D5.4 EGNSS Services Evolution for railways and ETCS impacts

Project acronym:	STARS
Project full title:	Satellite Technology for Advanced Railway Signalling
EC Contract No.:	(H2020) 687414

Version of the document:	07
Protocol code:	STR-WP5-D-TPZ-075-02
Responsible partner:	Thales Alenia Space (TAS-F)
Reviewing status:	Final
Delivery date:	30/11/18
Dissemination level:	PUBLIC

European Global Navigation Satellite Systems Agency

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 687414

CHANGE RECORDS

Version	Date	Changes	Authors
01	30.05.18	First draft	A. Ruggeri (Radiolabs) C. Stallo (Radiolabs) F. Rodriguez (Telespazio)
02	20.09.18	Update based on comments from TAS, CAI, ALS, ASTS, TTS, ZCU and BTSE. Version that integrates the contributions of the Railway Suppliers in sections 5.1 (5.1.1. and 5.1.2), 5.2.8 and 6.1. Preliminary conclusions (chapter 7) shared by ASTS	A. Ruggeri (Radiolabs) C. Stallo (Radiolabs) F. Rodriguez (Telespazio) Railway Suppliers
03	10.10.18	EGNOS description and SBAS integrity details are now in the Annex chapter 3 is reduced accordingly New introduction section in chapter 5 Change of the title of section 5.2 Change of the structure of the section 5.1 with the introduction of the following subsections: 5.3.1 SBAS integrity figures in the aviation domain 5.3.2 SBAS integrity figures in the Rail domain 5.3.3 The GNSS in the Virtual Balise Reader function	A. Ruggeri (Radiolabs) C. Stallo (Radiolabs) F. Rodriguez (Telespazio)
04	19.10.2018	Review of deliverable *D5.4_EGNSS_Services_Evolution_for_railways_and_ETCS_impacts_20180906-4.docx* based on SIE and ASTS comments	B, Brunetti L. Freda Albanese S, Sabina B. Stamm
05	22.10.2018	Integration of all the contributions (TPZ,RALS, ASTS, SIE)	F. Rodriguez (TPZ) A. Ruggeri (RALS) C. Stallo (RALS)
06	20.11.2018	Review and integration of the last comments	TPZ, RALS, ASTS,
07	28/11/2018	Final TMT Revision	AZD
08	30/11/2018	Quality Check	RINA-C BE

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 EXECUTIVE SUMMARY

The aim of the document is to provide an overview of the Evolution of the EGNSS service for the application in the railways environment with a specific reference to the ETCS architecture and operation impacts.

The analysis starts from the definition of the present European SBAS service as conceived for the aviation sector.

The document provides a description of the EGNOS system and EGNOS SoL service provision environment. In particular the Section 3 considers the Architecture, the space segment, the ground segment.

The section 4 described the EGNOS SIS and the messages that are used by a GNSS receiver to compute the augmented PVT.

A specific focus is put on the EGNOS performance specified in the range domain in terms of integrity, accuracy and availability as they are expressed for the aviation application.

The analysis is then focused on the definition of the EGNOS requirements for the rail and tries to spot the main differences between the rail application and the aviation application with reference to the conception of the EGNOS service.

A more specific view of the EGNOS augmentation service for the safety aspects is provided in the section 5.2 where the integrity concept is summarized and the main assumptions listed.

The Application of the SBAS Integrity Concept to the rail domain is analysed comparing the possible architecture in the ETCS system that integrate the GNSS receiver and the advantages and disadvantages of the two solutions are briefly discussed. Some recommendations are also provided to overcome the issues pointed out during the analysis.

On eof the possible solution dedicated to the broadcast of the EGNOS messages in the rail environment is EGNOS EDAS FOR RAIL described in the section 6, where the EDAS-R is defined and analysed with a comparison to the EDAS present service.

2 INTRODUCTION

2.1 PURPOSE AND SCOPE OF THE DOCUMENT

From the assessment of GNSS performances achievable in the railway environment and the target performances requested by ETCS L2/L3 the objective of this document is to identify the deltas between both and propose the possible evolutions that could be implemented on EGNSS and ETCS systems to converge.

2.2 DEFINITIONS AND ACRONYMS

Acronym	Meaning
ABAS	Airborne Based Augmentation System
AFTN	Aeronautical Fix Telecommunication Network
AIP	Aeronautical Information Publication
AIS	Aeronautical Information Service
AL	Alert Limit
AMC	Accepted Means of Compliance
AME	Accuracy Major Event
ANSP	Air Navigation Service Provider
APV	Approach with Vertical guidance
ASQF	Application Specific Qualification Facility
ATPE	Along Track Position Error
ATPL	Along Track Protection Level
C/A	Coarse/Acquisition
CA	Consortium Agreement
CAT	I/II/III Category I/II/III
CCF	Central Control Facility
CDM	Collaborative Decision Making
CEN	European Committee for Standardisation
CFTA	*Chemins de Fer et Transport Automobile*
CNES	Centre National d'Études Spatiales
CN0	Carrier to Noise Density
COTS	Commercial off-the-shelf
CPF	Central Processing Facility
DA/H	Decision Altitude/ Height
DAB	Digital Audio Broadcast
DC	Direct Current
DDoS	Distributed Denial of Service
DOP	Dilution Of Precision
DoS	Denial of Service
DSNA	Direction des Services de la Navigation Aérienne
DVB-T	Digital Video Broadcasting Terrestrial

EASA	European Aviation Safety Agency
EC	European Commission
EC	European Commission
ECAC	European Civil Aviation Conference
EDAS	EGNOS Data Access Service
EDAS-R	EGNOS Data Access Service for Railway
EGNOS	European Geostationary Navigation Overlay Service
EGNOS OS	EGNOS Open Service
EMI	Electromagnetic Interference
ENAIRE	Aeropuertos Españoles y Navegación Aérea
ENT	EGNOS Network Time
ERA	European Union Agency for Railways
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
ESR	EGNOS System Release
ESSP	European Satellite Services Provider
ETCS	European Train Control System
ETRF	EGNOS Terrestrial Reference Frame
ETSO	European Technical Standard Orders
EU	European Union
EVC	European Vital Computer
EWA	EGNOS Working Agreement
EWAN	EGNOS Wide Area Network
FAA	Federal Aviation Administration
FAF	Final Approach Fix
FAS	DB Final Approach Segment Data Block
FDE	Fault Detection and Exclusion
FIR	Flight Information Region
FS	Full Supervision
GA	Grant Agreement
GAGAN	GPS Aided GEO Augmented Navigation
GBAS	Ground Based Augmentation System
GEO	Geostationary Satellite
GIVD	Grid Ionospheric Vertical Delay
GIVE	Grid Ionospheric Vertical Error
GLONASS	Global Navigation Satellite System
GLS	GNSS Landing System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPST	GPS Time

GSA	European GNSS Agency
HAL	Horizontal Alert Limit
HMI	Hazardous Misleading Information
HNSE	Horizontal Navigation System Error
HPE	Horizontal Position Error
HPL	Horizontal Protection Level
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
IERS	International Earth Rotation and Reference Systems Service
IGS	International GNSS Service
IS	Interface Specification
ISRO	Indian Space Research Organisation
IT	Information Technology
ITRF	International Terrestrial Reference Frame
ITU	International Telecommunications Union
LNAV	Lateral NAVigation
LP	Localiser Performance
LPV	Localizer Performance with Vertical guidance
MA	Movement Authority
MCC	Mission Control Centre
MDA/H	Minimum Descent Altitude/ Height
MI	Misleading Information
MOPS	Minimum Operational Performance Standards
MT	Message Type
NLES	Navigation Land Earth Stations
NLOS	Non Line of Sight
NOTAM	Notice To AirMen
NMA	Navigation Message Authentication.
NSA	National Safety Authorities
OS	Open Service
PACF	Performance Assessment and Checkout Facility
PMO	Project Management Office
PR	Pseudo Range
QM	Quality Manager
RBC	Radio Block Centre
RHCP	Right Hand Circular Polarized
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SARPs	Standards and Recommended Practices
SBAS	Satellite-Based Augmentation System

SDCM	System for Differential Corrections and Monitoring
SDR	Software Defined Radio
SES	Single European Sky
SIS	Signal in Space
SNR	Signal to Noise Ratio
SoL	Safety of Life
SoM	Start of Mission
SR	Staff Responsible
SREW	Satellite Residual Error for the Worst User Location
UDRE	User Differential Range Error
UIVD	User Ionospheric Vertical Delay
US	United States
UTO	Unattended Train Operation
THR	Tolerable Hazard Rate
WAAS	Wide Area Augmentation System
WP	Work Package

3 DESCRIPTION OF THE EGNOS SERVICE AND EGNOS SOL SERVICE PROVISION ENVIRONMENT

This section and the next presents the characteristics of the service offered to users by EGNOS Safety of Life (SoL) Service, as stated in [23], highlighting the positioning performance currently available to suitably equipped users using the EGNOS SoL augmentation signals.

3.1 EGNOS: THE EUROPEAN SBAS

The European Geostationary Navigation Overlay Service (EGNOS) provides an augmentation signal to the GPS standard positioning service. The EGNOS signal is transmitted on the same signal frequency band and modulation as the GPS L1 (1575.42MHz) C/A civilian signal function. While the GPS consists of positioning and timing signals generated from spacecraft orbiting the Earth, thus providing a global service, EGNOS provides correction and integrity information intended to improve positioning navigation services over Europe.

EGNOS is part of a developing multi-modal inter-regional SBAS service, able to support a wide spectrum of applications in many different user communities, such as aviation, maritime, rail, road, agriculture. Similar SBAS systems, designed according to the same standard (i.e. SARPs), have already been commissioned by the US (Wide Area Augmentation System – WAAS) and Japan (MTSAT Satellite based Augmentation System – MSAS). Analogous systems are under commissioning or deployment in other regions of the world (e.g. GPS Aided GEO Augmented Navigation – GAGAN in India and System of Differential Correction and Monitoring – SDCM in Russia).

3.1.1 Space segment

The EGNOS space segment consists of navigation transponders onboard geostationary satellites broadcasting corrections and integrity information for GPS satellites and the L1 frequency band (1575.42 MHz).

3.1.2 Ground segment

The EGNOS ground segment is mainly composed of a network of ranging integrity monitoring stations, four mission control centres, six navigation land Earth stations and the EGNOS wide-area network, which provides the communication network for all the components of the ground segment. Two additional facilities, the performance assessment and system checkout facility and the application specific qualification facility, are also deployed as part of the ground segment to support system operations and service provision.

The European Satellite Services Provider (ESSP) SAS is the EGNOS Services Provider within Europe, certified according to the SES regulation as Air Navigation Service Provider (ANSP). ESSP SAS provides the EGNOS Open Service (OS), Safety of Life (SoL) Service compliant with ICAO (International Civil Aviation Organization) Standards and Recommended Practices throughout the European Civil Aviation Conference (ECAC) region. And additional EGNOS Data Access service (EDAS) is also provided. ESSP SAS as EGNOS service provider also generates EGNOS Notice To Airmen (NOTAM) proposals to the appropriate Aeronautical Information Service providers within Europe that should validate and distribute the final Official EGNOS NOTAM.

About the EGNOS SoL minimum performance characteristics, these are described in term of accuracy, integrity, availability and continuity (Table 1) [23]. This minimum performance is conservative since it has been derived to take account of a number of degraded conditions or abnormal environmental conditions that could be experienced throughout the lifetime of the system.

	Accuracy		Integrity		Continuity	Availability
	Horizontal Accuracy 95%	Vertical Accuracy 95%	Integrity	Time-To-Alert (TTA)		
Performance	3 m	4 m	For NPA service level: $1 - 1x10^{-7}$/h For APV-I and LPV-200 service levels: $1 - 2x10^{-7}$/ approach	Less than 6 seconds	For NPA service level: $<1 - 1x10^{-3}$ per hour in most of ECAC $<1 - 2.5x10^{-3}$ per hour in other areas of ECAC For APV-I and LPV-200 service levels: $<1 - 1x10^{-4}$ per 15 seconds in the core ECAC $1 - 5x10^{-4}$ per 15 seconds in most ECAC $1 - 1x10^{-3}$ per 15 seconds in other areas of ECAC	0.999 for NPA service level in all the ECAC 0.99 for APV-I and LPV-200 service levels in most ECAC

Table 1. EGNOS SoL Service performance values [23]

where the Time To Alert (TTA) is the maximum allowable time elapsed from the onset of the navigation system being out of tolerance until the user equipment enunciates the alert and the availability, in the LPV-200, the most demanding scenario among the EGNOS SoL Service levels, is showed in Figure 3-1 [23].

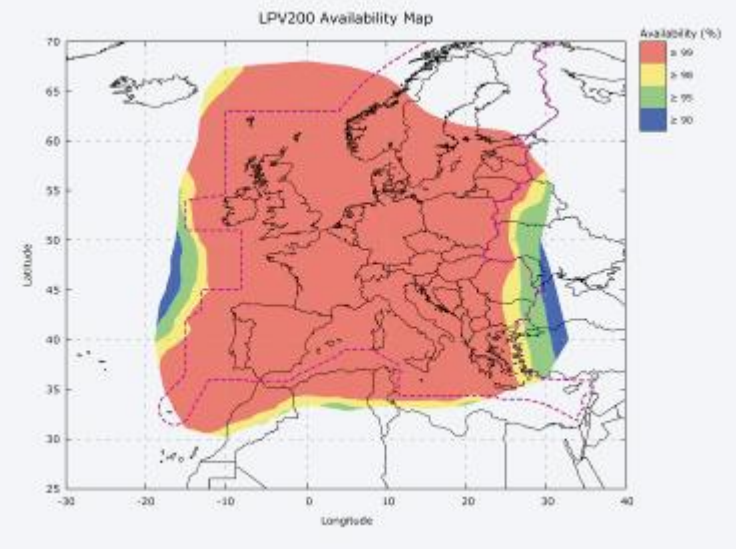

Figure 3-1. EGNOS LPV-200 availability

In the Annex (ref. Section 8) a summary of the EGNOS architecture is provided.

3.2 TIMING SERVICE

In order to support timing applications, the EGNOS system transmits specific corrections that make it possible to trace “EGNOS Network Time” to the physical realization of UTC by the Observatoire de Paris.

4 EGNOS SIS

4.1 EGNOS SIS INTERFACE CHARACTERISTICS

"The *EGNOS Signal In Space* format is compliant with the ICAO SARPs for SBAS. This section provides an overview of the EGNOS SIS interface characteristics, related to carrier and modulation radio frequency and structure, protocol and content of the EGNOS message", as stated in [23].

4.1.1 EGNOS SIS RF Characteristics

"The EGNOS GEO satellites transmit right-hand circularly polarised (RHCP) signals in the L band at 1575.42 MHz (L1). The broadcast signal is BPSK modulated by a combination of a 1023-bit PRN navigation code of the GPS family and a 250 bits per second navigation data message carrying the corrections and integrity data elaborated by the EGNOS ground segment.

The EGNOS SIS is such that, at all unobstructed locations near ground level from which the satellite is observed at an elevation angle of 5 degrees or higher, the level of the received RF signal at the output of a 3dBi linearly polarised antenna is within the range of –161dBW to –153dBW for all antenna orientations orthogonal to the direction of propagation [23].

4.1.2 EGNOS SIS Message Characteristics

"The EGNOS SIS Navigation Data is composed of a number of different MT as defined in the SBAS standard (See Table 4-1 of [23]). The format and detailed information on the content of the listed MTs and their use at SBAS receiver level are given in ICAO SARPs [15] and RTCA SBAS MOPS [20] [23].

4.2 EGNOS SIS PERFORMANCE IN THE RANGE DOMAIN

4.2.1 Accuracy in the Range Domain

"This section focuses on the EGNOS SIS accuracy performances in the range domain. Accuracy in the range domain is defined as the statistical difference between the range measurement made by the user and theoretical distance between the true satellite position and the true user position. The EGNOS system has been qualified using conservative models that take into account the detailed behaviour of the EGNOS system under a number of operating conditions.

The accuracy performance at range level is mainly characterised by two parameters, representing respectively the performance of the time and orbit determination process, and the ionospheric modelling process:

- The Satellite Residual Error for the Worst User Location (SREW) in the EGNOS service area, representing the residual range error due to the ephemeris and clock errors once EGNOS corrections are applied.
- The Grid Ionospheric Vertical Delay (GIVD) which represents the residual vertical range error due to ionospheric delay after applying the EGNOS ionospheric correction at each of the grid points predefined in the MOPS [20]. The ionospheric vertical delay relevant for a given user/satellite pair is the delay at the geographical point where the satellite signal crosses the ionospheric layer. This is called the User Ionospheric Vertical Delay (UIVD) and it is computed by interpolation of GIVDs of the neighbouring grid points. Finally the slant ionospheric delay is obtained from this UIVD by applying the equations defined in MOPS [20] and SARPs [15]."

Other minor error sources are:

- Troposphere (vertical);
- GPS receiver noise;

- Local effects (e.g. multipath).

Table 2 provides the comparison of the pseudorange error budget when using the EGNOS OS and GPS standalone to correct for clock, ephemeris and ionospheric errors.

Error sources (1σ)	GPS - Error Size (m)	EGNOS - Error Size (m)
GPS SREW	4.0 (see note 1)	2.3
Ionosphere (UIVD error)	2.0 to 5.0 (see note 2)	0.5
Troposphere (vertical)	*0.1*	*0.1*
GPS Receiver noise	*0.5*	*0.5*
GPS Multipath (45º elevation)	*0.2*	*0.2*
GPS UERE 5º elevation	7.4 to 15.6	4.2 (after EGNOS corrections)
GPS UERE 90º elevation	4.5 to 6.4	2.4 (after EGNOS corrections)

Table 2. Typical EGNOS and GPS stand-alone SIS UERE[1]

4.2.2 Integrity in the Range Domain

"As the SREW and GIVD range accuracy parameters cannot be monitored in real time, the EGNOS system provides an estimation of the statistical distribution (i.e. standard deviation) which bounds the real SREW and GIVD. The two integrity parameters provided by EGNOS are the User Differential Range Error (UDRE) and the Grid Ionospheric Vertical Error (GIVE). The UDRE characterises the SREW parameter while the GIVE characterises the GIVD.

For the integrity in the range domain, the range error is bounded by a threshold based on the UDRE and GIVE parameters. For each pseudorange, the range error shall be less than 5.33 times the estimated standard deviation ($\varepsilon \leq 5.33\sigma$ where ε is Range error and σ is the computed SBAS Range error estimate standard deviation).

The metrics used for analysis in the range domain aim at demonstrating that the UDRE and the GIVE parameters bound respectively the pseudo-range errors at the Worst User Location (SREW) and the Grid Ionospheric vertical delay (GIVD). In other words, in order for UDRE and GIVE to bound properly the true range error in the measurements, it should be ensured that 5.33xUDRE > SREW and 5.33xGIVE > GIVD with the adequate level of probability[2].

[1] User Equivalent Range Error (UERE). The UERE is an estimate of the uncertainty affecting the range measurements for a given satellite. When trying to characterise the overall range measurement errors, all error sources described above are aggregated and a unique parameter is used (UERE).

[2] Regarding the bounding requirement of UDRE and GIVE, the 5.33 relates to the level of confidence > $1 - 10^{-7}$ / 150 seconds, where: Normal CDF^{-1} $(1 - 10^{-7}/2) = 5.33$;
In practice, these estimates are computed as 3-sigma UDRE and GIVE values by EGNOS. Transformation of these into 5-sigma values (i.e. bounding of residual errors with a $1 - 10^{-7}$ probability) requires multiplication by a K-factor of 1.62. The K-factor is determined as follows:
Normal CDF^{-1} $(1 - 10^{-7}/2) = 5.33$; Normal CDF^{-1} (1-10-3/2) = 3.29; K-factor = 5.33 /3.29 = 1.62.

EGNOS is designed in such a way that the SoL service ensures that the satellite correction error and Ionospheric error are bounded with a probability of 99.99999%." ([23], §4.3.1).

