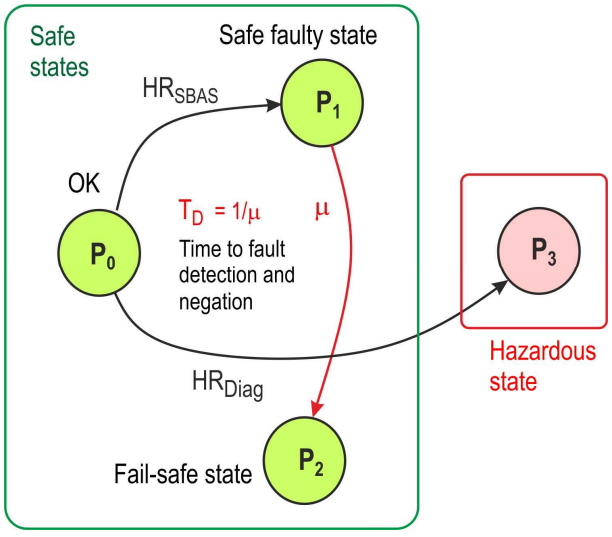

Fig. 6. Markov model of LDS based on SBAS with reactive fail-safety architecture.

The following four system states are defined for the model:

- P_0 – Fully functional LDS state: both SBAS and independent SBAS diagnosis work well according to the specifications;
- P_1 – Safe faulty LDS state: SBAS is faulty and rapid diagnosis is functional;
- P_2 – Fail-safe state of the LDS: SBAS fault was detected and negated;
- P_3 – Hazardous LDS state: Independent diagnosis of SBAS is faulty. Note: Although SBAS is functioning properly according to the specifications, the LDS is in a dangerous state.

The corresponding time-dependent LDS state probabilities can be derived from the model as follows:

$$P_0(t) = 1/\exp(t*(HR_{SBAS} + HR_{Diag})) \quad (1)$$

$$P_1(t) = -(HR_{SBAS}*(1/\exp(t*(HR_{SBAS} + HR_{Diag})) - -1/\exp(\mu*t)))/(HR_{SBAS} + HR_{Diag} - \mu) \quad (2)$$

$$P_2(t) = (HR_{SBAS}*(HR_{SBAS} + HR_{Diag} - \mu + +\mu/\exp(t*(HR_{SBAS} + HR_{Diag})) - -HR_{SBAS}/\exp(\mu*t) - HR_{Diag}/\exp(\mu*t)))/ /((HR_{SBAS} + HR_{Diag})*(HR_{SBAS} + HR_{Diag} - \mu)) \quad (3)$$

$$P_3(t) = -(HR_{Diag}*(1/\exp(t*(HR_{SBAS} + HR_{Diag})) - 1))/ /(HR_{SBAS} + HR_{Diag}) \quad (4)$$

where HR_{SBAS} – Hazard Rate of SBAS per 1 hour, HR_{Diag} - Hazard Rate of SBAS independent diagnosis, μ - rate of diagnosis and fault negation. $P_1(t)$ is the safe faulty state probability in case of SBAS failure. Since $(HR_{SBAS} + HR_{Diag})$ is much smaller than μ, then (2) can simplified by as follows

$$P_1(t) \approx -HR_{SBAS}[1-0]/(HR_{SBAS} + HR_{Diag} - \mu) = = HR_{SBAS}/\mu = HR_{SBAS} \times T_D \quad (5)$$

where T_D is time to fault detection and negation, which is also sometimes called Safe Down Time (SDT) [9]. It is evident from (5) that $P_1(t)$ depends on T_D (i.e. on $1/\mu$) and is no longer dependent on the time t. This relation is also depicted in Fig. 7. It also means that the corresponding Hazard Rate during 1 hour long mission can be expressed as $HR_{SBAS} \times T_D \times 1\ hour^{-1}$. It is used for derivation of the ETCS THR requirement for SBAS in Section V.