When a satellite failure occurs, the ground segment will provide the appropriate corrections along with the parameters allowing XPL calculation, unless the error gets too large in which case the faulty satellite is flagged with a "don't use" status. When the error is not significantly large, the user equipment will process these data and the only impact will be on system availability and continuity through XPL inflation at user level. In EGNOS system, specific modulation distortion failures (evil waveforms) are also managed through Signal Quality Monitoring (SQM) defined in ICAO Amendment 77 using specific Reference and Integrity Monitoring Stations type C (RIMS C) [31].

4.2.3 Availability

As described in [8], the EGNOS service availability is not optimal along railway lines, mainly due to the fact that EGNOS satellites are geostationary.

The tests performed in the LOCOPROL project[3], considering over 3000km of rail route in Italy, showed an overall measured availability of 66% for accuracy enhancement. LOCOPROL also simulates EGNOS availability on other tracks along the CFTA[4] railway mountainous line between Nice and Digne in the south of France. Because of the very quick changes of the environment around the antenna, EGNOS state of reception can vary very quickly also. Simulation results showed that 60% of the reception durations were shorter than 10 seconds and 40% shorter than 5 seconds, this limited signal availability prevents the receiver from applying the integrity information. Nevertheless, some long areas of reception are observed. The longest one has a duration of 275 seconds, which enables the receiver to benefit at least from corrections for positional accuracy.

In the RUNE project[5], the EGNOS-based solutions along the line between Torino and Chivasso (and return) showed availability of around 45% of time.

Even if in the road environment, where the reception conditions can be very close from railway ones, has been demonstrated that EGNOS was received 84% of the time along the highway against around 10% in the urban context [14]. The rail and road environments show the same conditions since they are generally not far between each others as the case of Italy where 10,000 km of rails and roads are distant less than 1 km [26].

Despite all availability limitations, depending on the use of EGNOS in railway domain, the actual availability percentage can be an issue for safety applications because global anomalies as faulty satellites, if any, are not detected during this time of EGNOS signal unavailability.

An alternative of the use of the EGNOS signal is the broadcast of the EGNOS information via terrestrial transmitters or via internet as proposed by the EDAS service.

4.2.4 Cyber Security Threats

Space-based systems play an important role within national critical infrastructures. They are being integrated into advanced air-traffic management applications, rail signalling systems, energy distribution software etc. The following pages focus on concerns associated with potential cyber-attacks. These are important because future attacks may invalidate many of the safety assumptions that support the provision of critical space-based services. These safety assumptions are based on standard forms of hazard analysis that ignore cyber-security considerations This is a significant

[3] https://cordis.europa.eu/project/rcn/60945_en.html

[4] *Chemins de Fer et Transport Automobile (CFTA)* was a French transport company which operated thousands of kilometres of local railways (mostly narrow gauge) in France in the late 19th century through to the 1930s. CFTA became a part of the Veolia Transport as part of the Veolia Cargo division of the company. In 2009 Veolia Cargo was acquired by SNCF and Eurotunnel.

[5] http://www.esa.int/Our_Activities/Navigation/Railway_User_Navigation_Equipment_RUNE2

limitation when, for instance, security attacks can simultaneously exploit multiple vulnerabilities in a manner that would never occur without a deliberate enemy seeking to damage space based systems and ground infrastructures.

The mass transport scenario is even more vulnerable to cyber-attacks due to the predefined mobility pattern and the number of persons involved.

4.2.4.1 VULNERABILITIES

Most of the design and the development of GNSS infrastructures have focused on safety rather than security requirements. The existing infrastructures remain vulnerable to a range of attacks. An early warning was provided by an approach into New Jersey during December 1997. The crew of a Continental trans-Atlantic flight lost all GPS signals; jeopardizing confidence in on-board systems. It was initially believed that this had been caused by an intentional jamming attack. It later turned out to have been the unintended result of a US military test. A 200-kilometer “interference zone” was created by a GPS antenna with a 5-watt signal, stepping through frequencies.

The UK Ministry of Defence (MOD) illustrated the potential threat for maritime navigation [25].A medium powered jamming device generated noise over a pre-defined area of the UK coastline. This study clearly illustrated the impact that the threats to GNSS integrity can have upon the end users of these infrastructures. Particular problems were identified for crews using integrated bridge systems. This technology brings together navigation tools with autopilot control so that a jammed GPS signal could lead to a significant deviation without warning. Even if an alert was issue, it can still be difficult to determine the vessel’s correct position given a consequent loss of situation awareness. The crews in this trial were all aware that the GPS signals would be jammed. However, multiple simultaneous alarms rapidly increased their workload as the crew crosschecked navigational information. The consequences for on-board systems were compounded by the impact of jamming for shore-based systems. Numerous errors began to undermine the Vessel Traffic Services that provide an overview of coastal areas. Some of the data returned by vessels was based on incorrect GPS fixes that contradicted radar sources.

Many of the vulnerabilities associated with conventional GNSS architectures stem from the relatively weak signals that are used. A common analogy is to compare GPS output to using the power of a car headlight across one third of the Earth’s surface at more than 20,000km. Most western military organizations can interrupt GNSS signals; simulation software enables planners to identify the optimal allocation and distribution of jamming systems. The military development of satellite navigation jamming devices has been mirrored by the increasing availability of hand held systems that cost little more than $100 and have a range of several kilometres. These portable technologies can be used in a range of criminal activities – for instance, to disrupt the signals to GPS tracking devices that would otherwise report the location of a stolen vehicle or shipment.

Some of these concerns are being addressed through technological innovation. For instance, spoofing will become far more difficult once Galileo begins to provide encrypted signals for use in safety-related applications. Other threats continue to affect future GNSS architectures. The design of the EGNOS and Galileo ground based systems focused on a series of ‘feared events’ and failure modes. Algorithmic barriers and standard operating practices, including maintenance procedures, were then created to address these concerns.

4.2.4.2 A TAXONOMY

In this section, we focus on the GNSS service provision for the signalling system in the European Rail Traffic Management System (ERTMS), the standard for signalling and management systems in Europe. We provide an analysis of the potential vulnerabilities in current deployments. Our contribution focuses on a cyber-security analysis of the current system, taking into consideration new risks that have emerged over the past two decades. A range of organisations across Europe and North America are concerned about the vulnerability of new space-based, critical infrastructures.

Security attacks may invalidate many of the safety assumptions that are based on the analysis of system failures rather than security concerns.

Cyber security has been defined as a casualty of the transition from closed to open systems. In the industrial domain, migration from closed legacy systems to public data service provider has clearly introduced an enhancement in performance and resilience. However, such strategy also introduces a new challenge that requires protection from current cyber security threats.

This section provides a taxonomy of cyber security attacks in the general IT domain. These cyber-attacks can be classified according to their interaction with the target, their goal, and the methodology used during the attack.

Extra challenging are IT scenarios that deal with critical and vital services, such as vehicular and guided transportation scenarios. Services such as vehicular platoons, UTO, virtually coupled train sets, and the signalling system itself clearly depend on the security and reliability of the underlying architecture.

4.2.4.2.1 Passive Attacks

These types of attacks do not require any interaction with the target or the network under attack. Usually, they are difficult to detect, and their aim is to collect information for future, more complex, attacks.

Eavesdropping: This is the most common type of passive attack and is performed by capturing packets traveling along the network. This attack can be performed in both wireless networks and wired networks that are not correctly segmented.

4.2.4.2.2 Active Attacks

Unlike passive attacks, these attacks interact directly with the target or the network in order to cause intentional malfunctioning. These attacks are therefore more easily detected but also more dangerous.

Denial of service (DoS) attacks: As their name indicates, the goal of these attacks is to put the target out of service, usually by making the target work beyond its capabilities. Depending on how the attack is performed, DoS attacks can be classified into different groups. They can be categorized into physical and logical attacks, but they can also be defined according to the origin of the attack (i.e., whether the attack has one or multiple sources).

- Physical attacks (jamming): Jamming attacks do not require any logic or knowledge of the target and/or its network. The attack occurs when physical conditions that are able to interrupt communication are introduced into the network. For example, high-power electromagnetic emissions can abruptly reduce the signal-to-noise ratio (SNR) in the target's receptor.
- Logical attacks: The execution of these attacks requires exhaustive knowledge of the target's system, or of the network topology where it is located. Usually, these attacks — also called replay attacks — are based on the attacker copying valid packets of the service provided by the target and inserting these extra copies into the network. This action causes a data overflow in the target.
- Distributed attacks: When a DoS attack has more than a single source it is called distributed DoS (DDoS). DDoS attacks can be identical to regular DoS attacks, but by carrying out the attack from different sources, the probability of success increases considerably. Moreover, as there are multiple sources, it is more difficult for the target to recover from the attack.

Identity theft or spoofing attacks: These attacks permit the injection of packets into an unauthorized network by adopting the identity of an entity that is authorized by the network. When this identity theft is performed in both communication directions, it is called a "man-in-the-middle" attack; that is, attacker C alters communication between entities A and B by communicating with A as if it were B, and at the same time communicating with B as if it were A.

Equipment infection: The exploitation of known or unknown system vulnerabilities using viruses has become a common and effective means of cyber war. Cases such as StuxNet have demonstrated that incorrectly isolated industrial equipment can become a target. It is difficult to protect industrial equipment against these attacks for two main reasons. First, it is difficult to update such equipment in cases where the elements are geographically dispersed or are based on embedded systems. Second, protective software, such as antivirus software, has a negative effect on real-time performance.

4.2.4.2.3 Taxonomy of Intentional Attack Scenarios on GNSS on board of train

This paragraph briefly summarizes the considered attack scenarios. The taxonomy is based on the following drivers:

- Type of Attack
  - Jamming: the attacker that might be either on board or outside the train uses a jammer to block the GNSS signal acquisition/tracking;
  - Spoofing: the attacker, which might be either on board or outside the train, uses a GNSS signal simulator to generate a falsified signal.
  - Meaconing: the attacker, which might be either on board or outside the train, transmits a deception signal with high power. The transmitted signal is simply a rebroadcast of a previously recorded GNSS signal. Two main types are considered, depending on the equipment used to mount the attack:
    - Direct meaconing: This meaconing event involves the use of direct means to delay and rebroadcast GNSS RF signals (e.g. use of a drum of cable in conjunction with COTS GNSS rebroadcasting products, with a cost below €100). In a few words, it involves reception, amplification and re-broadcast (e.g. with GPS re-broadcaster) of the GNSS signal.
    - Network meaconing: This spoofing event involves the use of equipment to record and replay GNSS RF signals, where one node at a specific location (e.g. at the other end of the train or on another train) digitizes the signals, packetizes RF samples and transmits them over a network to the other node, which receives and replays the RF signal in order to position the target at the specific location. The network meaconing involves digitization of RF signal, communication over a network and upconversion/regeneration of RF at the other end, giving the attacker more degrees of freedom. (Probably record and replay threat can also be considered as a type of meaconing).
- Attacker Position (see Figure 4-1):
  - On-Board: the attacker is on-board, hence is still with respect to the victim, and experiences similar channel impairments.
  - External: The attacker is positioned external to the train, being stationary or moving. In any case, it has to estimate the relative dynamics and to compensate it to mount sophisticated attacks (i.e. spoofing)
  - Indirect: The attacker is targeting another victim that is not the train itself. Due to radio-propagation, the train GNSS antenna may capture some signal.
- Target asset (optional, for jamming it is not applicable since the un-availability degrades all the assets):

- Time: the attack aims at forging time. The attacker, which might be either on board or outside the train, transmits a deception signal consistent with the train dynamics. The attacker attempts to cheat the victim countermeasures by transmitting a signal the slowly changes the time solution.
- Trajectory: attack aims at forging the trajectory, by transmitting a falsified signal consistent with the train trajectory. After an alignment phase, the trajectory is drifted.
- Channel: the attack aims at forging certain channels, by adding channels not in view or forging channels in view.

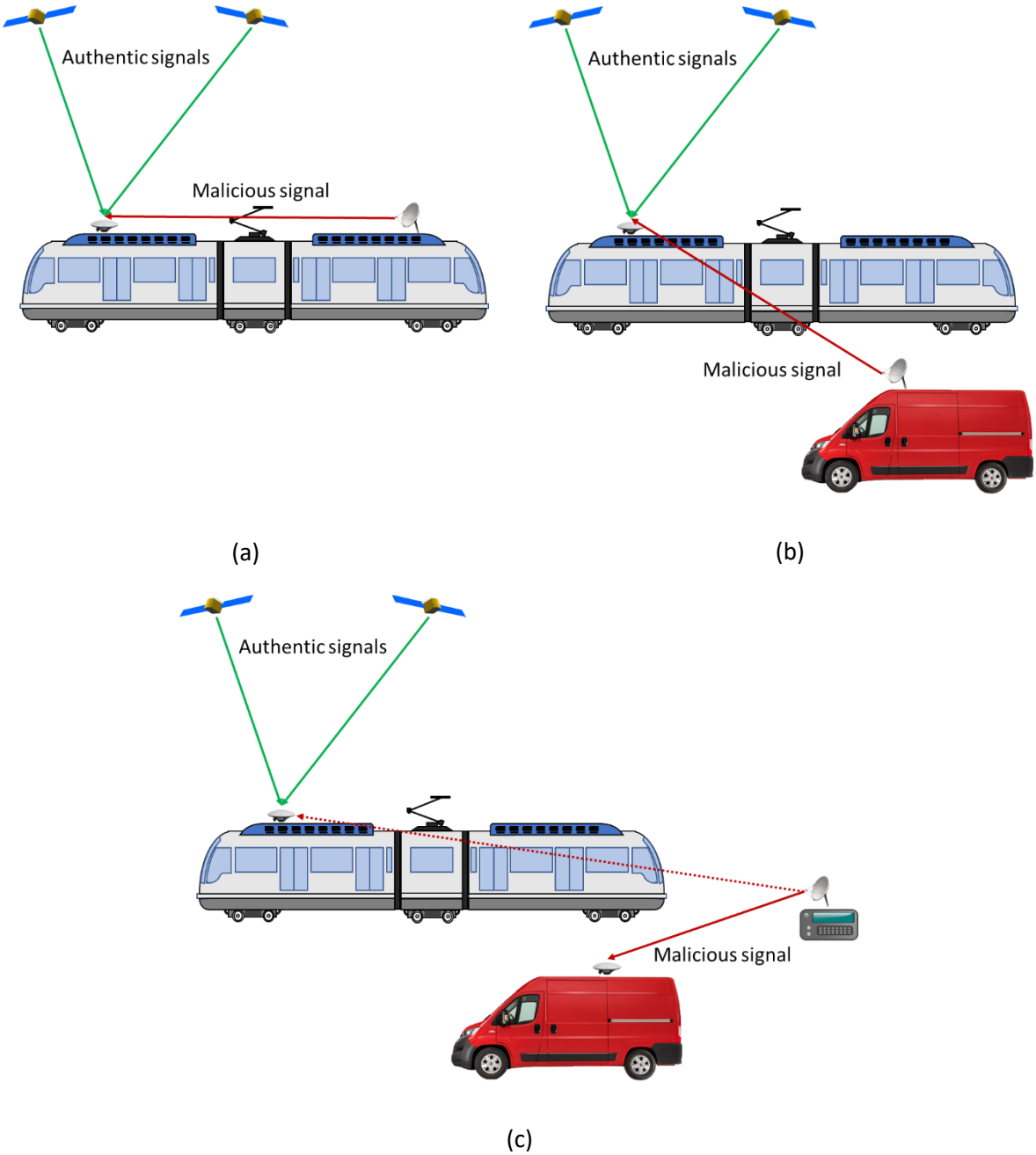

Figure 4-1: Attacker position: (a) Onboard, (b) External, (c) Indirect

4.2.4.3 EGNOS LIMITATIONS IN RAILWAY ENVIRONMENT

Both un-intentional and intentional interferences can occur in the railway environment. On-board EMI can be induced by interference from electric supply systems to the train, e.g. DC-DC converters or due to effect of arcing of the pantograph with the contact wire.

Unintentional EMI within and external to rail corridor can be due to electromagnetic wave broadcasting stations, in particular, DVB-T signals which are considered the most important source of unintentional interference in the GNSS frequency bands. It can also be due to radar signals, nearby transmitters, harmonics of other ground and airborne transmitters.

Intentional EMI within and external to rail corridor can be due to jamming devices, spoofing, and meaconing malicious attacks that can be easily carried out due to the availability on the market of cheap COTS GNSS jamming equipment, SDR and COTS GNSS rebroadcasting products, as widely described in 4.2.4.2.3.

EGNOS SoL, as currently is, not robust to local threats as jamming or more malicious spoofing attacks and does not provide authentication signal service [3].

These two phenomena can have a different impact on the GNSS performance in the rail context. Jamming can affect the availability of the system since it can significantly increase the error position. If Horizontal Protection Level (HPL) is higher than a selected Alarm Limit (AL) (its value depends from the considered railway operational scenario [5]), the estimated train positioning for the epochs affected by this phenomena is not available. Jamming in particular increases C/N0 degradation and Pseudorange Noise (PR). If PR is not bounded, possible Hazardous Misleading Information *ATPE* > *ATPL* could occur.

Spoofing can affect the safety of the system, since it is more malicious creating fake GNSS signals and forcing the on board unit on the train to use these replicas for estimating the train positioning.

Existing networks used for the broadcast of GNSS augmentation data such as EDAS (EGNOS data access service) could be potentially ideal candidates for the transmission of EGNOS corrections and integrity data [4] in order to overcome this significant issue.

In fact, these corrections can be transmitted from EDAS to ERTMS/ETCS control centre encapsulated in an EURORADIO like protocol over a ground network link, ensuring the needed security level (secure and authenticated communications) [4], by avoiding to use directly EGNOS SoL service, that is instead vulnerable to GNSS intentional attacks.

In the future evolution of EGNOS V3 (multi-constellation and multi-frequency), it will augment Galileo that will improve the communication system by providing encrypted signals through GNSS Navigation Message Authentication (NMA) using the Galileo Open Service signals. The proposed NMA scheme will be based on the TESLA protocol [27].

5 EGNOS SoL SERVICE PERFORMANCE FOR RAIL

5.1 INTRODUCTION

In this section the introduction in the railways signalling of GNSS and in particular of EGNOS is analysed.

The assumption is that the reference signaling system for this analysis is the ETCS since it is mandated in Europe for the next decade(s)

Moreover the application of GNSS with ETCS is limited to ETCS Level 2/3 through the Virtual Balise concept; an application with ETCS Level 1 is not considered, as Level 1 requires balises for data transmission which reduces the benefits of GNSS to a minimum.

For ETCS applications safety integrity level 4 (SIL 4) is currently required. While this does not necessarily mean that the GNSS/EGNSS system itself needs to be SIL 4 compliant, the overall application shall still maintain that safety level when using GNSS.

Therefore EGNOS, or an adequate replacement, will be required for safety reasons, as it is currently the only means to detect malfunctioning in the GPS constellation

So the analysis covers initially aspects that are specific to the railway application and differences with the aviation will be pointed out. It includes the “EGNOS services definition for railway” in terms of performances requirements on accuracy and integrity (alarm limit, time to alarm, integrity level) as requested.

As a second step the analysis is focused on the convergence between ERTMS architecture and SBAS services, operational impacts and some recommendations on the implementation of the architecture to take into account some limitation intrinsic in the GNSS service (like sky visibility, RF propagation, fading, interference etc.).

5.2 REQUIREMENTS ON EGNOS SoL SERVICE FOR RAIL APPLICATIONS

5.2.1 Assumptions

EGNOS was defined for aviation applications. The requirements on EGNOS resulted from gap between aviation navigation performance requirements (“the aviation application”) and the performance delivered by GPS. Performance is understood as positioning accuracy, availability (including continuity) and safety.

EGNOS for aviation therefore closes the gap between GPS performance and the aviation application. For railway applications the situation is fundamentally different for a number of reasons:

- The railway application is much more complex, as it not only includes many more operational situations (characterized by different ETCS modes), but railway also operate in a much more complex and diverse environment
- The railway application performance requirements are ensured by ETCS and the underlying signalling system, which currently use balises and odometry as “navigation” system.

EGNOS plus GPS are therefore not considered as a complete solution to fulfil the railway “navigation” requirements, but as an input into ETCS, which shall continue to fulfil these requirements even when physical balises are not being used. EGNOS for railway applications does not alone close the gap between GPS performance and the rail application, it only does this as an element of a more complex solution.

It is also assumed that EGNOS cannot be fundamentally changed for railway applications. This document therefore only covers requirements on EGNOS which can be implemented realistically ("EGNOS Rail Service").

It is assumed that additional measures are implemented in ETCS to close the gap between GPS/EGNOS + EGNOS Rail Service and the railway application.

The balance between requirements on an EGNOS Rail Service and requirements on additional measures in ETCS will be decided by what can be realistically included in an EGNOS Rail Service.

5.2.2 From Railway Application Perspective

The basic assumption for this analysis has been that the GNSS signal is used to apply the Virtual Balise concept. This is performed by the virtual balise reader (VBR) function (whose main subfunction is the Virtual balise detection), which detects virtual balises in the correct sequence using GNSS and pre-known absolute virtual balise positions.

When introducing GNSS in ETCS it must be ensured that the performances required from the overall ETCS system are maintained, in terms of ground and on-board sub-systems. In particular, it is necessary to confirm that the system/sub-system/equipment meets its THR target measure in the event of systematic and random fault to ensure the principle of fail-safe operation [35].

The intent of this section is to provide the rationale behind the performance-related concepts which are commonly used in aviation and require a different interpretation and formalization in the railway case.

By using the data collected and analyzed in the frame of STARS, the contextualization of these parameters prepares a valid basis for both their qualitative and qualitative analysis to be conducted in the future. A preliminary rating focused on the main performances required for GNSS-based train positioning is proposed in D5.3 (see Table 2 in [36]). A complete set of performance will be provided in the context of the S2R TD 2.4 Fail-Safe Positioning project.

5.2.2.1 CONTINUITY VERSUS AVAILABILITY

Availability is expressed by percentage of time during which the GNSS-based positioning function is usable for intended purpose, meaning that this information (estimated inside Virtual Balise Reader) is provided in sufficient quality.

In aviation domain the availability is evaluated within the specified coverage area. For railway domain, this approach has to be modified in that sense, that the coverage area is further restricted when the availability is evaluated. First, only railway lines within the specified coverage area are considered. Further, on these lines, segments where local conditions fulfil certain quality from GNSS reception perspective are used as areas where availability is evaluated. The reason for this is to exclude segments of lines which are not suitable for virtual balise placement due to predictable poor GNSS performance (obvious examples of such line segments are tunnels, but it can also be deep terrain or urban canyons or a line segment close to a strong terrestrial transmitter). Note that the procedure how to determine which segments of lines are suitable for virtual balise placement has to be standardized and will be part of engineering rules.

Availability is impacted by both, by technical capabilities (including all three GNSS segments: ground, space, and user) and environmental conditions. The environment impact has a significantly greater role in railway domain when compared with aviation. Even if the availability evaluation is restricted on line segments suitable for virtual balise placement the environment impact still has a significant role.

Exact specification of what is the minimal level of GNSS position quality is of great importance. This level is used for discrimination of states when the GNSS position function is considered as available or unavailable. Therefore, the availability is on the top of performance characteristics, meaning that

the level of GNSS position quality is expressed with other performance parameters (in aviation domain, the accuracy, continuity, integrity are used for this purpose).

It was confirmed with the STARS measurement campaign that the position quality significantly depends on local conditions and has a huge variability along the railway track. As main local factors impacting the position quality the following can be mentioned: restricted view of sky (signal blockage/attenuation), multipath, RF interferences (regardless if intentional or unintentional).

The position information will be used for safety of life purpose (determining train position, including track selectivity), therefore the availability is also impacted by utilized algorithms inside Virtual Balise Reader (inside the receiver) due to included counter-measures. The reason is the fact that fault-detection (and exclusion) algorithms, like RAIM, have more demanding requirements on satellite visibility than ordinary PVT (since RAIM requires GNSS measurement redundancy). Further, due to a non-zero false alarm probability of detection algorithms, the unavailability of the position information can be also caused by wrongly detected feared events.

Instant satellite visibility of required minimal number of satellites (even if satellite signals are tracked) is not a sufficient condition for providing GNSS position. Valid navigation messages have to be available too. The same is valid for EGNOS data to be possible to provide the position with the integrity. The railway environment is characterized by frequent signal outage due to obstacles along the track. If such outage occurred during the reception of some subframe (in case of GPS L1 C/A), or a message (in case of EGNOS), the information is not updated and a receiver has to wait when impacted subframe or message is broadcasted again. Frequent signal outage is especially relevant to EGNOS reception whose data are provided from geostationary satellites (with relatively low elevation in latitudes of Central Europe). To improve the described situation, and thus to mitigate the negative impact on the availability, a terrestrial data channel is considered.

When the applicability of the continuity, as another performance characteristic, is evaluated for the rail domain, the definition used in aviation has been used as a starting point for the analysis. The key aspect of continuity is a specification of an intended operation named mission, during which the reference function must not be interrupted accidently (assuming that the function was available at the beginning of the operation).

In the railway case the reference function is the train positioning function based on physical/virtual balises detection.

As defined in RTCA SBAS MOPS [37], the missions for aviation are en route, terminal, and approach phases of flight, where the pilot has to intervene when the GPS/SBAS function are no longer suitable for the defined missions, namely when an alert is notified to the pilot.

Regard to positioning system (function) consisting of GNSS and odometry, in the rail domain the mission must be intended as complete operation, i.e. from the original station to the end station with the same train number. With ATC systems, the driver cannot intervene on the system when the position of the train is not specified. The driver can only intervene as a result of the automatic intervention of the ATC System and perform the actions to be granted as required by the regulations. Therefore, the continuity requirement as used in avionics for missions is not a concept applicable to the rail.

By its nature, the virtual balise, as for the physical balise, implies a discontinuous signalling system. In order to guarantee the continuity of the overall railway mission it is necessary ensure the availability of the signalling system. This means that it is not necessary that the GNSS signal is continuously available on the whole railway line, but it is sufficient that it is in the **areas**[6] where virtual balises ar e located.

[6] In order to mitigate temporary poor GNSS SIS quality in a specific track point, the Virtual Balise detection algorithm would also take into account the GNSS SIS, its related augmentation data and the data coming from on-board sensors (e.g. IMUs) and/or odometry information associated with previous track points w.r.t. the train moving direction. This is reason

Therefore, unlike the aviation application, the concept of continuity of GNSS for generating virtual balises is not applicable, while the availability remains a stringent requirement to be assessed.

5.2.2.2 ACCURACY

The requirements on the position accuracy in the railway context must be evaluated separately as: along the track accuracy requirement and lateral accuracy requirement for track discrimination.

Along the Track Accuracy

The along the track position of the train is determined as distance from a balise group, which in this context is called the Last Relevant Balise Group (LRBG). With physical balises the estimated train maximum position error (i.e. a bound of the actual train position error) is calculated as:

Estimated Train Maximum Position Error = ±(*Q_LOCACC* +(5m+5%*d))

In this formula

- *Q_LOCACC* is the tolerable inaccuracy, with which the LRBG is placed on the track, including both measurement and mounting errors. Note that Q_LOCACC also includes the distance to the redundant reference location balise, in cases where the application requires redundant balises.

7.5.1.115 Q_LOCACC

Name	Accuracy of the balise location		
Description	This Qualifier defines the absolute value of the accuracy of the Balise location (i.e., the value 63m identifies a location accuracy of +/- 63m)		
Length of variable	***Minimum Value***	***Maximum Value***	***Resolution/formula***
6 bits	0 m	63 m	1 m

- "5 m" is a fixed maximum absolute error, which includes both the accuracy with which the balise reader can determine the centre of the reference balise, as well as errors resulting from data processing associated with the odometry processing chain.
- "5%" is the maximum relative tolerable inaccuracy of the odometry system, under normal operating conditions.
- "d" is the measured travelled distance since the last reference balise.

Note that the Estimated Train Maximum Position is added, respectively subtracted from the measured distance, the resulting range within the train front is located with high certainty (SIL 4) is called the Train Confidence Interval.

The maximum resulting inaccuracy of the train position along the track therefore depends on the distance from the referenced balise group, as well as the location accuracy, with which the reference balise(s) of the LRBG are placed on the track. It can range from, as absolute value, 5 m + Q_LOCACC just after passing a balise group to 118 m at 1 km distance from the LRBG, if reference balises are mounted with the maximum tolerable error of 63 m and the odometry errors is 5%.

Which maximum error is tolerable depends however on the actual application, with signals close to junctions or buffer stops being more critical than e.g. changes in permitted speed due to curves. Due to the described mechanism, the application can control the maximum train position error by placing

why it is important to take into account the track area around the location of the virtual balise. The virtual balise detection algorithm, will be described in the context of the S2R TD 2.4 Fail-Safe Positioning project.

balises with high accuracy (low value of *Q_LOCACC*) and at the right distance (d) from critical locations.

High demanding values for "*Q_LOCACC"* and "d" (distance from last balise to required stopping point) at critical locations are 1 m and 40m, which results in an inaccuracy of the position of 8 m, but this is application dependant. If 5 m and 100 m are used, the resulting inaccuracy is 15m.

When integrating GNSS into ETCS with the virtual balise concept the maximum accuracy will be calculated as above, but an additional value for the inaccuracy of the GNSS position has to be included [52]. In this case the estimated train maximum position error is calculated as follows:

Estimated Train Maximum Position Error = ±((VBDACC-EVBDACC) + Q_LOCACC + (5m + 5%*d))

In this formula

- *VBDACC* is the dynamically computed inaccuracy of the virtual balise reader function.

EVBDACC is the estimated value to be achieved by the on-board virtual balise reader function(under which normal operation shall be possible) to be statically a priori used for trackside engineering If the accuracy specified in EVBDACC cannot be guaranteed then train operation might be impacted in terms of intrusiveness, similar to the case where odometry accuracy cannot achieve the 5% minimum value.

Note: Depending on the criticality of the environment, different a-priori estimate values for EVBDACC can be used for different lines and their different parts based on the environment associated with the lines.

Note: It still needs to be determined what minimum accuracy the on-board virtual balise reader function has to achieve for also guaranteeing interoperability. This value and its associated EVBDACC are critical parameters to the performance of virtual balise application.

Lateral Accuracy

The lateral accuracy requirement refers to the distance that is perpendicular to train orientation (i.e. to the track) so that track discrimination can be guaranteed.

When the Eurobalise system and the ERTMS standard have been developed great care was taken to ensure that cross-talk between tracks can be excluded, meaning a train running on a track will not read a balise from a neighbouring track. When a train reads a balise it can therefore be concluded with a very high safety level (SIL 4) on which track the train is running.

When switching from physical balises to virtual balises such physical lateral cross-talk exclusion is not guaranteed anymore by using GNSS only, guaranteeing track selectivity therefore becomes more complex.

The [40] defines the nominal horizontal distance between track centres for new lines. In particular, in Table 4 of [40] for the lower range of maximum allowed speed it is reported a value of 3.8m as minimum nominal horizontal distance between track centres. Therefore, the required maximum safe lateral positon error for track discrimination is +- 3.80/2 = 1.90m.

It should be noted that the requirement of maximum error on the lateral position with respect to the track centres is not an ERTMS requirement, but it must be considered if the requirement to discriminate the track through GNSS is to be met.

The above-defined performance requirements consider the most demanding case scenarios for GNSS-based positioning. However, the following considerations apply:

- the longitudinal inaccuracy can be variable along a railway line, as expected for the location accuracy (named *Q_LOCACC*) of a physical balise, according [39].

- Depending on ETCS operational mode (see Chapter 4 of [39]) and the procedures to reach to this operational modes (see Chapter 5 of [39]) in which the train is at a specific moment the along the track accuracy may not be needed at all or it can be relaxed. How far is possible to extend this accuracy is still subject to discussion (a preliminary assumption of 20 meters has been considered in [36]).

- In case of lateral accuracy, the expected performance cannot be relaxed due to the need of tracks discrimination. “From the results obtained in STARS, GNSS based only on code phase (pseudorange) measurement seems not be able to safely guarantee this value. It remains to be evaluated in future projects whether the accuracy achievable with multi constellation / multi frequency receivers will be better, and also whether the use of GNSS carrier phase measurement, additional sensors and of signalling mitigations will help to guarantee the discrimination between parallel tracks.

Consequently, the current train position accuracy performance is expected to be: ±((VBDACC-EVBDACC) + Q_LOCACC +(5m + 5%*d)) meters for along the track error, and better than 1.9m for lateral error.

In the case of VB concept application, the along the track accuracy will be associated to the GNSS along-track PL, defining a new metric, namely a maximum estimated dynamic VB error (EVBDACC). This metric, together with its value of minimum accuracy to be guaranteed for the ERTMS interoperability under the nominal environmental GNSS conditions (EVBDACC, value still to be specified) and on-board fault free conditions, will be defined in the context of the S2R TD2.4 project with the support of the GNSS experts such as GSA and ESA.

5.2.2.3 INTEGRITY

In normal operation and for longitudinal errors along the track the concept of an Alarm Limit as defined for aviation does not apply for railway applications. The railway system only loses its safety integrity level when the actual train positioning error is not bounded by the train confidence interval, see figure below, as the Max Safe Front (Rear) End and the Min Safe Front (Rear) End are, in general and depending on the specific ERTMS functions, used to safely supervise the train movements.

The specific peculiarity of a railway signalling system is that the actual train position error can be temporally very large and, provided that it is still bounded by the train confidence interval, the supervision of the train movements is still safe. Bounded large train position errors have impacts on the mission quality (e.g. high intrusiveness), i.e. on the system availability and NOT on the system safety. This is the reason why the concept of aviation Alert Limit cannot be applied as is in railways.

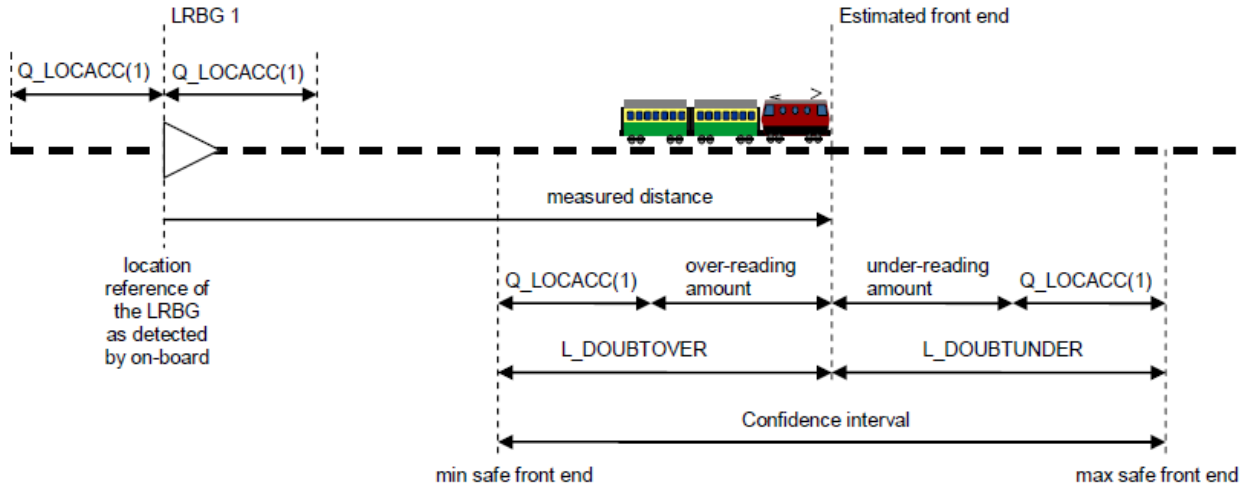

Figure 2. ERTMS Train Confidence Interval

Starting from the NGTC safety analysis and complemented by some further considerations carried out in the context of STARS (see [36]), the following figure describes a preliminary simplified safety integrity allocation tree for virtual balise detection.

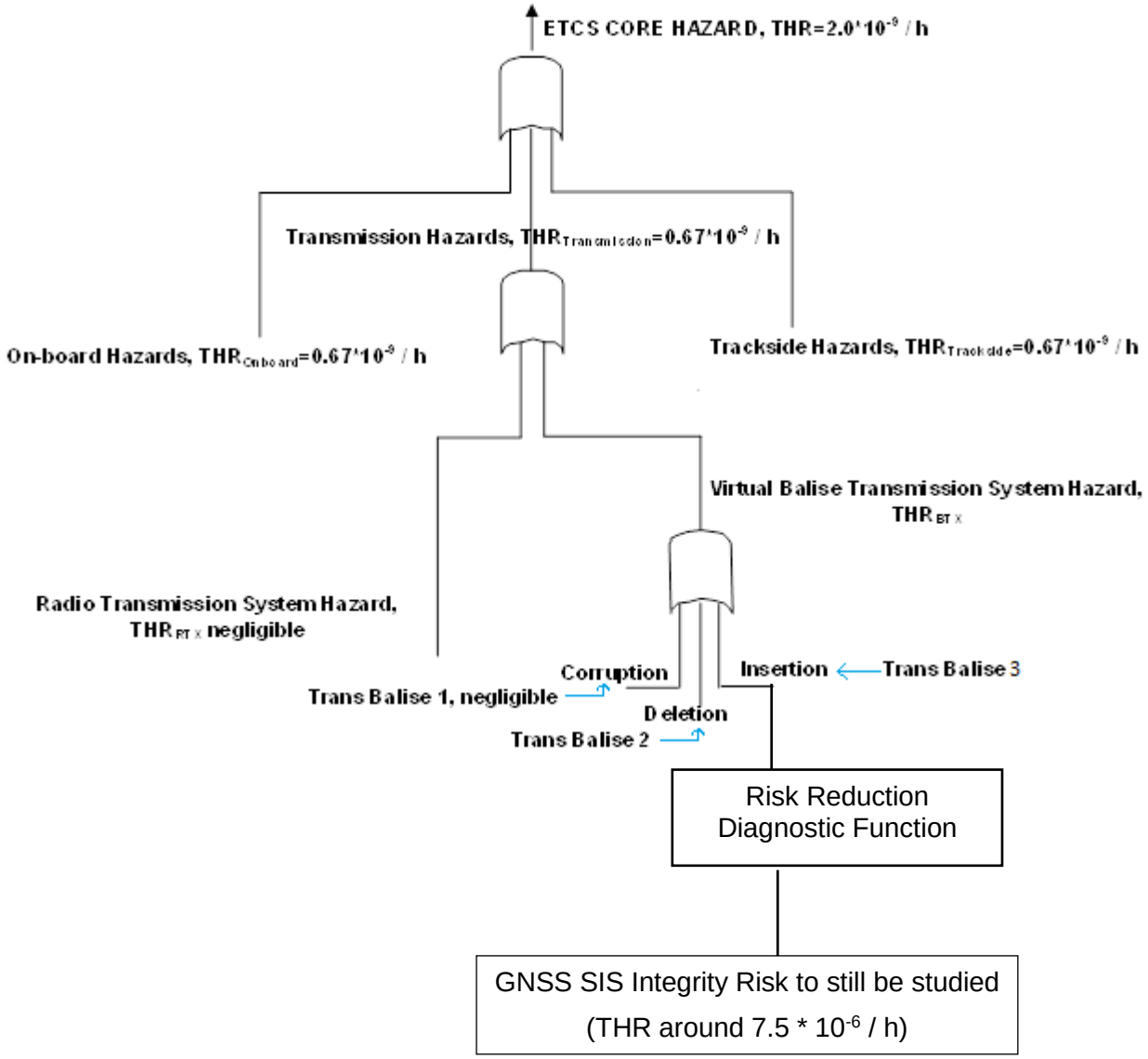

Figure 3. Simplified safety integrity allocation tree with VB detection

This preliminary safety analysis has been based on the following principles:

- As for the physical balise, the preliminary safety analysis has been carried out by using the same approach applied for physical balises and by adopting the recommendations coming from EN 50159 about the protection of communication channels. Therefore, virtual balise concept has also been considered in the context of a safety-related transmission system [41] made up of the non-trusted and the trusted parts.