At least two independent GNSS constellations are needed for composite fail-safety to achieve the required level of LDS safety. It seems it might be much easier to employ the composite fail-safety principle using multi-constellation SBAS because the safety evidence can be performed on high system level and it is generally much simpler than for reactive systems [13]. It is because the safety evidence of reactive systems shall be performed on individual component level according to the standard EN IEC 61508.

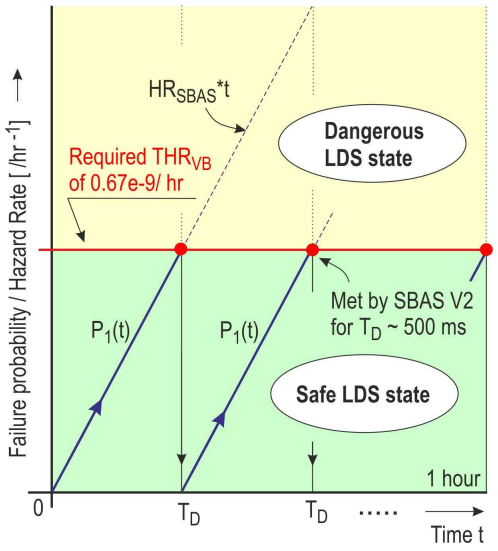

Fig. 7. Probability of virtual balise failure as a function of HR_{SBAS} and T_D.

On the other hand multi-constellation SBAS is more complex than singe-constellation one and its development currently faces different technical problems. Further, SBAS SIS availability can be limited in case of composite fail-safety in the favour of higher safety integrity. The SBAS architecture with composite fail-safety is also not in line with the aviation multi-constellation SBAS concept. The safety integrity of current SBAS is sufficient for LPV-200 operations and it is expected that the main benefit of the multi-constellation/multi-frequency SBAS will consist in the significant availability of integrity improvement for aviation. Therefore, re-evaluation ETCS safety requirements [10], [12] for GNSS SIS (THR_{SIS} of 1e-8/ 1 hour, SIL 4, and CI=14 m) seems desirable. If it were possible to meet the updated THR requirements for GNSS SIS with a single-constellation SBAS, then Galileo and other GNSS constellations within the multi-constellation SBAS might be used for SIS availability improvement – similarly as it is intended for aviation.

The Annex B of the EN50129 standard [9] is related to architectures, techniques and measures to avoid systematic faults and control random and systematic faults to the different Safety Integrity Levels 1-4. The tables in the Annex B describe various techniques and measures against the SILs. However no difference results from the B-tables in the Annex B for SIL 3 and SIL 4. Further, criteria for selection of techniques and measures regarding SW for safety-related systems are contained in the Annex A of the EN50128 standard [8]. Again, no difference results from the A-tables for SWSIL 3 and SWSIL 4. We can say that techniques and measures for the railway safety-related systems for avoidance of systematic faults and control of random and systematic faults are the same for SIL 3 and SIL 4. Thus the only difference between SIL 3 and SIL 4 is at the system level where Tolerable Hazard Rate per hour and function for SIL 4 is lower. The quantitative analysis can only distinguish the compliance of the GNSS based train position determination function with SIL 3 or SIL 4.

In case of SBAS the Design Assurance Level (DAL) is used as a safety measure. SIL 3 corresponds to DAL B (Hazard Rate of 1e-7/ 1 hour) and SIL 4 to DAL A (Hazard Rate of 1e-8/ 1 hour). For example, the EGNOS Central Processing Facility shall be compliant with DAL B. The above relations between SIL 3 and SIL 4 and also relations between SILs and DALs can be used for design of the high-level LDS architecture with reactive fail-safety, but finally detailed SBAS analysis according to railway safety standards will be required in any case.

The following conclusion results from the above analysed LDS fail-safe solutions: while composite fail-safety was mainly used for SBAS safety integrity improvement to meet demanding ETCS safety requirements for the LDS, then reactive fail-safety implemented in the LDS is indented for reduction of ETCS safety requirements for SBAS. The reactive LDS solution based on existing aviation SBAS SoL service is described in more details in sections below.