  The former (i.e. non-trusted part) is logically composed of:

  - Global Navigation Satellite System;
  - Airgap GNSS signal in space (it does not include the airgap between the trackside and the on-board);
  - On-board GNSS antenna.

The latter (i.e. trusted part) logically includes the trusted functions of the Virtual Balise Transmission System such as the VBR functions as well as the "GNSS Augmentation Dissemination" and "Position Verification" [36]

Please, note that no hypothesis has be done on the physical architecture and the redundancy required to guarantee the ERTMS RAM [42].

This approach based on non-trusted and trusted parts enables the use of the same apportionment methodology used for the ERTMS safety analysis.

- Up to now, virtual balises have been mainly supposed to be used to reset the train odometry error and not for sending information, that if missed, or associated with a location not bounded by the static Q_LOCACC value (e.g. information of "Stop if in SR") could result in a hazardous consequence. To remove this potential limitation and allowing also the use of virtual balise for sending this type of information, further analysis are required. This will be carried out in the context of the S2R TD2.4 project where different VB detection algorithms along with the estimated VB location detection errors will be study and developed.
- The VB detection would be based on the combined use of GNSS and odometry (or other sensors) to guarantee a small probability of missing the detection of a VB. The VB detection algorithm will guarantee the high availability of the VB detection function.
- An allocation of THR = 10E-11/hour is made for TRANS-BALISE-1 (i.e. incorrect balise group message received by on-board Kernel functions as consistent), due to the very high level of data integrity protection provided by measures such as CRCs or CHECKSUMs for detecting the corruption of the balise information stored in the on-board track database or track geometry storage. This allocation leads to the consider TRANS-BALISE-1 as a negligible hazardous event;
- Under the preliminary assumption that virtual balises are used to reset train odometry error only, virtual balises do not sent TSRs, and "smart virtual balise detection" algorithms[7] can be adopted, a THR allocation much lower than 10E-10 / hour can be potentially assigned to TRANS-BALISE-2 (i.e. balise group not detected by on-board Kernel functions). This value will be determined in the context of the S2R TD2.4 project.

Based on the above consideration, a THR allocation of the order of 0.5 10E-9 / hour can be potentially done to TRANS-BALISE-3 (namely, when inserted balise group message is received by on-board Kernel functions as consistent). Thus, assuming that the track discrimination is done with the support of other means, the 100% of TRANS-BALISE-3 can be allocated to longitudinal error (erroneous localization of the balise location reference) only. The gap between the target for TRANS-BALISE-3 and the GNSS SIS integrity risk must thus be addressed by a diagnostic function independent from GNSS (e.g. an independent channel based on propagation of position using sensors and track constraint). This diagnostic function was only preliminary addressed in NGTC; further detailed studies are required and will be performed in the context of the S2R TD2.4 project (e.g. use of additional sensors to improve the fault detection and exclusion VBR capabilities, use of the dual frequency for improving the detection of multipath).

A complete and accurate safety analysis will be done during the execution of the S2R TD 2,4 Fail Safe Train Position project.

[7] The use of these algorithms may lead the probability of missing a VB detection equal to the probability of the VBR failure.

5.2.2.4 TTA

RTCA DO-229D defines Time to Alert (TTA) as the maximum allowable elapsed time from the onset of a GNSS positioning failure until the equipment (GNSS End User Receiver) annunciates the alert. To be noted that if the standard EGNOS functions for integrity monitoring are used, the impact of the current TTA on the VBR functions and the possible additional delay caused by the ERTMS communication channel for transmitting the SBAS information to the train will be evaluated. The best VBR solution for not exporting requirements to both the EGNOS current TTA and the ERTMS channel will be investigated.

In order to allow the design of the ERTMS enhancement also based on the GNSS Positioning that can meet the ERTMS safety and performance requirements, the VBR function will assume that the EGNOS TTA is guaranteed to be less than or equal 6 seconds as it already does for some aviation scenario.

5.2.2.5 COVERAGE AREA

For GPS and Galileo, the Space Service Volume (SSV) and the terrestrial service volume are generally considered to specify signal strength/capabilities and availability for users far from or near the surface of Earth, respectively.

In railway domain, since the trains move along the surface of the Earth, it is possible to refer only to the terrestrial service volume. It is defined as a near-Earth region where the healthy or marginal signal-in-space can be received when no localized obstructions are considered. The terrestrial service volume extends from the surface of the Earth up to 3000 km of altitude and has 100% seamless coverage [43], [44].

In the case of EGNOS V2, the service area is basically defined by the network of Ranging and Integrity Monitoring Stations and footprint of geostationary EGNOS satellites. So the EGNOS service is fully ensured over European Civil Aviation Conference (ECAC) region that comprises approximately latitudes from 20N to 70N and longitudes from 40W to 40E [45]. Note that the development of EGNOS will optionally provide a larger service area [45].

The possible use of EGNOS for GNSS-based train positioning must guarantee the possibility of acquiring the SBAS corrections potentially on all European lines, in order to allow the application of the virtual balise concept on an arbitrary ERTMS equipped line compliant with interoperability requirements.

Therefore, the requirement on the service area is formulated as follows. The EGNOS coverage service area must include at least all EU28 member states depicted in **Error! Reference source not found.**. Note that small islands like Canarias, Guadeloupe and others that belong to EU member states are not required to be included into the service area. Therefore, the service area of GNSS augmented by EGNOS for the use of the virtual balise concept on European railway lines should include land masses within latitudes from 34N (southernmost point of Cyprus) to 70N (northernmost point of Finland) and longitude from 11W (westernmost point of Ireland) to 35E (easternmost point of Cyprus). The seamless 100% coverage of this service area should be guaranteed.

As there are candidate countries for joining the EU in future, the service area is subject to change in future.

Figure 4. EU member states

5.3 CONVERGENCE BETWEEN THE ERTMS ARCHITECTURE AND THE SBAS SERVICE

This second step of the analysis is focused on the identification of possible gaps between the railways requirements and what is effectively providing the SBAS service as it is conceived today. The focus here is on the safety aspects of the signalling function and the related possible impacts of the GNSS.

In chapter 5.2 the SBAS performance, with particular focus on integrity, are analysed and compared with the rail requirements on the Virtual Balise Reader - GNSS subsystem in the framework of the architecture options discussed in section 5.2 in D5.3.

A brief summary of the integrity figures of the SBAS service in aviation are given and then the impact on the architecture and possible choices and recommendations are discussed.

5.3.1 SBAS integrity figures in the aviation domain

In the SBAS framework the overall integrity requirement is apportioned between both ground and user receiver contribution (assuming the fault free condition).

Fault free means that the system in a nominal state (no GPS/GLONASS/GEO satellite failure, no ground segment/user equipment failure). So misleading information (MI) is induced by the uncertainty due to measurements noise.

Measurement of code delay is affected by errors consisting into different contributions: atmospheric fading due to the electromagnetic wave passing through the troposphere and ionosphere, multipath, noise of the HW of the receiver (induced by thermal noise, clock etc.).

The integrity service of the SBAS tries to protect the user against the above issues on the signal and finally on the computed position.

The high level definition of integrity in the SARPs is:

A measure of the trust which can be placed in the correctness of the information supplied by the total system. Integrity includes the ability of a system to provide timely and valid warnings to the user (alerts).

The integrity is specified by its inverse, integrity risk. The integrity risk may be defined as the probability of providing a signal that is out of tolerance without warning the user in a given period of time.

The SBAS augmentation was originally designed for aviation applications (the EGNOS V3 next evolution of the European SBAS includes input from other application domains like Maritime), Therefore the focus is on Non Aircraft, signal in space (SIS) integrity risk as it is described in the fault tree for approach (fig 5 Appendix 1) with vertical guidance (APVI,II and Category 1 approach type) corresponding to the most demanding operations supported by SBAS..

The table below indicates the SIS integrity risk requirement for each flight phase as originally defined in SARPS.

	Accuracy		Integrity				Continuity	Availability
Typical operation	Horizontal Accuracy 95%	Vertical Accuracy 95%	Integrity	Time-To-Alert (TTA)	Horizontal Alert Limit (HAL)	Vertical Alert Limit (VAL)		
En-route (oceanic/ continental low density)	3.7 km (2.0 NM)	N/A	$1 - 1x10^{-7}/h$	5 min	7.4 km (4 NM)	N/A	$1 - 1x10^{-4}/h$ to $1 - 1x10^{-8}/h$	0.99 to 0.99999
En-route (continental)					3.7 km (2 NM)	N/A		
En-route, Terminal	0.74 km (0.4 NM)	N/A	$1 - 1x10^{-7}/h$	15 s	1.85 km (1 NM)	N/A	$1 - 1x10^{-4}/h$ to $1 - 1x10^{-8}/h$	0.99 to 0.99999
Initial approach, Intermediate approach, Non-precision approach (NPA), Departure	220 m (720 ft)	N/A	$1 - 1x10^{-7}/h$	10 s	556 m (0.3 NM)	N/A	$1 - 1x10^{-4}/h$ to $1 - 1x10^{-8}/h$	0.99 to 0.99999
Approach operations with vertical guidance (APV-I)	16.0 m (52 ft)	20 m (66 ft)	$1 - 2x10^{-7}$ in any approach	10 s	40 m (130 ft)	50 m (164 ft)	$1 - 8x10^{-6}$ per 15 s	0.99 to 0.99999
Category I precision approach	16.0 m (52 ft)	6.0 m to 4.0 m (20 ft to 13 ft)	$1 - 2x10^{-7}$ in any approach	6 s	40 m (130 ft)	35.0 m to 10.0 m (115 ft to 33ft)	$1 - 8x10^{-6}$ per 15 s	0.99 to 0.99999

Table 3. SIS integrity risk requirement for each flight phase

SIS integrity risk by approach (150 s) has been further decomposed into a 10^{-7}/approach allocation for the **ground system integrity risk** and a 10^{-7}/approach allocation for the **fault free case**.

The out of tolerance condition is defined in the SARPs in the user position domain

It means: when any user navigation system error (NSE) in horizontal or vertical dimensions is superior to Horizontal or Vertical Alert Limit (HAL or VAL)

The above situation (NSE > HAL or VAL) is often referenced as “Hazardously Misleading Information case (HMI).

Details about the apportionment of the integrity risk are provided in the Annex (Section 9).

5.3.2 SBAS integrity figures in the Rail domain

In this section the SBAS performance are characterized for the rail domain starting from the concepts developed in the aviation domain. Differences in the application of the SBAS concept in the rail framework will bring to a different methodology to define and assure the integrity during the different operational phases of the signalling function.

The GNSS based signalling architecture is based on the use of the GNSS receiver in two different options, see section 5.2 in D5.3.

In the first architecture option, the GNSS receiver is receiving the GNSS signals and outputs only measurements. The measurements will be then input to a box where a navigation filter will compute the position using possibly also other sensors and information.

In the second architecture option, the GNSS receiver is implementing the SBAS corrections and it provides the 3D position. This GNSS receiver could implement also other sensors input in a unique box.

The main difference between the two architectures is the apportionment of the integrity and the consequence need for a certain safety level for each element of the localization system.

In order to understand the impact on the SBAS and more specifically in the European case EGNOS service on the system a first step is the analysis of the compatibility of the SBAS specifications with the rail safety requirements.

The services that will be analysed in this document are EGNOS SoL (Safety of Life) and EDAS (with a proposal for adaptation for the use in the railways and called EDAS-R).

As defined in the section 7.2 of D5.3 the fault tree of the GNSS integrity risk gate is specified for the three different operation modes.

- Staff responsible
- Full supervision (Movement authority)
- Start of mission

As described in D5.3 in MA and SR, GNSS integrity risk THR apportionment of 7.5*1e-6 (with 10s TTA) among the main functional blocks is calculated by assigning each identified hazard coming from the non trusted part of the virtual balise transmission system to a functional block based on the described reference architecture.

Recalling the analysis in D5.3, THR should amount to **7.5*1e-6 / hour** Total THR amounts to the sum of the lower level gates THR assigned to this functional block. In fact, the hazard gates assigned to the architectural element GNSS receiver type II, build up a total lower bound of 7.2*1e-6/hour+1e-9/hour

In SoM, GNSS integrity risk THR apportionment of 1.0*1e-4 (with 10s TTA) among the main functional blocks is calculated as in the MA and SR cases.

The total apportionment presented in D5.3 and detailed in the tables for each operation mode, should be divided between ground and user segments and so a comparison between the EGNOS case and the rail case can be made. This analysis can be performed in deeper detail in a second step in a future activity once the methodology here discussed for the SBAS compatibility assessment will be agreed and the detailed information about the internal apportionment of EGNOS will be available.

In the Annex (Section 9) a brief summary of the main concepts regarding the SBAS integrity is reported together with the allocation of the integrity figures on the ground segment and on the user segment.

This distinction is important since if the system is designed following a specific requirement in terms of integrity for a certain application (and it is actually coming from the aviation domain) the system is designed accordingly, leaving small or even no room for any modification to accommodate more stringent requirements (coming from another application).

This analysis is provided just to anticipate that if the SBAS system as it is conceived today cannot cover directly and as an alone mean the location function of the ETCS architecture, it can be included in the architecture as one of the element and its performance will be analysed accordingly.

So it is important to have a clear picture of the requirements expressed from the rail domain and understand how they can be translated into specification of the SBAS system (which can be matched or not by the present system).

Then the possible architectures that were introduced into D5.3 are analysed in terms of the use of the GNSS receiver capabilities.

Some recommendation on the SBAS receiver are then provided in order to fill the gap between the performance requested and what is actually possible with the present SBAS service.

In the future the EGNOS design tailored for the railway environment should consider these values to assess the feasibility of such requirements

5.3.3 The GNSS in the Virtual Balise Reader function

In the document D5.3 EGNSS Target Performances to meet railway safety requirements (deliverable STR-WP5-D-ANS-034-06) two possible architecture of the Virtual Balise Reader function on board the train are sketched.

The two architectures are:

Option 1: The Virtual Balise Reader consists in four functional blocks; a “GNSS receiver type I”, a GNSS Algorithm tailored for railway (named “R-GNSS Algorithm”), “Virtual Balise Detector” and “Track Database Manager”.

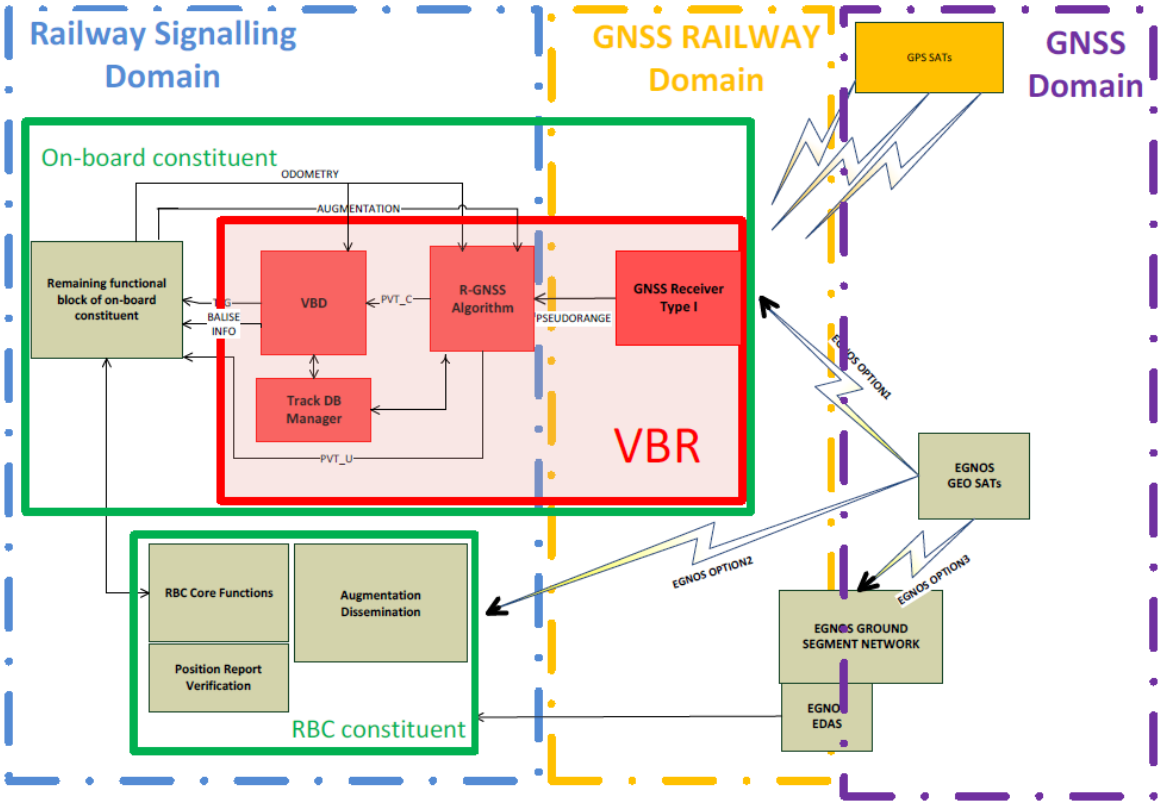

Figure 5-5. VBR architecture Option 1

Option 2: the VBR consists in four functional blocks:

- "GNSS receiver type II",
- "Position mapping and monitoring checks"
- "VBD" and
- "Track Database Manager".

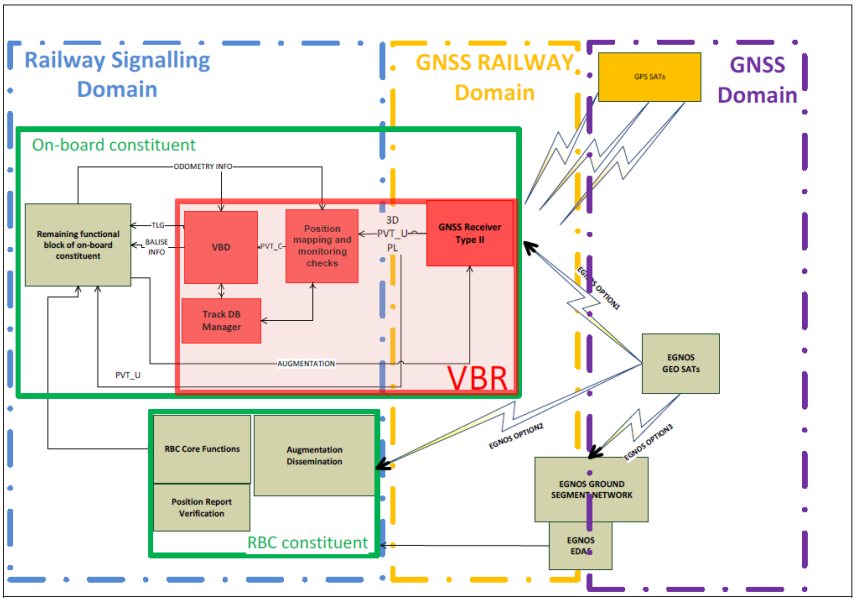

Figure 5-6. VBR architecture Option 1

As a first hypothesis we can think about applying the same SBAS concept developed in the aviation also in the rail domain.

So we can think about an on-board GNSS receiver and algorithms block dedicated to PL evaluation (option 2) outputting PVT and XPL as in the aviation case.

Which are the limitation of this approach?

We know from the introduction that the integrity figures applied on the localisation function are different from the aviation case.

In the option 2 the THR requirement of the VBR must be split among the different elements of the architecture and in particular on the receiver.

If the GNSS receiver type II is a standard GNSS receiver (standard means standalone and compliant to the MOPS), the following reasoning can be made.