IV. Tolerable Hazard Rate for Virtual Balise

The ETCS Tolerable Hazard Rate (THR) requirements for virtual balise and GNSS LDS were derived by means of the ETCS Core THR allocation as it is outlined in Fig. 8. The ETCS Core THR of 2e-9/ 1 hour/ train is equally allocated to all ETCS onboard equipment (1e-9/ 1 hour) and all ETCS track-side equipment. Then THR related to Balise Transmission hazard THR_{BTX} of 0.67e-9/ 1 hour was determined [5] - see Fig. 8. THR_{BTX} was further sub-allocated to different track Information Point (IP) failure modes, such as balise deletion ($THR_{BTX\ Deletion}$ < 3.3e-10/ 1 hour), balise

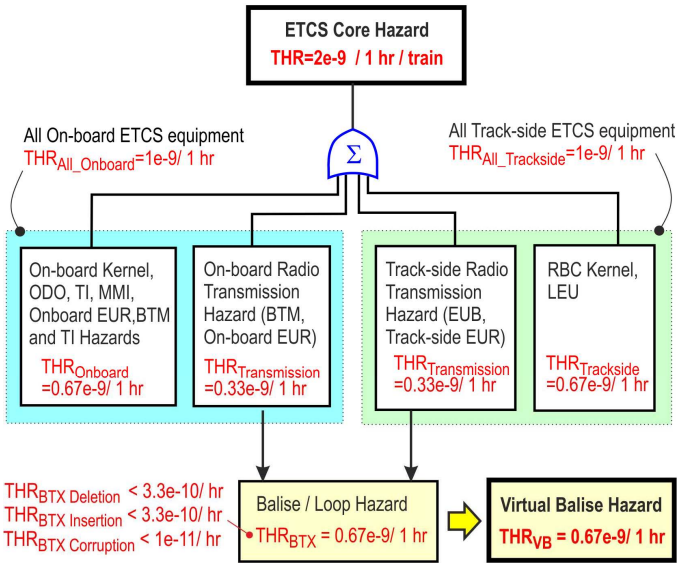

Fig. 8. ETCS Core THR allocation to THR for virtual balise.

insertion ($THR_{BTX\ Insertion}$ < 3.3e-10/ 1 hour), and balise corruption ($THR_{BTX\ Corruption}$ < 1e-11/ 1 hour) [5], [6]. Since GNSS position is determined on board of train, then only two following failure modes for virtual balise were analyzed: virtual balise deletion, and virtual balise insertion [12].

These two VB failure modes can be described as:

- *Virtual Balise Deletion* - means an event, when the VB (i.e. virtual IP) was not determined by means of on-board GNSS LDS. It can happen due to: 1) excessive latent LDS error (wrong position), or 2) absence of train position in the GNSS LDS output. In both cases no VB is detected within the Expectation Window (ExW) provided by the odometry.
- *Virtual Balise Insertion* - means an event when a wrong virtual balise is determined due to wrong GNSS LDS position.

Since both VB failure modes are caused by a wrong GNSS LDS position (i.e. incorrect or no position), and diagnosis for both failure modes is provided by rapid and independent diagnosis in GNSS service volume, then the total THR_{BTX} of 0.67e-9/ 1 hour was taken as THR for virtual balise, i.e. THR_{VB} = 0.67e-9/ 1 hour. THR_{VB} will be further used for derivation of the ETCS THR requirement for GNSS, i.e. THR_{GNSS} (THR_{SBAS}). In next section derivation of THR_{GNSS} for the virtual balise insertion/ deletion is described.

V. Derivation of Tolerable Hazard Rate for GNSS

The classical ETCS requires both track balises and on-board equipment (ONB) for safe train position determination. On the other hand GNSS estimates the position on board of train. Let us assume that λ_{ONB} is the rate of occurrence of ONB being unable to detect a correctly working ETCS Information Point (IP). If linking of IPs is active, then the duration of ONB failure corresponds to the time interval T_L between two successive IPs marked as linked. Further if the average speed of train is v and the linking distance D_L, then the probability of ONB failure causing the IP deletion is

$$P_{f,\,ONB} = \lambda_{ONB} \times T_L = \lambda_{ONB} \times (D_L/v) \qquad (6)$$