The ground segment of the SBAS system is designed for the aviation application therefore the countermeasures to minimized the probability of missed detection are taken with respect to aviation requirements and procedures (refer to page 22 - Probability of missed detection equation)

The Probability of missed detection in the ground segment depends on the integrity requirement (that can change as seen in the introduction for the rail case) and on the capacity to put all the possible countermeasures to reach the target Pmd.

If the Pmd reached in the aviation case, in the ground segment doesn't meet the rail requirements, nothing can be done at ground level without changing the way the system is implemented (resilience, redundancy, hybridization, design procedures etc.).

Any ground segment failure is impacting the user receiver algorithm in the sense that the integrity levels (XPL) computed by the receiver are based on the messages computed by the ground.

If the ground experiments errors without detection, this is immediately reflected on the user level inducing an error in the evaluation of the XPL or in the application of the corrections (or both depending on how the missed detection at ground is distributed among the different algorithms).

Another limitation comes from the integrity risk allocated to the user segment that is defined as fault free case that is to say the protection from the MI is considered only for noise on measurements.

It appears that multipath/RF interference can be the most important noise contributions in the rail domain that is an important difference with respect to the original SBAS noise model

They need to be properly dimensioned when redefining the sigma of the residual errors in the receiver. SBAS computation are based on the knowledge a bound of the local environment effect on receiver (Multipath/interferences). For sure the value defined for aviation are not convenient for a train.

It is also an important driver for regulation applicable to the receivers.

Finally, the K factor choice in the railway PL computation is another issue to be investigated

So the result of this reasoning is that:

1. The gap in the integrity risk difference between aviation and rail must be deeply investigated, considering also the concept of ERTMS/ETCS to generate train position information from "absolute" positions at balises and odometry information between balises. (see D5.3, §3.7).
2. Local multipath effects, as well as electromagnetic interferences and shading of satellites, should be properly evaluated, modelled and outliers measurements shall be detected and

rejected. The STAR study identifies the need for this “rail domain” specific function that do not exist in today aviation receivers

3. Since the environment can change considerably from clear open sky into urban canyons ERTMS specific procedure should be considered to optimally define the location of the virtual balise
4. Since SBAS messages are coming from the GEO link in obstructed areas it is necessary to use a different communication mean (see in the next of this section).

From the point of view of the accuracy performance it appears that the SBAS should be enough to meet the rail target (ref. D5.3) for along track direction. The real concern is the availability and continuity that are again impacted by the different environment with respect to the aviation case. Availability and continuity issues can be partly mitigated by sending the SBAS messages with different telecommunication means, for example terrestrial wireless communication, overcoming at least the GEO satellite visibility discontinuities.

It remains a major concern the high variability of the DOP (Dilution of Precision) due to “canyons” and foliage. DOP is a measure of the impact on the position error due to the geometrical layout of the satellites.

The higher is the DOP the higher is the position error. The optimal DOP is obtained when the receiver is in the centre of a Tetrahedron where the vertices are represented by the satellites. When the user is in a difficult environment where there are obstructions, the geometrical layout becomes unequal and the DOP will increase.

The approach based on the direct application of the SBAS rules inside a GNSS receiver as seen before can bring to some difficulties.

The architecture option 1 instead separates the measuring function (extraction of pseudoranges) from the SBAS and other sensors and mitigations implementation.

The reasoning is similar as in option 2, but in this case the GNSS receiver is not a SBAS receiver.

The augmentation functions are all in another box where specific mitigations are put to fill the gap between the integrity risk reachable with SBAS and what is needed in the case of the rail.

THR is therefore split into more than one block; the THR required for a single block (in particular the receiver) could be different (higher) than the THR of the entire VBR system, depending on the design choices. This could allow a less complex HW/SW implementation.

Nevertheless, the same limitations we discussed for option 2 are also applicable in option 1:

1. Multipath and interference
2. Definition of the optimal location of balises
3. continuity of SBAS link

5.3.4 The service impact and evolution

From the service provision point of view we can look at the following figure (Ref. D5.3 EGNSS Target Performances to meet railway safety requirements, deliverable STR-WP5-D-ANS-034-06):

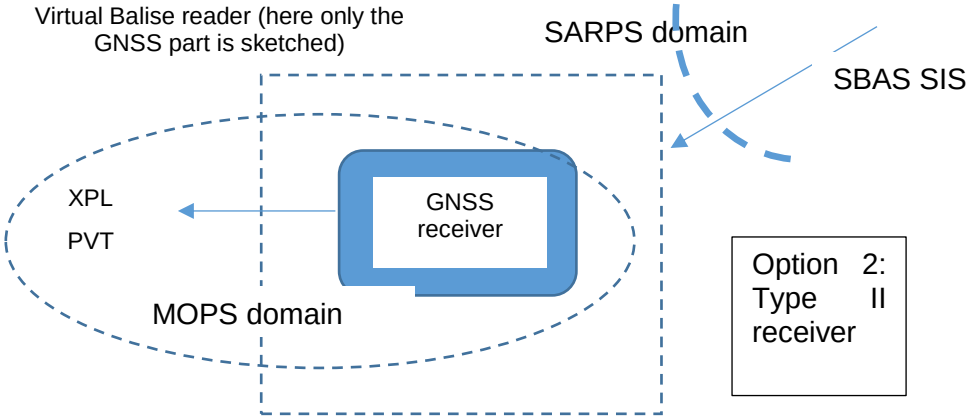

Figure 5-7. MOPS and SARPS domains in VBR architecture Option 2

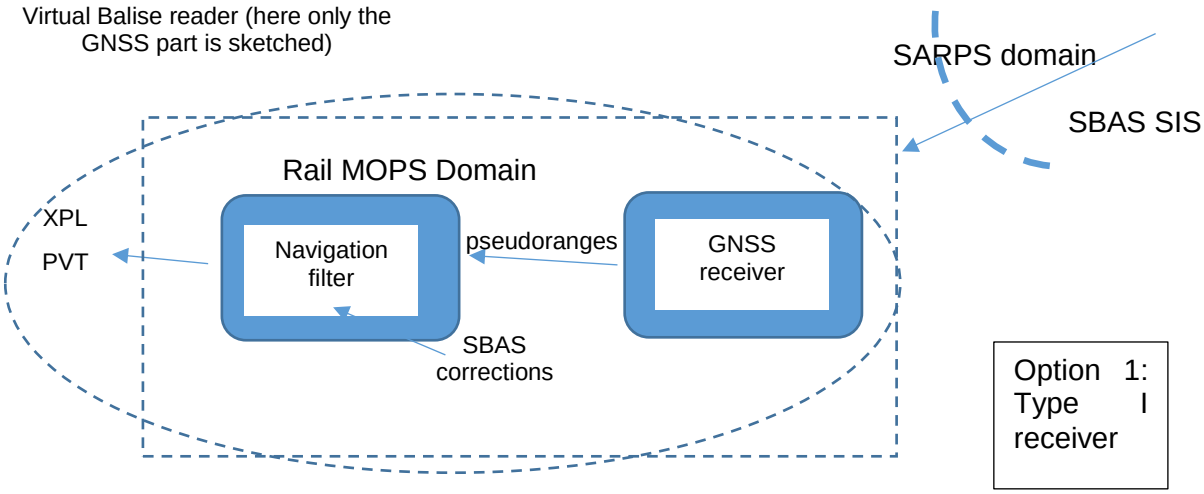

Figure 5-8. MOPS and SARPS domains in VBR architecture Option 1

The dashed box is the location function and it is detailed for both the architectures (option 2 - top figure and option 1 - bottom figure), from the SBAS point of view it contains a module that is able to compute the ranges and a module that is able to compute the SBAS correction. This is valid for both the options.

The SARPS are specifying the requirements on the SBAS SIS and the SBAS service provider is responsible of this component of the overall performance.

The MOPS specifies the requirements on the user receiver side (the nominal environment where the receiver can operate and where the performance can be met, the corrections parameters, the testing for the certification and the way the XPL are computed). By the integration of the two elements (the requirements expressed in the SARPS and the requirements expressed in the MOPS), the safety case can be met.

The MOPS domain in the option 2 is very clear and covers the entire receiver. This means that in the original aviation case the receiver must be designed following the MOPS specification against which it has to be certified.

This reasoning is applicable also in the railways context since the GNSS part must be certified against a standard (a “rail” MOPS) today not existing.

As discussed in the previous section, in order to reach the overall integrity figure in rail, the receiver must implement other functions that can mitigate other effects and reduce the probability of missed detection. This introduces differences between the aviation MOPS and the rail MOPS.

The option 1 analysis is not so straightforward and some discussion is needed.

In principle the SBAS correction are implemented by the navigation filter that is outside the GNSS physical receiver. Therefore a MOPS specific for rail should be defined covering:

- The GNSS receiver for the multipath and interference detection and mitigation components (that are of paramount importance).
- The way the SBAS corrections are computed and added to the pseudorange measurements coming out from the GNSS receiver (this point could still follow the aviation MOPS).

Up to this point the SBAS service is covering the safety case correctly and it assures that the residual error after the implementation of the corrections follow the statistical distributions as expected as in the original MOPS (therefore covering up to the aviation safety case).

Then the rail MOPS will add specifications for the definition of the navigation filter that will put together corrected pseudoranges and other sensors to output PVT and XPL matching the rail safety case.

In the near future EGNOS V3 will be deployed (it is foreseen around 2025) and it will bring augmentation for multiconstallation and dual frequency.

This new service should improve the SBAS SIS side further reducing the gap between the aviation case and the rail case and helping in easing the implementation of the two possible architectural options.

5.3.5 Recommendations

Except for the multipath and interference, the residual error after the application of the SBAS corrections should bring the accuracy inside the threshold specified for the rail application (this is confirmed by the preliminary results of the on field tests of the STARS WP 4 and WP 5 analysis).

Major concern is the loss of integrity due to MI or HMI events, linked to the visibility of a sufficient number of satellites and to the availability of the SBAS message communication link.

Moreover:

1) In the case of option 2 sensor fusion could be mandatory to fill the gap as much as possible between the aviation case and the rail case but the needed safety level would be probably at the highest level (SIL 4) of the overall subsystem, resulting in a very high cost of the receiver.

   This is a recommendation that must be supported by testing campaign and a possible future evolution of the STARS project should analyse this topic.

2) In the case of option 1 only pseudoranges are output from the receiver. In principle this could be a simple GPS receiver but as we said before multipath and interference levels require some architectural specific design inside the receiver itself carrying to a specific “rail GNSS receiver” (essentially recommendations should be made for the RF front end in terms of interference detection and mitigation, at correlator level and discriminator/tracking level for dealing with multipath and interference). SBAS corrections application and sensor fusion can be made in another box taking as input the pseudorange.

   The pseudorange can be then corrected by the SBAS carrying in the range domain to residual errors that are following the bounds indicated by the SBAS standard (always taking in mind the important impact of multipath and interference). It remains a “gap” between the total level

of integrity and what the SBAS is able to offer. This gap can be filled using in the navigation filter other sources of information like other sensors, helping to reach the overall integrity features.

This means that the SBAS component is only one of the possible contributors to the overall integrity figure and with the exception of multipath and interference it could be used with reference to the SIS component (from the above discussion the receiver part is completely different from the aviation standard). An important prerequisite for the SBAS application is to adopt technical solutions to overcome the issue in the visibility of the GEO.

From a general point of view impacts on integrity, availability, continuity and accuracy are coming from the varying satellite geometry layout. For this problem, mitigations are coming from the application of ERTMS specific rules and procedures (ref. next point 3).

Also signal attenuation due to e.g. foliage must be taken into account; signal attenuation brings to degradation of C/No and then to an increase of the pseudorange noise. It should be taken into account by additional contribution in the error budget.

3) In general (and it is valid for both the above mentioned options) in the framework of the ERTMS Virtual Balise concept, the virtual balise should be “virtually” put in places where multipath and interference meet the aviation requirements (and where visibility of the satellites in terms of DOP is good). This leads to several possible impacts on the ERTMS deployment procedures but it dramatically contributes to meet the safety case. This helps to solve the problem of the multipath and interference contributions to the integrity of the SBAS component. By the way since the environment surrounding the virtual balise location cannot be under continuous monitoring (building, foliage etc., may change in time) it should be mandatory to have receiver internal functions able to assess the local environment (multipath/interferences) using some kind of measurement (not only pseudoranges e.g. based on direct signal processing on I&Q samples).

   The above functions will identify that the present environment is no longer bounded by the maximum value known by the ground segment and so that the service shall be declared unavailable at that point at that instant.

4) The evolution of the SBAS (like in EGNOS V3) should of course improve the overall performance figures. Moreover, parallel initiatives like EDAS-N could open the way to new means of SBAS message transmission that can match integrity requirements.

5.4 EXPECTED IMPACTS ON THE ERTMS ARCHITECTURE AND OPERATIONAL PROCEDURES

The virtual balise concept has been used to minimize the impact of the introduction of GNSS in the ERTMS solution. Moreover, its introduction must guarantee the backward compatibility with existing ERTMS systems and the ERTMS interoperability requirements. As requested by the main ERTMS stakeholders (i.e. ERA, IMS, RUs, Industrial Suppliers), the introduction of any new technology and new functions must not jeopardize the existing investments done in last decades.

In the context of the STARS project, the preliminary high level functional architecture defined in NGTC has been further analyzed. This high level functional architecture foresees the on-board functional block named “Virtual Balise Reader” (VBR) and two trackside functional blocks respectively named “GNSS Augmentation Dissemination” and “Position Verification” [36].

The additional analysis carried out in STARS has been based on the objective of using EGNOS as is (i.e. without exporting safety and performance railways requirements to the EGNOS space segment) and evaluating two possible different alternative apportionment of the GNSS functions, required to perform the VBR functions:

1. on-board GNSS functions allocated to the GNSS receivers only (i.e. GNSS receivers that guarantee the safety and the operational performances up to the position domain) or
2. on-board GNSS functions allocated to a railway equipment responsible for ensuring the safety and the operational performances into the position domain, starting from (a) the information received from GNSS receivers operating into the pseudorange domain only and (b) the received SBAS augmentation data.

The VBR logical interface towards the on-board ETCS kernel is invariant w.r.t the alternative apportionment of the GNSS functions whereas the impacts on (a) the liability of the GNSS and Railways Stakeholders, (b) the GNSS service provision, and (c) the certification process and conformity declarations strongly depend on the alternative solution adopted. However, independently of the alternative solution, the detection of virtual balises is foreseen using GNSS, where EGNOS (as the SBAS augmentation system) has been investigated as the key enabling technology to support the safe virtual balise detection. This section provides some preliminary description of these impacts whose detailed and complete analysis will be carried out in the context of the S2R TD 2.4 Fail-Safe Positioning project.

In addition, the S2R TD 2.4 Fail-Safe Positioning project will use the outputs of STARS for performing a complete functional specification and a safety functional hazard analysis of the Fail-Safe Train Position. The specification and the safety analysis phases will take into account the STARS results related to, for example, the Geostationary GNSS SIS poor coverage, the need of specific Position, Navigation and Timing (PNT) algorithms to cope with local feared events, and the preliminary indication for the along-track protection level equation along with the preliminary analyzed error model. The output of these analysis phases will be a set of technical specifications (where FFFIS interfaces are well described) to be harmonized with the future CCS TSI version, consistent with specific objectives applicable to the CCS TSI, see Article 7 - Specific objectives applicable to CCS TSI [46] and item 28 of the CCS TSI [46] where the Satellite Positioning has been identified as one of the main contributors of the strategic challenges identified from ERA, see Annex 1 of [47].

The set of technical specifications related to the introduction of the Virtual Balises whose detection is based on GNSS would also cover the review and update of at least the following ERTMS Subsets:

- Subset 023 to introduce the new definition related to Virtual Balises (e.g. Virtual Balise Antenna Marker, Virtual Balise, Virtual Balise Marker, …);
- Subset 026 to specify the functional requirements related to virtual balise only (e.g. TSRs must be sent from RBC in ERTMS L2 and L3 and not by means of virtual balises, train confidence interval also based on the dynamic value of the virtual balise location error computed by the VBR at the VB detection, use of track geometry information received from RBC, static balise location accuracy also for Virtual Balise, new ERTMS Language for transferring augmentation data, track geometry information, ERTMS modes and transition, ERTMS Procedure, …);
- Subet 040 to include the dimensioning and engineering rules related to Virtual Balises and Virtual Balise Antenna); this update version or another subset would include guidelines for the new RBC Data Preparation for Virtual Balise;
- Subset 041 to take into account the minimum interoperability performance requirements that depend on the balise detection location error; this error is not a fixed value as for the case of physical balises;
- Subset 076 to outline, if necessary, the functional and performance test cases and test descriptions that can be affected by the use of Virtual Balises instead of Physical Balises;
- Subset 088 and Subset 091 to also carry out the Safety Analysis suitable for the use of Virtual Balises and to specify the THRs related to the Fault Model caused by the use of Virtual Balises;

- Subset 027, to include JR diagnostic data to enable the off-line analysis for the correct assignment of responsibility in case of failure or degraded performances.

In addition, a new, dedicated subset for virtual balise may be prepared (to complement signalling perspective) if decided by UNISIG.

In order to specify the requirements for the functions related to the GNSS domain and guarantee the safety and interoperability requirements, this set of technical specifications would also include the Railway MOPS where the minimum operational performance standards for railways applications (i.e. to cope with the railway environment and the railway mission profile) are specified. This Railways MOPS would also specify the liability perimeter between the GNSS Domain and the Railway Domain. For example, with regard to the first domain:

- The SBAS / EGNOS requirements and performances relevant to railway might only address pseudorange SIS performances and not those related to position domain because robust and safe GNSS monitoring techniques to cope with local feared events are required;
- The GNSS Receivers and the EGNOS Service provision would guarantee the pseudorange SIS performances in the pseudorange domain only, assuming all other SBAS service conditions are met;
- The GNSS Receiver would provide GNSS Diagnostic data to enable the safe detection of a failure in the GNSS on-board chain made up of GNSS Antenna and the GNSS Receiver.

On the other hand, for example, for the railway domain:

- the VBR is in charge of (a) protecting the user from local feared events, (b) bounding of residual errors due to local phenomena, (c) protecting the ETCS Kernel from residual risk of errors due to system feared events and ionosphere events, (d) the correct translation of the range domain bounds to position domain bounds, and (e) the appropriate management of the SBAS Time to Alert;
- the ERTMS On-board Supplier is responsible for demonstrating the VBR safety and performance requirements with respect to both the system and the local environment phenomena. The Supplier Generic Product Safety Case would include qualification evidence based on Laboratory Tests and Field Tests that also inject GNSS faults caused by the railway local environment.

As the introduction of the Virtual Balise can be in general considered “a significant modification to the existing ERTMS standard”, in accordance with the [48], the Common Safety Method (CSM) on risk assessment would be applied, then the applicant has to evaluate the associated risk according to the following six criteria [48].

- Failure consequence: credible worst-case scenario;
- Novelty: innovative or new to organization;
- Complexity: the complexity of the change;
- Monitoring: the inability to monitor the implemented change throughout the system life-cycle & intervene appropriately;
- Reversibility: the inability to revert to the original system;
- Additionally: assessment of the significance of the change taking into account all recent safety-related changes which were not judged to be significant.

Moreover, a CSM Assessment Body (CSM AB) would also be appointed by the Applicant. Please, note that a CSM AB makes judgments whereas a NoBo carries out an independent assessment (see Regulation 402/2013 [48]); a NoBo checks formal conformity of a structural sub-system versus all requirements defined in relevant TSIs.

Assessment of conformity of ERTMS interoperability constituents and subsystems, based on the GNSS technology, with respect to the new CCS TSI and other relevant technical specifications and standards would be carried out by the Notified Body as currently required by the CCS TSI. The NoBo would complete its own activity by providing the EC declaration of conformity for the product or the EC declaration of verification for the subsystem.