There is no safety requirement in respect of not being able to detect an information point when IP linking is active [5]. As lately as two expected consecutive IPs announced by linking are not detected by on-board in the expectation window, measured from the Last Relevant Balise Group (LRBG), the on-board vital computer shall consider the linking command of the second IP as a command to apply the service brake. Then the hazardous failure rate of ONB corresponding to the deletion of any IP met during 1 hour long mission is

$$HR_{ONB} = \lambda_{ONB} \times (2 \times T_L) \times 1\ \text{hour}^{-1} \qquad (7)$$

In order to check the ONB functionality even before the detection of a regular and properly working BG by the ONB, an additional hypothetical "testing" BG can be placed on the track ahead of the regular BG in the direction of movement from the LRBG – see Fig. 9. A much shorter ONB failure duration T_D is achieved in this case. Then (6) can be then modified as

$$P_{f,\,ONB} = \lambda_{ONB} \times T_D \qquad (8)$$

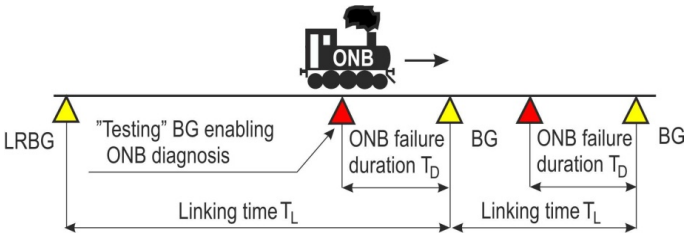

Fig. 9. Diagnosis of ETCS on-board unit using "testing" BGs.

and the corresponding ONB hazardous failure rate per mission (1 hour) is

$$HR_{ONB} = \lambda_{ONB} \times T_D \times 1\ \text{hour}^{-1} \qquad (9)$$

The hazardous ONB failure rate (9) due to IP deletion can be thus reduced with respect to (7) significantly. It is evident that installation of the additional "testing" BGs on a track would be very inefficient. Nevertheless, this reactive fail-safety principle can be easily implemented in case of the GNSS LDS. The "testing" BG is simply replaced by a so-called Travelling Virtual Balise (TVB), as it is depicted in Fig. 10.

The TVB is equivalent to LRBG or LRVB from viewpoint of safety integrity because it is a validated GNSS train position by the independent diagnosis. The TVB arises from the Last Relevant Virtual Balise as a subsequent validated train GNSS position generated just after LRVB is detected and further *travels* to the next virtual balise location in a given direction of movement. The TVB can also originate on a track section between VBs during LDS initialization.

The detection function of the presence of an Information Point (IP) by ETCS on-board unit (ONB) is a critical function and this function is the most critical when IPs are employed in scenarios where linking is not used. It is e.g. during ONB initialization in SR mode or during entry into an ETCS area from unfitted area when wrong IP can be inserted or IP can be deleted. The ETCS THR requirement for GNSS must be derived using these scenarios considering that VB insertion can cause a more dangerous situation than VB deletion.

It is evident that the TVB can be utilized for the LDS diagnosis of the next VB from viewpoint of VB deletion or

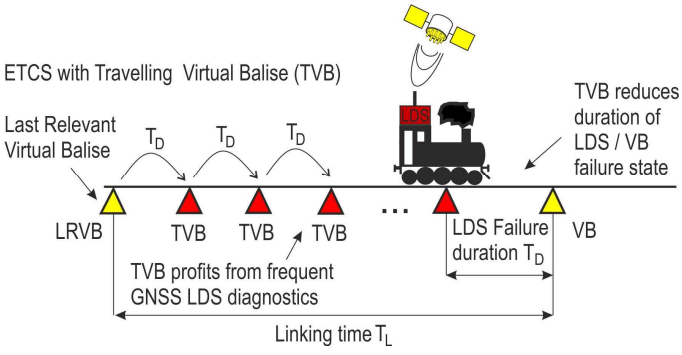

Fig. 10. ETCS LDS concept with reactive-fail safety and justified using Travelling Virtual Balise.

insertion failure modes in the same manner as the hypothetical static "testing" BG is used in Fig. 9. The ETCS THR requirement for GNSS (i.e. THR_{GNSS}) can be determined for the LDS start-up from the THR requirement for VB deletion or insertion per mission, i.e. $THR_{GNSS\ VB}$ of 0.67e-9 $hour^{-1}$, (see Section IV.) as follows

$$0.67\text{e-}9\ hour^{-1} = THR_{GNSS} * T_D * hour^{-1} \qquad (10)$$

where T_D is the duration of GNSS hazardous failure defined as the time interval between the two consecutive linked TVBs or linked TVB and next VB. Let's assume e.g. HR_{GNSS} of 1e-7/ hour which corresponds to the SBAS Integrity Risk requirement for the aviation Non Precision Approach (NPA or En-route). Then according to (10) the acceptable hazard duration T_D due to VB deletion/insertion is

$$T_D = 0.67\text{e-}9/\ 1\text{e-}7 * 1\ hour = 6.7\text{e-}3\ hour = 24.12\ s$$

It should be noted that the allowed Horizontal Alert Limit (HAL) is quite large in this case, i.e. 0.3 nmi (556 m).

The Signal-In-Space (SIS) Integrity Risk (IR) of 2e-7/150 s for Precision Approach (PA) including LPV-200 operations is required in the vertical direction. Excepting this the SIS IR of 1e-9/150 s in the horizontal/ lateral (one dimensional) direction shall be also met for the aviation PA operations. It seems that the integrity (i.e. guarantee) of accuracy in the horizontal plane or in the track direction would be sufficient for signalling in case of the reactive LDS architecture. Nevertheless, three dimensional (3D) track map appears as an effective means for the independent diagnosis of SBAS, and therefore the IR of 2e-7/150 was conservatively selected for signalling. The corresponding SBAS SIS Hazard Rate is approximately 4.8e-6/ 1 hour. Then the allowed duration of SBAS failure can be estimated as

$$T_D = 0.67\text{e-}9/\ 4.8\text{e-}6 * 1\ hour = 1.36\text{e-}4\ hour = 0.50\ s$$

The HAL of 40 m and VAL (Vertical AL) of 35 m is required for LPV-200 operations, where the pilot's decision height is 200 feet (60 m) above the runway. The actual WAAS/ EGNOS accuracies (95%) in horizontal/lateral and vertical directions are typically better than 1.1 m and 1.5 m, respectively. The real SBAS performance in terms of SIS integrity is better than required by aviation. Let's consider the real EGNOS IR for of 6e-8/ 150 s for LPV I operations. Then the corresponding EGNOS SIS Hazard Rate is 1.44e-6/ 1 hour and the acceptable duration of failure T_D of 1.44 s can be according to (10) estimated. If SBAS receiver with an output rate of 10 Hz will be used, then all the above calculated values of T_D are realistic.

VI. SBAS THR Allocation Within LDS

The Tolerable Hazard Rate related to virtual balise failure due to its deletion or insertion, i.e. THR_{VB} of 0.67e-9/ 1 hour, has been taken from the THR_{BTX} requirement for Balise Transmission (BTX) failure for a single physical ETCS information point [5]. The THR_{BTX} has been derived on the basis of the hazard analysis and risk assessment for the ETCS Level 1 and Level 2. The related ETCS core THR allocation to the BTX and GNSS LDS failures is outlined in [5]. The previously derived THR requirement for the GNSS LDS, i.e. $THR_{GNSS\ LDS}$ of 3e-8/ 1 hour has been mainly achieved at the expense of shortening of the spacing between VB to about 200 m for LDS initialization [12]. The linking of GNSS train positions only at VBs locations was considered in that case.