As far as the certification of EGNOS for being used in ERTMS, the CENELEC cross-acceptance process would be applied. This cross-acceptance process would cover the following two aspects:

- the acceptance by ERA and by Railway Stakeholders of the certificate granted by the competent EU authority to the GNSS service provide for aviation application, and
- the acceptance of the performance guaranteed for rail application by the service provider to be identified for rail applications. This service provider, once selected and certified also for rail applications, would be responsible for ensuring that the operated system, the operations and the maintenance of the system ensure the navigation service with the specified safety and performance.

This cross acceptance process would be performed under the control and the acceptance of GSA, ESA and ERA and it would also cover the quality management recommendations required by CENELEC. Furthermore, GSA and ESA would declare and ERA would accept that EGNOS can be used for ERTMS in accordance with the Railway MOPS and the Service Provision for railways to be specified with an adequate document.

5.5 EGNOS SoL Service Limitations

Currently, EGNOS SoL service has some significant limitations. This section is devoted to list and describe them.

First of all, EGNOS is a SBAS that currently augments only GPS and it is single frequency.

However, it is foreseen that the next generation of EGNOS (EGNOS v3) will offer two additional features: it will augment the Galileo positioning service (i.e. dual constellation capability with GPS and Galileo), and will provide correction data and integrity information with a second signal in the GPS L5 and Galileo E5a frequency bands (i.e. dual frequency capability in the L1/E1 and L5/E5a frequency bands) [34]. Dual frequency measurements will allow user to directly correct ionospheric error without the support of external corrections.

These features will increase the robustness of the service and improve the performance provided to users for navigation services, notably in terms of positioning accuracy, and in the same time offering additional resistance to signal blockage, for example in urban and sub-urban canyons, by through the increased number of satellites[8].

The SoL service based on GPS & Galileo in the L1/E1 and L5/E5a frequency bands is foreseen to become operational around 2023. Before that date, EGNOS shall be used as it is currently with the significant limitation of single constellation and frequency.

Secondly, EGNOS computes for each pseudorange a residual error that is partially bounded by a threshold mainly based on the UDRE and GIVE parameters, knowing that the local phenomena such as interference and multipath have a bounded value for an airplane. The railway context is completely different from the aviation one, since the local phenomena occurring in rail environment, as multipath, has a big impact on GNSS performance. HPL computed by EGNOS assumes that the local errors are bounded by the values defined in MOPS.

The bounding formulas for residual errors (sigma) used in aviation domain cannot be applied to the railway environment, so new formula must be formulated.

As output of STARS study is the necessity to include inside user positioning equipment a function to detect and reject measurement for which the multipath effect overpasses the defined bounding formula.

A first study to adapt the avionic concepts to the railway context has been carried out in the RHINOS project, where the definition of new bounds of local errors as multipath and then HPL in nominal and fault conditions has been performed, [5], [6].

Moreover, the RHINOS study has developed and assessed a variety of multipath mitigation methods and examining which ones should be used. The analysis supports this by determining the necessary level of multipath mitigation to achieve the desired performance goals. There are many reasonable methods that can be employed for detection: 1) multiple frequency combinations (L1/E1-L5/E5), 2) carrier phase-based detection, 3) multiple separated OBU antennas, and 4) skyview surveys. The first three methods use measurements that should be uncorrelated from single antenna L1/E1 pseudorange to test for discrepancies from multipath. A skyview camera can be used to pre-survey the track to create location and azimuth dependent elevation mask to limit NLOS satellites and multipath signals.

Thirdly, the availability of the EGNOS geostationary satellites is not optimized for guaranteeing the needed coverage along railway lines.

An alternative way to use EGNOS signal is the broadcast of the EGNOS corrections and integrity information via terrestrial transmitters or via internet as proposed by the EDAS service. The availability of this alternative link is then to be verified. Moreover, let us mention that the availability of the SBAS may be required only in concrete locations (e.g. in the places where the virtual balise should be placed) and not along the entire railway line. The global availability of the SBAS can then be reduced along the line.

Fourthly, EGNOS TTA in avionics is 6s. In the rail domain, a new value shall be defined according to specific selected scenarios of the interest.

Fifthly, EGNOS SIS is not robust to jamming or more dangerous spoofing and signal authentication is not provided [3]. An alternative way to use EGNOS is to distribute its corrections from EDAS to ERTMS/ETCS through EURORADIO protocol that guarantees the needed security level [4].

6 EGNOS EDAS FOR RAIL

6.1 EDAS-R SERVICES

The EGNOS Data Access Service (EDAS) is a terrestrial commercial service (with an architecture as proposed in Figure 6-1) offering ground-based access to EGNOS data through the Internet on controlled access basis. Geared to users requiring enhanced performance for professional use, EDAS provides users with the same data broadcast by the EGNOS satellites (EGNOS Message) in near real-time.

In order for EDAS services to be applicable to the railway domain, bringing to a new service named EDAS-R, there will be railways specific requirements on the EDAS service content as well as the bearer of the data. It is advisable that the communications requirements upon the bearer should be compliant to a similar form of communications already implemented within the railway domain such as RBC-RBC communication [49]. The requirements upon the content delivered by the EDAS-R in order for the railway domain to produce vital train positioning are covered in section 6.2.

It will be necessary for the EDAS service communications bearer to be compliant to, at the very least current railway standards, and in the future at evolution of those standards in order to accommodate parallel developments within communications technology.

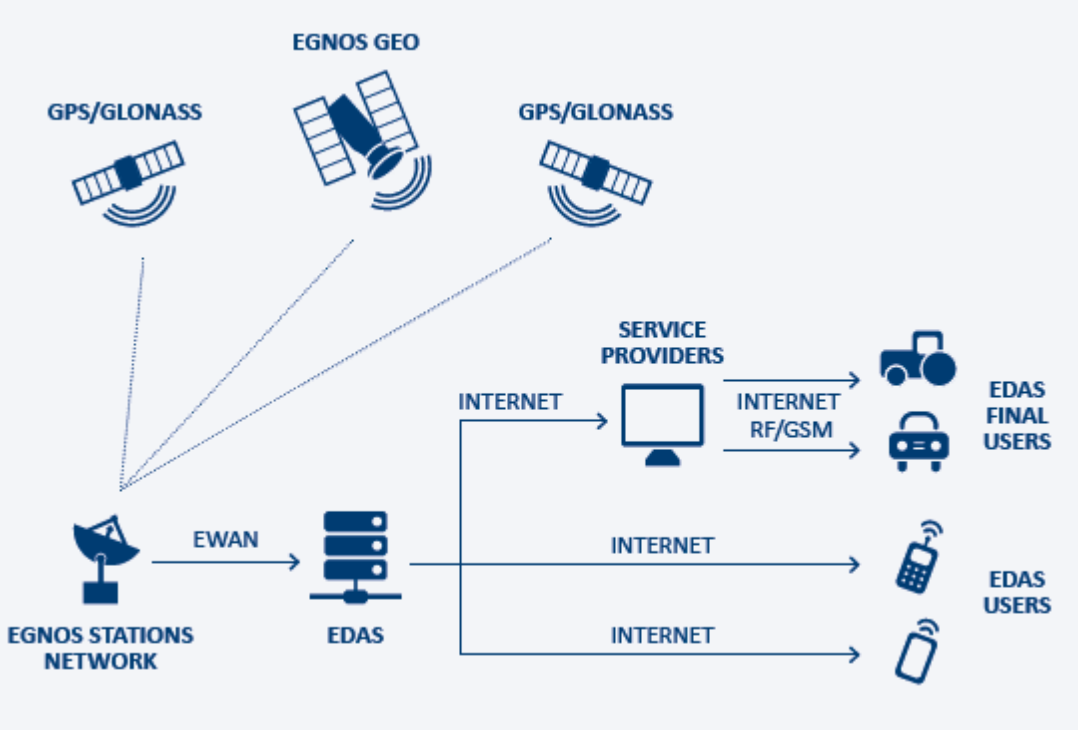

Figure 6-1. EDAS High-level Architecture

6.1.1 Current EDAS Data Access Service

While EGNOS (subject to application conditions for SoL) together with a receiver compliant with RTCA DO-229D MOPS is certified for SoL applications within aviation, EDAS services available today are not and as such the requirements gap between EDAS->EDAS-R should follow a similar path as EGNOS OS -> EGNOS SOL suitable and appropriate for rail applications. Current EDAS service provided by EDAS are identified in the following table.

EDAS Service[8]	Application notes for Rail
Service Level 0 (SL0)	Raw Data stream. Uses ASN.0 protocol which allows reconstruction of the complete EGNOS message by the receiver of the data. Contains EGNOS data. Requires the use of EDAS Client software.
Service Level 2 (SL2)	Raw data stream. Uses RTCM 3.1 protocol and thus contains, overhead for DGNSS. Contains EGNOS data. Requires the use of EDAS Client software.
EDAS Data Filtering Service	Provides a predefined subset of the Raw Data Service Levels 0 and 2. As such the predefined data sets are most likely not suitable for rail applications as they are tailored to aviation. Requires the use of EDAS Client software.
EDAS SISNeT Service	Currently used mainly for education, EGNOS monitoring and R&D. GETPOS command allows positioning functionality but this is of a differential nature and thus not suitable for rail applications for the same reason as the NTRIP service and the raw data SL 2 service. This service distributes EGNOS data as it would be received by a physical EGNOS receiver. SISNet is an ESA defined protocol.
EDAS FTP Service	Could be used for historical analysis.
NTRIP Service	The EDAS-based NTRIP service retrieves GPS and GLONASS raw measurements from the EGNOS stations (RIMS and NLES) and disseminates this information through the NTRIP (version 2.0) protocol in RTCM 3.1, RTCM 2.1 and RTCM 2.3 formats. Differential GNSS corrections and phase measurements, as well as additional messages for RTK (real-time kinematic) implementation, are provided within the NTRIP. This service should be further investigated for railway. Real Time service.

Table 4. EDAS services description

The various EDAS services currently available provide different type of data; Table 5 below shows the type of data associated with each service.

[8] Notes: All of the services except the FTP are near real time services. EDAS Client software provides a software interface as well as basic security functions.

Mode	EDAS Service	Type of Data			
		Obs. &nav.	EGNOS messages	RTK messages	DGNSS corrections
Real Time	SL0 & SL2	X	X		
	DF0 & DF2	X	X		
	SISNET		X		
	Ntrip	X		X	X
Archive	FTP	X	X		

Table 5. EDAS Services data categorization

The EDAS system is fed by EGNOS data; it provides, among others, the following functions:

- Allows accepting connection from Users with correct credentials.
- Introduces an additional security layer between EGNOS and the Users.
- Protects EGNOS proprietary protocols and data formats.
- Processes EGNOS data and produces the different products provided through EDAS services.

The interface with the Users is done via Internet or dedicated Frame Relay lines.

6.1.1.1 DATA AVAILABLE FROM EDAS

The data collected by the RIMS network includes dual-frequency GPS data, GLONASS L1, and the EGNOS geostationary L1 SIS. The data collected by the NLES network includes only the GPS data. For each RIMS/NLES and each tracked satellite a set of observables is provided. Therefore, at a given time, information from each RIMS/NLES will be provided with a set of observables from visible satellites. This data is provided by EDAS in real-time with an update rate of one second. Each message contains a variable number of sections (depending on the number of tracked satellites).

EGNOS Augmentation Message, this is the EGNOS augmentation message as uplinked and broadcast from the EGNOS geostationary satellites. The augmentation message from EGNOS has been internationally standardized along with all other space-based augmentation system.

6.1.1.2 EDAS PERFORMANCES

See Table 6 for a summary of EDAS services performance taken from Appendix B, Observed EDAS Performances of [50], where:

- Availability: percentage of time during which the service provides the data according to the specification.
- Latency: average of the percentile 96% latencies monitored for every 5 minutes period within the month.

EDAS Service	Jan 2014	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	July 2014	Aug 2014	Sept 2014
SL 0	99.95%	99.99%	100.00%	99.99%	100.00%	99.32%	100%	100%	99,93%
SL 2	99.95%	99.99%	100.00%	99.99%	100.00%	99.30%	100%	100%	99,89%
Ntrip Service	99.13%	99.96%	99.99%	99.96%	99.46%	99.41%	99.98%	100%	99,69%
SISNET									
SISNET GEO1	99.36%	99.38%	99.45%	99.29%	99.39%	98.58%	99.14%	99.26%	98.92%
SISNET GEO2	99.33%	99.41%	99.38%	99.25%	99.49%	98.27%	98.06%	99.25%	99.05%
Data Filtering Service									
DF RIMS A	99.93%	99.98%	99.98%	99.93%	99.96%	99.26%	99.96%	99.96%	99.82%
DF Central	99.93%	99.98%	99.97%	99.93%	99.96%	99.24%	99.95%	99.98%	99.81%
DF MEDA	99.93%	99.96%	99.97%	99.92%	99.96%	99.24%	99.95%	99.94%	99.81%
DF NorthEast	99.93%	99.97%	99.97%	99.92%	99.96%	99.24%	99.93%	99.96%	99.82%
DF NorthWest	99.93%	99.96%	99.97%	99.94%	99.96%	99.25%	99.97%	99.98%	99.81%
DF SouthWest	99.93%	99.98%	99.97%	99.92%	99.96%	99.26%	99.95%	99.91%	99.80%
FTP Service	99.35%	99.49%	99.85%	99.95%	99.87%	98.40%	100%	99.96%	99.76%

Table 6. Availability of EDAS services

EDAS Service	Jan 2014	Feb 2014	Mar 2014	Apr 2014	May 2014	Jun 2014	July 2014	Aug 2014	Sept 2014
SL 0	554.10	539.54	528.87	525.53	531.10	529.17	539.77	532.87	501.01
SL 2	559.42	543.93	532.94	529.63	534.77	533.83	544.58	539.77	542.43
Ntrip Service	931.26	255.57	256.97	336.83	391.23	262.23	267.84	246.97	246.57
SISNET									
SISNET GEO1	323.90	262.25	175.61	249.37	133.32	72.50	314.68	300.71	315.77
SISNET GEO2	331.32	253.00	167.39	241.17	135.58	72.53	308.74	301.52	318.10
Data Filtering Service									
DF RIMS A	502.23	489.14	502.48	569.13	548.71	507.30	581.39	2174.42	1017.57
DF Central	584.20	452.60	428.17	477.62	486.83	431.14	902.47	1369.03	946.79
DF MEDA	597.90	482.76	482.87	530.63	537.77	479.4	934.19	712.61	835.3
DF NorthEast	187.03	184.67	200.19	249.53	251.42	201.53	747.9	1545.45	818.4
DF NorthWest	457.26	444.57	460.90	527.80	520.45	492.97	780.03	2109.77	985.5
DF SouthWest	644.32	498.48	504.77	575.10	554.42	498.53	580.68	2173.26	444.00

Table 7. Latency (ms) of EDAS services

To put the data from the above two tables into context, the availability and latency figures are shown on the high level architecture diagram below.

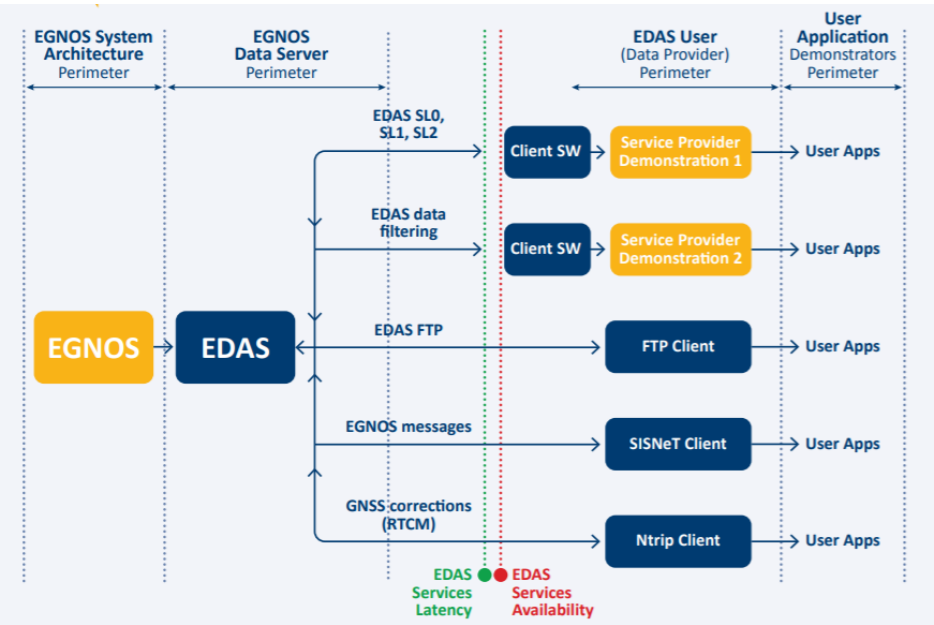

Figure 6-2. Performance measurement point

6.1.1.3 EGNOS DATA SERVICE APPLICATION IN THE RAILWAY DOMAIN EDAS-R

A simplified railway signalling deployment is shown below in Figure 6-3. The RBC is the wayside link to the on-board signalling equipment according to the Euroradio standard [51]. The communication link also will provide the bearer for the EGNOS augmentation, integrity and alerts to the train as to reutilize the functionality that is already there for train control signalling.

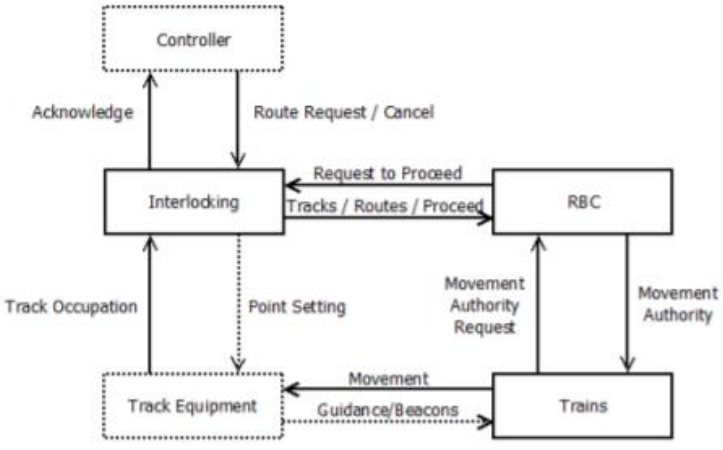

Figure 6-3. Simplified railway signalling deployment

As shown in Figure 6-2, the availability and latency figures are relevant from the CPF to the EDAS external DNS server. Between the EDAS external DNS and the railway external IP the data will have to travel over an open network, even if that is over dedicated direct connections and services. The ETCS specification defines what is required from an open network in order to fulfil the CENELEC requirements according to the functional allocation for the RBC-RBC Safe Communication Interface [49]. RBC/Interlocking and RBC/RBC communication is made by reusing the UNISIG Euroradio Safety Layer within the safe transmission architecture (see Figure 6-5).

If we consider that the user external IP as shown below in Figure 6-4 is at the RBC (for reference to a railway signalling layout see Figure 6-3) in a railway site, then the CENELEC requirements necessitate that the architecture for safe communication (Figure 6-5) is distributed at either side of the TCP connection shown in Figure 6-4.