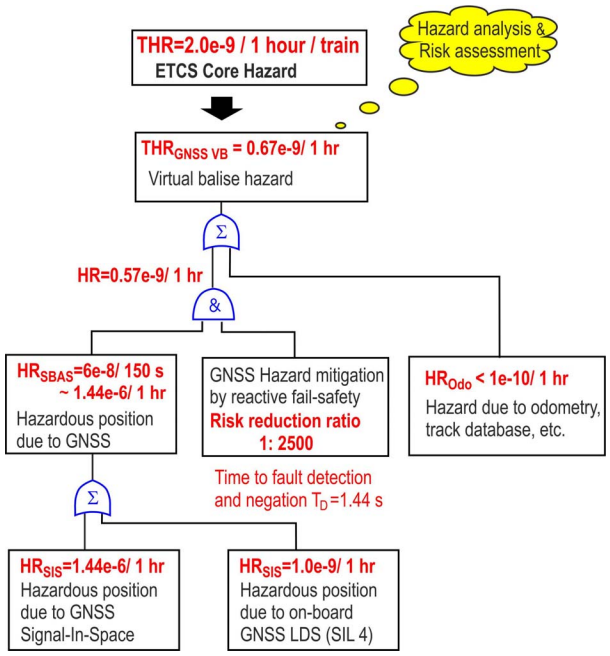

Fig. 11. ETCS core THR apportionment to SBAS SoL service.

The positive effect of the implemented reactive fail-safety technique into the ETCS VB concept on the relaxation of safety requirements for GNSS SoL service is evident from the ETCS core THR apportionment to GNSS SoL service depicted in Fig. 11. Hazard due to wrong GNSS position is mitigated by the risk reduction ratio of 1:2500. This ratio corresponds to the GNSS fault detection and negation time T_D of 1.44 s which was estimated for the EGNOS SIS Hazard Rate of 1.44e-6/ 1 in Section V.

Since the independent diagnosis of GNSS must be also able to detect excessive systematic errors due to local GNSS effects, against which SBAS doesn't protect, then a Tolerable Hazard Rate related to odometry (diagnosis) should be 1e-10/ 1 hour or less. The largest part of the THR_{SBAS} value is allocated to GNSS SIS because the relatively high safety integrity of the on-board GNSS LDS (SIL 4) can be achieved by a multi-channel structure with composite fail-safety.

VII. Travelling Virtual Balise Features And Benefits

The Travelling Virtual Balise (TVB) was introduced into the ETCS virtual balise concept with the intention to justify exploitation of the existing SBAS/EGNOS V2 SoL service for the train LDS to be compliant with SIL 4 at a system level. The TVB supports harmonization of the aviation and railway safety requirements for efficient use of the SBAS SoL service for railway safety-related systems. Further the TVB ensures a

continuity in the ETCS balise concept evolution oriented from the classical ETCS platform with physical balises to more efficient virtual ones stored in the on-board unit and track-side RBC.

The term TVB has been proposed to reflect the analogy between the ETCS (testing) track balise group and the virtual balise intended for fast fault diagnosis of the ETCS on-board unit. The adjective *travelling* means that geo-coordinates of the TVB are not a priori known. The TVB propagates on a track section between two subsequent virtual balises. The abundant GNSS train positions together with the odometry data on a track section between VBs completed with other diagnostic methods, e.g. pseudorange validation using 3D track map (see Section VIII.), etc. are used for the TVB validation for the required safety integrity.

The TVB is the validated train GNSS position that meets the THR requirement for VB deletion or insertion, i.e. THR_{VB} of 0.67e-9/ 1 hour. The diagnosis of both LDS ONB unit and GNSS Signal-In-Space mainly relies on TVB/VB linking. The TVB concept is fully consistent with the reactive fail-safety principle where the main channel (GNSS) itself may not meet safety requirements, but a diagnostic channel (odo+) must detect all dangerous failures so quickly that safety targets are met. This concept has the following features and benefits:

- TVB enables to preserve or even enlarge virtual balise spacing with the respect to the maximum allowed ETCS BG spacing (2500 m) without any impact on the entire LDS safety;
- TVB justifies exploitation of single-constellation EGNOS V2;
- Introduction of the TVB doesn't influence the ETCS safety concept because the TVB is used in on-board unit only;
- Temporal TVB unavailability doesn't influence safety of train position determination because safe ETCS odometry is used for the train position reporting from LRVB when required;
- Additional GNSS constellations (e.g. Galileo) can be used for availability improvement.