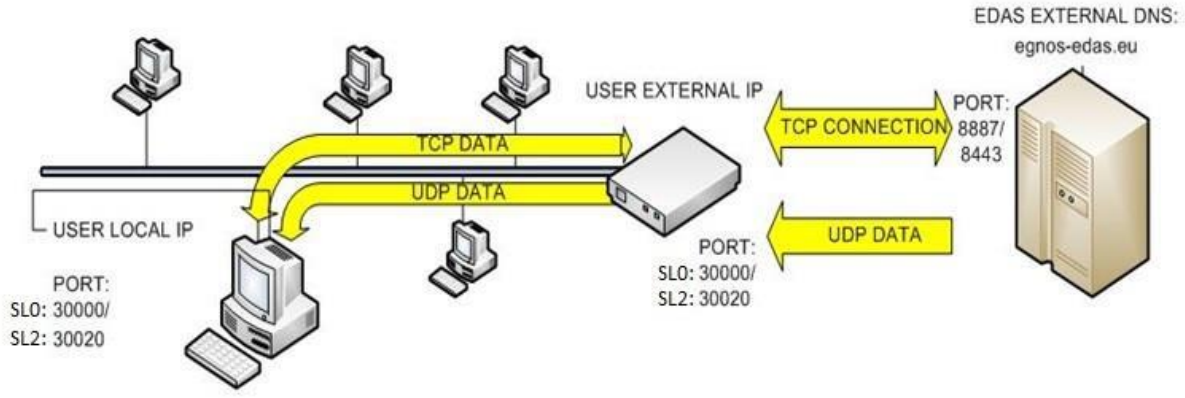

Figure 6-4. EDAS to user physical architecture

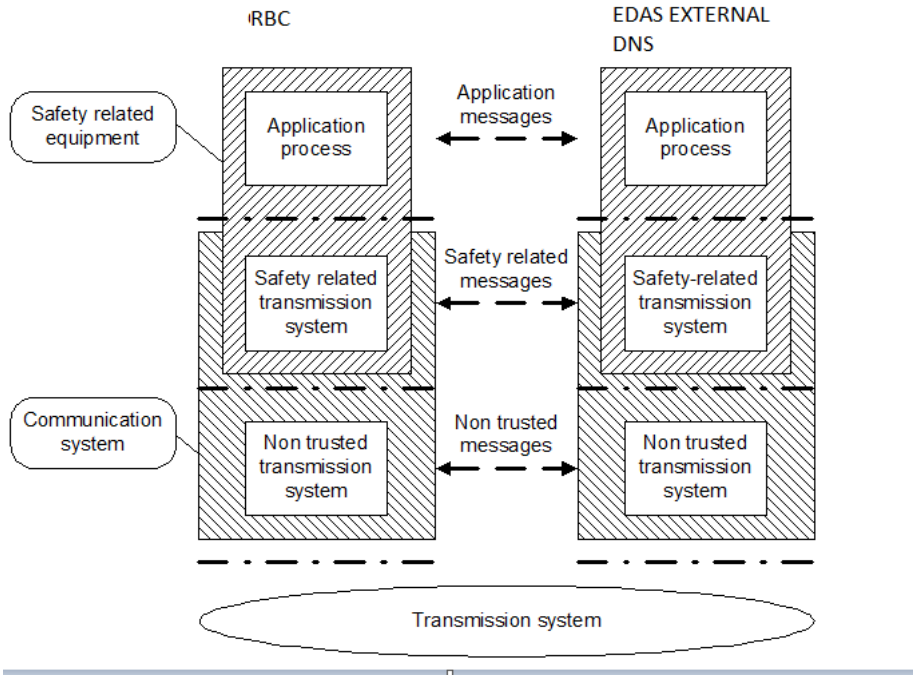

Figure 6-5. CENELEC safe transmission architecture

Implementing the CENELEC safe transmission architecture enables an open network to fulfil the requirements for:

- Message authenticity (origin and destination)

- Message sequence integrity
- Message integrity
- Reporting of safety relevant errors
- Configuration management (of the RBC-RBC safe communication protocol stack)
- Access protection
- Reliable, transparent and bi-directional transfer of data
- Retransmission of protocol data units, if necessary
- Monitoring of channel availability

Missing from the above are timeliness of data delivery for ensuring sufficient system mitigation arising for TTA and other alerts and redundancy of communications in order to fulfil subset-098 requirements.

Redundancy of communications bearer will need to be addressed and could be mitigated by having EDAS data connections to more than one EDAS data source-CPF (see EDAS architecture).

Ensuring timeliness of data delivery is a much more complex challenge as latencies with the TCP network (Figure 6-4) are difficult to quantify. The source of the EDAS data could be separated from the destination by several physical communications networks that would make specification of performance requirements difficult to define and to govern. A country or region wide network of CPF facilities distributing EDAS data could help to alleviate some of these issues.

6.2 EDAS-R Minimum Service Performances

EDAS-R should be intended as the next generation of EGNOS via EDAS, service provisioning for railway of SoL service providing integrity data through the EDAS interface, in order to meets the requirements imposed by the rail environment.

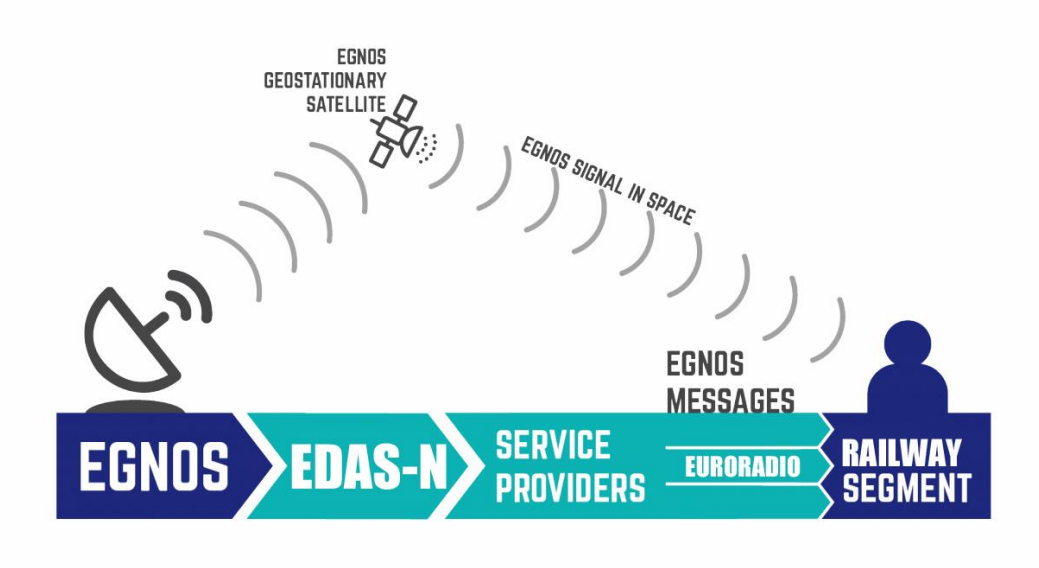

Figure 6-6. EDAS-R concept

6.2.1 Availability

The availability performance that shall be expected from EDAS-R in the railway scenario is 99%[9]. For similarity with the aeronautical environment, this value correspond to the expected minimum performance measured by a fault-free avionics application receiving EGNOS data using all the operational EGNOS GEOs.

6.2.2 Safety and Security

This section provides a security analysis of the communication layer of the proposed EDAS-R service with security recommendations that can be considered for improvements in the short-term evolution.

Security attacks may invalidate many of the safety assumptions that are based on the analysis of system failures rather than security concerns. However, the inclusion of a combined safety-security risk based methodology for the identification of attack scenarios would improve the efficiency and completeness of the design since:

- It would cover a wider range of hazard considering not only system failures but also directed security attacks.
- It would avoid duplicated/overlapping barriers that might otherwise waste resources if security and safety analyses were to be performed independently.

A number of threats have been identified for Global Navigation Satellite Systems (GNSS) infrastructures. These include denial of service attacks on elements of the ground-based infrastructures. Other concerns focus on data integrity and vulnerabilities to insider attacks. A security assessment must also consider a number of spoofing mechanisms.

6.2.2.1 Analysis of the Security mechanisms

As in the European railway signalling system, ERTMS, the Euroradio safety layer provides a secure data exchange, between RBC and EVC, by protecting delivery data in terms authentication and integrity, similarly EDAR-R (through an EURORADIO like protocol) should provide a secure way to exchange the data between EDAS and RBC considering the cyber security threats explained on the taxonomy of cyber-attacks on the IT domain presented in section 4.2.4.

Table 8 summarizes the potential cyber-attacks and their feasibility. It also ranks security risks using estimated values for likelihood of occurrence and impact of each attack on the network.

Attack type	Means	Knowledge needed	Detection capability	Occurrence likelihood	Impact	Risk level
Passive	Eavesdropping	Medium	Low	Possible	Low	Minor
Active	Jamming	Low	High	Likely	Medium	Critical
Active	Spoofing	High	Medium	Possible	High	Critical
Active	Flooding replay attacks	High	High	Possible	Medium	Major

Table 8. Review of potential attacks

[9] Indicative value subject to verification, based on the preliminary outcome of the EDAS-N Service Analysis project for the defined services.

https://ec.europa.eu/growth/sectors/space/research/horizon-2020/edas-n_en

6.2.2.2 EURORADIO SYSTEM DESCRIPTION

The security of Euroradio is achieved by calculating a cipher block chaining-message authentication code (CBC-MAC).

The CBC-MAC algorithm is based on the Triple Data Encryption Standard (3DES) and is defined in subset-037 v.3.1.0 of the ERTMS specification. The key material used in Euroradio is exchanged through a key management system (KMS) protected by different key materials. The ERTMS uses four different keys, which can be categorized in three levels. Table 9 summarizes this key material, including the entities that make use of each key and their functions.

Key name	Key size	Functions	Entities involved
Level 3: K-KMC	384 bits	Encryption, authentication and integrity	KMC-KMC[10]
KTRANS	384 bits	Encryption, authentication and integrity	KMC-RBC[11]KMC-OBU[12]
Level 2: KMAC	192 bits	Authentication and integrity	OBU-RBC
Level 1: KSMAC	192 bits	Authentication and integrity	OBU-RBC

Table 9. Summary of key material used in ERTMS

Session keys, KSMACs, are generated from the authentication key material, KMAC, for each session. This procedure is described in detail in subset-037 and can be summarized in the following two steps:

- Exchange two random numbers in plain text between two entities.
- Perform the 3DES-CBC-MAC algorithm three times, using these two random numbers as seed material and three blocks of 64 bits taken from KMAC as keys.

The key material in ERTMS is generated by the KMC, with the exception of KSMACs, which are negotiated for each session between ERTMS entities. Each ERTMS entity must have a valid KMAC shared with other ERTMS entities for establishing safe communication. In order to ensure the secure distribution of KMAC keys from the KMC to ERTMS entities and to other KMCs, transport keys (K-KMC and KTRANS) are used to provide confidentiality, authentication, and integrity. Half of the transport key is used for confidentiality by performing 3DES ciphering, and the other is used for authentication and integrity by calculating a CBC-MAC code.

The key distribution methodology, illustrated in Figure 6-7, is based on messages defined in Subset-114 v.1.0.0 of ERTMS specification. These messages are exchanged through an offline mode, using physical storage devices such as USB sticks or CDROMs.

[10] KMC: key management center

[11] RBC: radio block center

[12] OBU: on-board unit

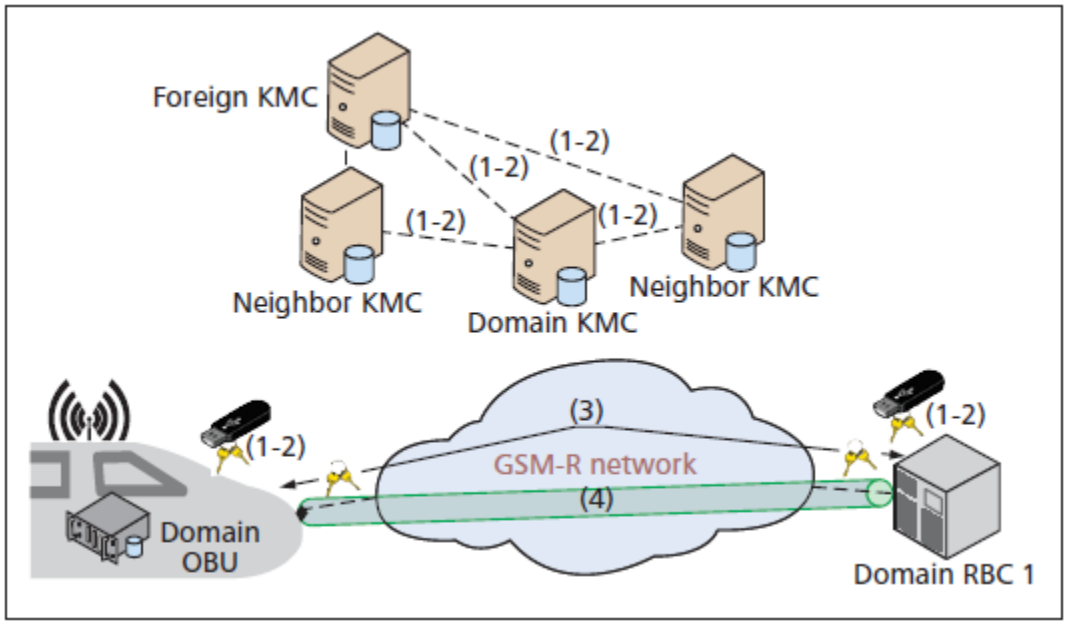

Figure 6-7. Current key distribution system in ERTMS: 1) KTRANS and KKMC keys distribution; 2) KMAC keys distribution; 3) KSMAC derivation from KMAC; 4) safe communication using KSMAC

6.2.2.3 POTENTIAL SECURITY RECOMMENDATIONS

With the aim of increasing the security and ensuring the ability to counteract attacks not considered, are proposed four main security recommendations.

1) **Symmetric ciphers vs. asymmetric ciphers**. In symmetric cryptography, since both parties involved in the communication must know a secret key, the weakness of the system depends on a correct and secure key exchange process. On the contrary, in asymmetric cryptography different keys are used for encryption and decryption, one of them public and the other private. Generally, this scheme is considered to be more secure and more suitable for communication between entities that do not know each other in advance. This is the case in broadcast communications. However, this is not the case in the railway environment, where the entities participating in the communication exchange are strictly controlled. Moreover, asymmetric schemes require more processing than symmetric ones. Thus, taking into account the real-time constraints, the optimal solution in the railway context is the use of symmetric cryptography for authentication and integrity. However, for the key exchange and negotiation processes, the use of asymmetric schemes is the most appropriate.

2) **Authentication and integrity codes**. Two of the most commonly used codes for providing authentication and integrity with a shared key are the CBC-MAC and hash-based MACs (HMACs). The first scheme uses a CBC process with a random initialization vector (IV), whereas the second is based on hash functions. The most popular algorithms that use both techniques are the CBC-MAC with AES and Secure Hash Algorithm (SHA-1) algorithms. It is worth noting that CBC-MAC-AES performs noticeably faster, especially when small packets are used —which is the case for EGNOS — due to the overhead generated by HMAC-SHA-1. Additionally, due to the collision vulnerability discovered in SHA-1, it has been recommended that it be substituted by the new SHA-3 algorithm. However, although this new algorithm is more robust, it generates even larger output than SHA-1 and therefore higher overhead in the communication.

3) **Key size and national recommendations**. Taking into account the computing improvement expected in the near future, national and international security agencies have published

recommendations for choosing the optimal authentication and integrity algorithm and the most suitable key size. We summarize these recommendations in Table 10. The key size determines the robustness of the secure communication. All recommendations made by security agencies state that after 2020, symmetric algorithms should not use a key shorter than 128 bits. Although an even longer key size may seem the best option, it is worth noting that an increment in key size implies an increment in processing overhead. As an example, a 192-bit key size represents an increment of 20 percent in the overhead compared to a 128-bit key size. With regard to the crypto algorithm, the European Network and Information Security Agency (ENISA) as well as the American National Institute of Standards and Technology (NIST) recommend the use of AES in cipherbased MAC (CMAC) mode. CMAC mode is defined in the document RFC 4493 and represents an improvement on the CBC-MAC mode since it solves CBC-MAC problems known to occur when using different size messages. In contrast to the other agencies, the National Security Agency (NSA) recommends the use of SHA.

Standard	Validity date	Symmetric key size	Authentication and integrity algorithm
NIST[9]	>> 2030	192	CMAC or SHA-3
ENISA[10]	> 2030	128	CMAC or SHA-3
NSA[11]: Secret **Top Secret**	-	128 192	SHA-256 SHA-384
RFC 3766	2053	128 192	-

Table 10. National and international recommendations for cryptographic

4) **Key exchange**. The key exchange system introduces the key distribution centre (KDC) element, which is responsible for distributing the keys generated by the KMC over the ERTMS entities (e.g. RBCs), according to UNISIG Subset-137 [32]. For secure distribution of this key material, the proposal suggests the use of transport layer security (TLS) combined with public key infrastructure (PKI) for validating the entities' identity. Introducing a distributed key negotiation scheme based on hybrid cryptography, the KMC takes the role of a certification authority (CA) in PKIs, and its main duty is the generation of valid certificates that will guarantee the identity of the ERTMS entities. Both the public/private key pair and the accompanying certificate generated by the CA are delivered from KMCs to ERTMS entities using online procedures according to Subset-137 [32]. However, once these keys and certificates have been correctly installed, and as long as the certificate has not expired, the ERTMS entity is able to renew both the key pair and the certificate using secure online procedures. However, it is worth noting that, due to the robustness of asymmetric cryptography, this cryptographic material could be valid for years before it needs updating.

6.2.3 Latency

The latency performance that shall be expected from EDAS-R in the railway scenarios may be less than 1s[13].

[13] See note 9.

7 CONCLUSIONS

An approach has been proposed for both evaluating the impact of EGNSS services into ERTMS/ETCS architecture and how implementing/applying the performance requirements usually used in avionics to characterize the EGNOS SoL service in the rail context.

These aspects contribute to define and evaluate the constraints that lead to the definition of the service designed specifically for rail, named EGNOS Rail Service.

To achieve this, as a first step, it was necessary to formalize the performance requirements required to use GNSS and/or EGNOS in the railways. In fact, some concepts traditionally used in avionics lose meaning, while others require being "adapted/re-aligned" in the perspective of the railway application.

Basing on the contextualization of these requirements a preliminary analysis of the parameters that are relevant has been performed (e.g. accuracy, integrity and availability). This represents a valid basis for the investigations to be conducted in the future; in particular, a complete performance analysis could be derived in the context of the S2R TD 2.4 Fail-Safe Positioning project.

After having specified the above mentioned performance requirements, the SBAS service is described as it is conceived today for the aviation, focusing on those aspects that accordingly to the previous analysis are not in line with the railways expectations. In particular the elements at the basis of the SBAS concept are further investigated in order to point out which could be the limitations in the railways adoption of this augmentation.

The preliminary analysis considers also advantages and disadvantages of the possible EGNSS receiver integration inside the ERTMS architecture and which could be the impacts on the present SBAS specifications to match the rail requirements and provides also some recommendations to overcome the present limitations.

In addition to the application, the railway context differs from the avionic one also because it experiences a more complex and different environment. Therefore, the local conditions were strongly impacting in terms of the reception quality of the EGNOS+GNSS signal, and consequently the resulting PVT solution. The analysis of the results carried out in this project showed that:

- The error budget for the railway sector has to be defined in a different way than in the aviation case. It will be crucial and it will have to be investigated in the future for fully predicting the EGNSS performances. The resultant Protection Level will limit the position error, influencing the train confidence interval.
- In addition, fault detection and exclusion techniques will have to be put in place to exclude those events that do not make part of the error budget definition, like RF interferences (not intentional and intentional ones).
- The most suitable communication channel for the acquisition of SBAS corrections is via EDAS (defined as EGNOS Option 3 in D5.3). This brings to the need of defining an EDAS service for the rail, namely EDAS-R Service, that must be conform to a similar form of communication already implemented in the railway sector, such as the RBC-RBC communication.

With reference to the EGNOS Rail Service, the focus was on those EGNOS requirements which can be implemented in the railway context and taking into consideration that. The concept of VB is applicable to the ERTMS/ETCS architecture, where performances and SIL4 are guaranteed by the traditional signalling system, based on odometry and/or additional sensors.

8 ANNEX - EGNOS ARCHITECTURE SUMMARY

8.1 EGNOS ARCHITECTURE

The EGNOS functional architecture is shown below.