VIII. Detection of Errors Due To Local Effects

Reflection of a GNSS signal from surrounding objects or environment along a track (e.g. high-rise buildings, overhead lines, landscape, etc.) causes the signal to reach the GNSS receiver antenna by two or more different paths. It is called the multipath effect and it can cause an excessive error in position of several tens of meters. Multipath belongs to GNSS local effects and thus differential GNSS techniques like SBAS or GBAS are not able to protect against it. This task may be much complicated by a harsh environment as railway is and especially during GNSS LDS initialization, i.e. when the first train position must be determined in stand-still and thus the ETCS odometry cannot be used in this case. To solve the problem of multipath for the ETCS and generally for signalling based on GNSS, a novel method enabling detection

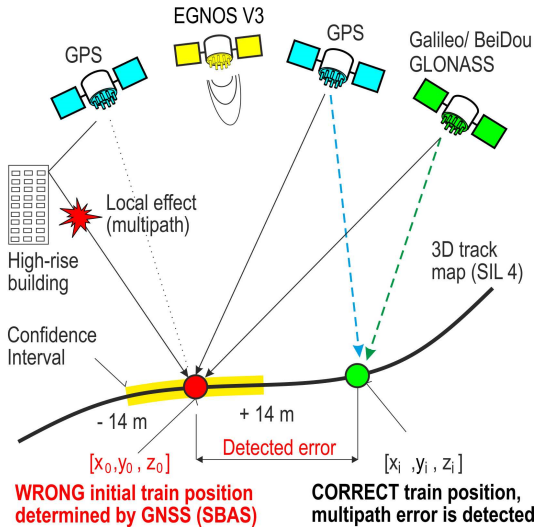

Fig. 12. Detection of multipath Error on multiple pseudoranges using 3D track map.

and identification of an excessive multipath error in train position was developed. The idea of the multipath error detection method is based on the following assumptions:

- Limited magnitude of multipath position error (±100 m is assumed as a sufficient error bound);
- Train trajectory is known - 3D track map (SIL 4) is used;
- At least two pseudorange measurements to two different Space Vehicles (SVs) used in the position solution are not affected by multipath.

The principle of multipath error detection is outlined in Fig. 12. Train position $[x_0, y_0, z_0]$ is determined first using pseudorange measurements to all healthy SVs and also using the EGNOS wide-area differential corrections. Two diverse on-board EGNOS receivers provide the required composite fail-safety. If a multipath error occurs, then it can also influence the receiver clock offset δ_0, which is a part of the train position solution $[x_0, y_0, z_0, \delta_0]$. Then the initial train position $[x_0, y_0, z_0]$ is checked by means of the position $[x_i, y_i, z_i]$ calculated using ranging data for individual satellite (SV) pairs and also by means of 3D track map (SIL 4). It means that all applicable pseudorange measurements to healthy satellite pairs and the corresponding differential corrections provided by EGNOS V3 are used. Since the calculated receiver clock offset δ_0 may be affected by wrong pseudorange measurements, it cannot be used. Instead the train position [x, y, z] is virtually changing on the 3D track map within a given interval (±100 m) around the initial position $[x_0, y_0, z_0]$ for a given satellite pair (e.g. j-th and k-th) as long as the *virtual* receiver clock offsets for these two satellites are equal, i.e. $\delta_i^{\,j} = \delta_i^{\,k}$ (Fig. 12). The position corresponding to the equality of $\delta_i^{\,j} = \delta_i^{\,k}$ is $[x_i, y_i, z_i]$. If at least one of positions $[x_i, y_i, z_i]$ calculated using SV pair(s) significantly differs from the wrong initial position $[x_0, y_0, z_0]$, then the excessive error is detected.

IX. Conclusion

Multi-constellation GNSS with its Safety-of-Life (SoL) services originally developed for aviation represents a strategic infrastructure for safe train position determination as well. It is expected that a train Location Determination System (LDS) based on EGNOS will not only provide a PVT solution with the required safety integrity (SIL 4) for the ERTMS/ETCS Virtual Balise concept, but the EGNOS SoL service has to be also utilised within the ETCS LDS effectively. It has been shown in this paper that the efficiency of multi-constellation EGNOS exploitation directly results from the technical safety principles, which are highly recommended for railway signalling subsystems to be compliant with SIL 3/SIL 4. Due to this reason LDS architectures with composite fail-safety and reactive-fail safety have been compared. While composite fail-safety realised via the EGNOS-R interface was mainly intended for the EGNOS SIS safety integrity improvement to meet demanding ETCS safety requirements for the LDS, then reactive fail-safety implemented in the LDS can be utilised for reduction of the ETCS safety requirements for EGNOS. It has been demonstrated in this paper that the required Tolerable Hazard Rate (THR) for the ETCS virtual balise THR_{VB} of 0.67e-9/ 1 hour can be met using the reactive LDS structure with single-constellation EGNOS V2, although stand-alone EGNOS V2 itself doesn't meet the THR_{VB} at all. The Travelling Virtual Balise has been introduced into the ETCS Virtual Balise concept to demonstrate the LDS compliance with the required THR_{VB}. Galileo as a second constellation within EGNOS V3 can be then used for availability of integrity improvement. Similarly, as it is intended for LPV-200 operations in aviation. It is evident that a very detailed safety analysis of EGNOS and its independent diagnostic channel according to relevant railway safety standards has to be performed.

References

[1] B. J. Sterner, "On the Method of combining GPS and ETCS for Localization Purposes", The European Railway Research Institute (ERRI), Draft of the 8th May 1998, 6 pages.

[2] RTCA DO-229D – "Minimum operational performance standards for GPS WAAS Airborne Equipment", RTCA Inc., Washington, D.C., 2006.

[3] S. Pullen, T. Walter, and P. Enge, "Integrity for Non-Aviation Users. GPS World," July, 2011, pp. 28–36.

[4] A. Neri, S. Sabina, F. Rispoli, and U. Mascia, "GNSS and odometry Fusion for High Integrity and High Availability Train Control Systems," ION GNSS+ 2015, Tampa, September 14-18, 2015, 11 pages.

[5] "ETCS/ERTMS – Class 1, ETCS Application Levels 1 & 2 - Safety Analysis, Part 3 – THR Apportionment," SUBSET-088 Part 3, ISSUE: 2.3.0, DATE: 02-04-2008, 91 pages.

[6] "ETCS/ERTMS Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2", SUBSET-091, ISSUE: 3.3.0, DATE: 2014-05-08, 51 pages.

[7] "EN 50126 Railway Applications: The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS)," CENELEC European standard, 2002.

[8] "EN 50128 Railway Applications: Communications, signalling and processing systems – Software for railway control and protection systems", CENELEC European standard, 2003.

[9] "EN 50129 Railway Applications: Safety related electronic systems for signalling," CENELEC European standard, 2003.

[10] A. Filip and F. Rispoli, "Safety concept of GNSS based train location determination system SIL 4 compliant for ERTMS/ETCS," Proceedings of ENC GNSS 2014, Rotterdam, April 2014, 15 pages.

[11] A. Filip and F. Rispoli, "SIL 4 Compliant Train Location Determination System Based on Dual-Constellation EGNOS-R for ERTMS/ETCS," Proc. of the International Symposium on Certification of GNSS System (CERGAL 2014), Dresden, Germany, July 8 - 9, 2014, pp. 109-114.

[12] A. Filip, "Multi-Constellation Railway SBAS Interface: A Common Platform For Advanced Signalling Compliant With SIL 4 World-Wide," Proceedings of the International Heavy Haul Association 2015 conference (IHHA), Perth, Australia, June 21-24, 2015, 10 pages.

[13] T. Lovric, J. Gülker, "Singe Channel ATP Architectures, a new Trend in Europe?," WCRR 2001, Köln, November 25-29, 2001, 9 pages. http://www.uic.org/cdrom/2001/wcrr2001/pdf/sessions/3_5/040.pdf