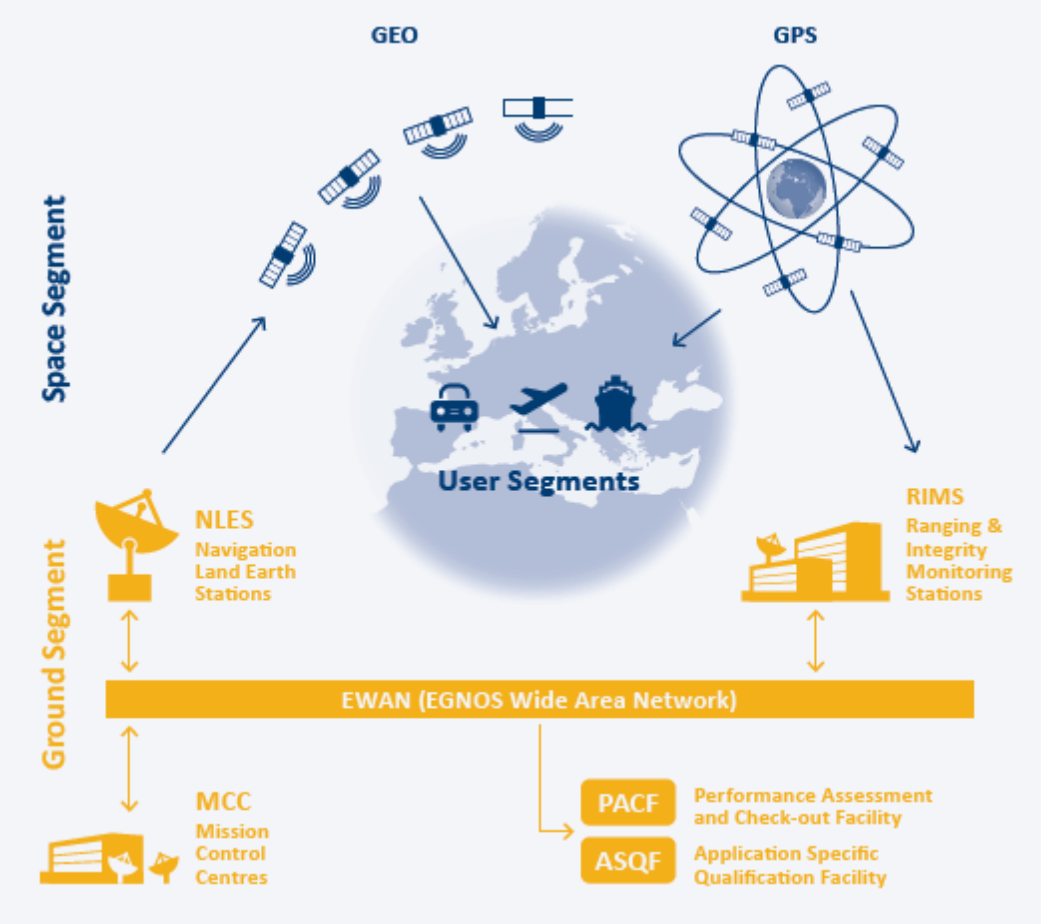

Figure 8-1. EGNOS architecture

8.1.1 Space Segment

The EGNOS Space Segment comprises 2 geostationary (GEO) satellites broadcasting corrections and integrity information for GPS satellites in the L1 frequency band (1575.42 MHz), plus 1 satellite as part of the EGNOS Test Platform broadcasting the TEST SIS [33].

EGNOS GEO Name	PRN Number	Orbital Slot	Status BEFORE 23rd August 2018 (10:00h UTC)	Status ON 23rd August 2018 (10:00h UTC)	Status FROM 30th August 2018 (13:30h UTC)
INMARSAT 3F2	PRN 120	15.5 W	Operational	Operational	Test
ASTRA-5B	PRN 123	31.5 E	Operational	Operational	Operational
SES-5	PRN 136	5 E	Test	Operational	Operational

Table 11. EGNOS GEO space segment

This space segment configuration provides a high level of redundancy over the whole service area in case of a geostationary satellite link failure[14]. The EGNOS operations are handled in such a way that, at any point in time, at least two of the three GEOs broadcast an operational signal. Since it is only necessary to track a single GEO satellite link to benefit from the EGNOS Services, this secures a switching capability in case of interruption and ensures a high level of continuity of service.

8.1.2 Ground Segment

The EGNOS Ground Segment comprises a network of Ranging Integrity Monitoring Stations (RIMS), two Mission Control Centres (MCC), eight Navigation Land Earth Stations (NLES), and the EGNOS Wide Area Network (EWAN) which provides the communication network for all the components of the ground segment. Two additional facilities are also deployed as part of the ground segment to support system operations and service provision, namely the Performance Assessment and Checkout Facility (PACF) and the Application Specific Qualification Facility (ASQF), which are operated by the EGNOS Service Provider.

[14] Ref. GSA official site (https://www.gsa.europa.eu/european-gnss/egnos/egnos-system)

9 ANNEX - SBAS INTEGRITY CONCEPT

9.1 NON INTEGRITY EVENT DEFINITION APPLICABLE TO A SBAS STANDARD USER

If the computed Horizontal Protection Level (HPL) exceed the Horizontal Alert Limit (HAL) for a particular operation, SBAS integrity is not adequate to support that operation. The same is true for precision approach and APV operations, if the VPL exceeds the vertical alert limit (VAL).

More specifically non integrity events occur when the PL is lower than the NSE. Hazardous Misleading information happens when the PL is lower than the AL and the NSE is greater than the AL. In particular if the NSE is higher than the PL but both lower than the AL then a MI occurs.

If the NSE is higher than the PL and the AL while the PL is lower than the AL then a HMI occurs.

HPL and VPL are computed each epoch by the on board SBAS receiver using the information coming from the SBAS GEO link,

This test (HPL or VPL > HAL or VAL), which is implemented at each epoch, allows to declare the SBAS "system unavailable" for a given level of operation since in this case the probability of an MI event is high.

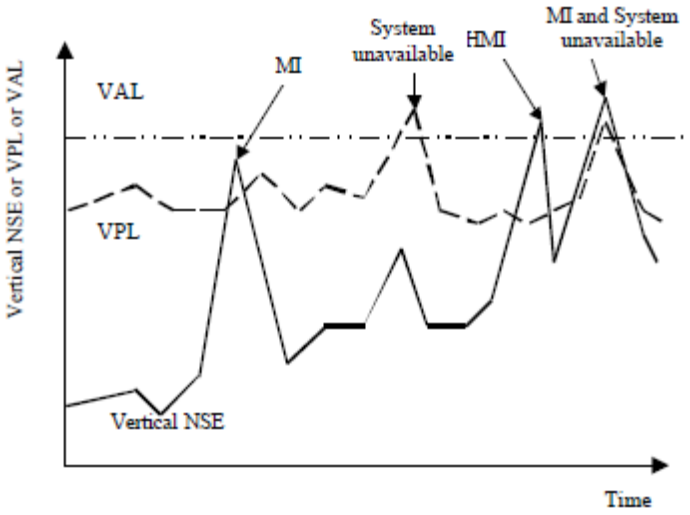

Figure 9-1. Graphical representation of the MI, HMI, system unavailable and MI&system unavailable situations

So this concept foresees the definition of an Alert limit to which comparing the H or V PL and declare if the system is available or not.

In the rest of the text the acronym XPL is used in those cases where the reasoning is applicable for both H and V PL (X stands for H or V).

9.2 GROUND SYSTEM INTEGRITY

Failures from which the aviation user is protected by the SBAS system are:

- Failures on navigation code and data transmitted by GPS/GLONASS satellites (including evil waveforms, i.e. a distortion of the correlation peak that may result in pseudoraneges errors values that may evolve with the correlation technique and characteristic used in the receiver).
- Corruption of data transmitted to the user, through the GEO satellites.

- Failures originating from the ground system hardware, software design or corruption of data through the Wide Area Network connecting the ground elements

The SBAS system cannot protect by local effect (in particular multipath, interference and signal attenuation).

When a failure occurs, the ground segment will provide the appropriate corrections along with the parameters allowing XPL calculation, unless the error gets too large in which case the faulty satellite or Ionospheric Grid Point (IGP) is flagged with a ”don’t use” status

The undetected failures from the ground segment could introduce erroneous data in the transmitted messages. If the integrity requirement is not met, the user will obviously not be protected against such failures by the XPL algorithms.

To fulfil the integrity requirements, the ground system shall reduce the probability of failure of each critical function and shall be able to detect this kind of failures with a global probability of missed detection (Pmd) defined by:

*Integrity risk of an event (probability of missed detection of the ground system) = Prob. occurrence of the event * Prob. impact of that event*

9.3 FAULT FREE CASE INTEGRITY

To protect the user against non-integrity events due to data corrupted by the noise induced by the measurement and algorithmic process when the system is in a nominal state (no GPS/GLONASS/GEO satellite failure, no ground segment/user equipment failure), the ground segment needs to compute two different parameters used in the XPL computation.

1. the variance (sigma UDRE) of a zero-mean normal distribution which describes the user differential range errors (UDRE) for each ranging source after application of fast and long-term corrections, and excluding atmospheric effects and receiver errors
2. the variance (sigma UIRE) of a zero-mean normal distribution which describes the L1 residual user ionospheric range error (UIRE) for each ranging source after application of ionospheric corrections. This variance is determined from the variance (sigma GIVE) of an ionospheric model based on the broadcast ionospheric vertical error (GIVE) at predefined ionospheric grid points.

The other potential errors to affect user integrity in nominal conditions are:

1. aircraft pseudo range errors due to the combination of receiver and aircraft multipath (ground multipath is not considered here). This error is well characterised in the **aviation domain** by a zero mean normal distribution whose variance sigma air is given by the sum of SARPs modelled variance of receiver and aircraft multipath error.
2. The residual pseudo range error of a tropospheric correction model, characterised by a variance sigma tropo which is defined by a standard model in the SARPs

Since all these individual pseudo range errors are supposed to be characterised by independent, zero mean, normal distributions, the global residual pseudo range error for the i-th ranging source (sigma i) may also be characterised by a zero mean normal distribution whose variance is:

$$\sigma^2_i = \sigma^2_{i,flt} + \sigma^2_{i,UIRE} + \sigma^2_{i,air} + \sigma^2_{i,tropo}$$

Here the subscript flt refers to fast and long term corrections (including the UDRE terms above introduced) while the subscript air refers to the multipath contribution to the total error.

Sigma UIRE represent the contribution of the L1 residual user ionospheric range error.

From the above equation, and for a given user to ranging sources geometry, the protection level (XPL) equation is derived in two steps:

1. translate from the pseudo range variance domain through the position variance domain (this is necessary because the integrity definitions are all in the position domain)
2. scale the position domain variance to the integrity requirement.

The first step is straightforward since it is well known that the position domain residual error can be considered as a linear combination of pseudo range errors used in the navigation solution (this in the hypothesis of considering the least square error algorithm defined by the MOPS). Therefore, the variance in the position domain residual error is a linear combination of sigma^2 and is also representative of a zero mean Normal law:

$$\sigma^2_{Vposition} = \sum_{i=1}^{N} s^2_{V,i}\sigma^2_i$$

Where Sv are the terms for the Geometry conversion from range to vertical position.

The second step is obtained by multiplication of the position domain variance by a factor K that propagates this variance to a level compatible with the integrity requirement. For example, the VPL equation is then simply

$$VPL_{SBAS} = K_V \sqrt{\sum_{i=1}^{N} s^2_{V,i}\sigma^2_i}$$

9.3.1 Derivation of K factors for XPL computations

First it is important to note that the probability of missed detection of a MI event associated to the XPL algorithm (PmdXPL) has to be expressed per sample (per each XPL computation).

If there are n independent samples/operation, and the integrity requirement for this operation is 10-x, the Pmd to be specified for the XPL will be:

$$Pmd_{XPL} = 10^{-x}/n$$

Where n is the number of samples/operations in the period of observation (e.g. one hour in the case of NPA).

Therefore in order to establish the appropriate value of K, it is necessary to first determine the number of independent samples per time unit. Originally 360 s has been adopted as a reasonable assumption for sampling period to ensure independence.

For example for En route to NPA the Integrity risk requirement 0.5.10-7/h therefore:

Integrity req=0.5.10-7/1 h so PmdHPL = 0.5.10-7 * 360 / 3600 ~ 5*10-9 per sample (integrity risk is considered over 1 hour=3600 sec)

10 ANNEX - GNSS CERTIFICATION PROCESS

The purpose of this section is to help the rail navigation community standardize its use of GNSS for safety-critical applications by making use of the procedures and techniques developed by civil aviation. The path laid out by the civil aviation standards documents described herein is suitable for application to rail navigation, with the key differences relating to technical aspects of how GNSS is applied in civil aviation vs. rail navigation. This document describes the key features of the aviation approach to GNSS standardization that are most useful to rail navigation as well as highlighting a few important differences

10.1 CERTIFICATION IN AVIATION

The EGNOS service provider is certified as an Aviation Navigation Service Provider (ANSP) under the Single European Sky (SES) legislative framework (SES EC 549/2004). The certified service provider is responsible for the system, operations and maintenance of the system, ensuring that the specified navigation service is delivered.

More specifically, the service provision regulation (SES EC 550/2004) applies to the EGNOS service provider as an ANSP, and the interoperability regulation (SES EC 552/2004) applies to the EGNOS system design and operation [30].

10.2 OVERVIEW OF GNSS AVIATION STANDARDS AND REQUIREMENTS DOCUMENTS

This section reviews the standards and requirements documents that have been developed or modified to cover the use of GNSS in safety-critical civil aviation applications. As with railways, most of the applications to which GNSS has been applied already existed in some form before standards for their use with GNSS were developed. Thus, in some cases, existing standards documents were modified or expanded to include the use of GNSS, and in other cases, new GNSS-specific standards documents were developed.

Where GNSS standards have been developed to support existing aviation applications, these standards have focused on the implementation of GNSS within the existing application context rather than attempting to alter it or provide new overarching requirements. For example, for precision approach under instrument landing conditions, GNSS is a sensor that provides position information in the format used by existing pilot displays and autopilot control laws. This format is the angular offset (relative to localizer and glideslope) provided by the pre-existing Instrument Landing System (ILS). Since GNSS position outputs are in Cartesian coordinates (e.g., North, East, Vertical), they must be converted to angular coordinates given knowledge of the desired lateral and vertical path. Parameters describing the desired paths for each GNSS-capable approach are either stored on-board the aircraft or broadcast to it from the ground subsystem. In general, a clear boundary between existing (and unchanged) equipment and new GNSS functionality is defined and maintained throughout GNSS standards documents.

10.2.1 ICAO Standards and Recommended Practices (SARPs)

The International Civil Aviation Organization (ICAO) is a component of the United Nations that develops and issues standards and requirements that are applicable to the entire world. Most nations that participate in civil aviation support and take part in ICAO to insure that requirements on aircraft, ground systems are as compatible as possible (“harmonized”) across countries and regions. Requirements harmonization is key to allowing, for example, an aircraft designed and built in North America to fly to Europe and Asia and execute the same flight phases without needing additional or specialized equipage. ICAO standards documents are known as “Standards and Recommended Practices” or “SARPs” and typically cover all components needed to support operations, such as both airborne and ground subsystems.

The ICAO SARPs document most relevant to GNSS safety-of-life applications is [15], which covers all radionavigation aids for aircraft and is known in shorthand as “Annex 10.” Applications of different

elements of GNSS have been progressively added to Annex 10 as they have been developed, starting with the standalone use of GPS and progressing to SBAS, GBAS, and (in progress) new constellations such as GLONASS and Galileo. The SARPs included within Annex 10 has two sections. The first represents requirements and standards which are expected to be met by all nations and airborne service providers (such as the U.S. Federal Aviation Administration, or FAA), while the second includes guidance material which is expected to be followed in general but which provides some flexibility to individual service providers in the details. In many cases, and especially with the more complex services provided by SBAS and GBAS, the guidance material becomes lengthy and is needed to fully understand the meaning and impact of the requirements in the first section.

10.2.2 RTCA and EUROCAE Standards

ICAO SARPs development takes place over many years of meetings and discussions hosted by ICAO (based in Montreal, Quebec, Canada) and supporting organizations. Delegates to these meetings are representatives of their nations and are often high-level policy makers and managers at private companies. As a result, ICAO SARPs requirements and guidance material are often first developed by other independent, non-profit standards bodies that invite participation from all interested parties. These standards bodies include Radio Technical Commission for Aeronautics (RTCA, based in Washington, DC, USA) and the European Organisation for Civil Aviation Equipment (EUROCAE, based in Lucerne, Switzerland).

As with ICAO, RTCA and EUROCAE divide their subject matter into subgroups focused on different technologies related to civil aviation. At RTCA, “Special Committee” (SC) 159 is the one that has the most responsibility for GNSS-based systems, and it is broken down into smaller working groups (WGs) focused on different applications. For example, SC-159 WG 2 has been responsible for SBAS requirements development, and the same is true for SC-159 WG 4 for GBAS (called “LAAS” by RTCA).

The approach taken by SC-159 WG 4 for GBAS is instructive in that three separate standards documents have been developed, following standard RTCA practice. The first is known as the “Minimum Aviation System Performance Standards” or MASPS [16]. As a top-level document, it covers the GBAS ground and airborne subsystems at a high level and sub-allocates performance and risk requirements to these subsystems. Both ground and airborne subsystem manufacturers are present to help influence the proper sub-allocation of these requirements, which is difficult to change once initially laid out in the MASPS.

Separate and more-detailed requirements on both the ground and airborne subsystems can flow from the MASPS, but in the case of GBAS and most RTCA projects, only an airborne standard was produced because the ground standard was effectively created by the development of a (MASPS-compliant) ground system specification by the FAA. RTCA airborne standards documents are known as “Minimum Operational Performance Standards,” or “MOPS,” and [17] was developed to serve this role for GBAS. In parallel with the MOPS, an Interface Control Document (ICD) specifying the physical characteristics and message content of the VHF Data Broadcast from ground to airborne subsystems was developed [18]. Both the MOPS and ICD for GBAS have been updated several times (most recently in mid-2017) to incorporate improvements and additional functionality (e.g., CAT II/III precision approach), and they are now the primary focus of the GBAS working group (as opposed to the MASPS, which has not been updated since 2004). In Europe, a slightly different approach was taken, and a GBAS ground system standards document was developed by EUROCAE [19] to attempt to harmonize requirements among different service providers in Europe.

The approach taken by SC-159 WG 2 for SBAS appears to be different but actually provides similar standards guidance. By the time that RTCA activity on SBAS (first focused on the FAA variant known as WAAS) got underway, the FAA had already laid out the WAAS system design and requirements allocations between ground and airborne subsystems. Therefore, an RTCA MASPS would have been superfluous. Instead, RTCA developed a MOPS [20] that includes the ICD within it and explains

in detail how to use each of the message types broadcast in the (already designed) datalink transmitted by GEO satellites. As with GBAS, this MOPS document has been updated several times, most recently at the end of 2016.

Thus, while different sets of standards documents have been developed by RTCA and EUROCAE to cover GBAS, SBAS, and other aviation applications of GNSS, the same elements are addressed in each (or referenced to other documents): top-level system standards, ground subsystem requirements (where augmentation is needed), airborne subsystem requirements, and a ground-to-airborne ICD (where needed). In addition, several key integrity and continuity requirements validation techniques are commonly used in these standards. The ones of greatest utility to rail navigation are described in the next section.

10.3 PRINCIPLES FOR ACCEPTANCE OF EGNOS FOR USE IN ERTMS

One possible approach for certifying the use of EGNOS in ERTMS is through a cross-acceptance process [29]. The cross-acceptance would need to focus on two aspects: the acceptance of the certificate granted by the competent authority to the air navigation service provider; and acceptance of the performance guaranteed by the service provider (this would be through an EC Service Definition Document for Railway SoL Services).

It is recommended that an assessment of the feasibility of this approach is undertaken, taking into consideration the points outlined in the following subsections.

10.3.1 Acceptance of Certificate granted by competent Authority to Service Provider

In order for a service provider to obtain the necessary certificate for providing air navigation services, they are required to comply with the following (common requirements for the provision of air navigation services):

- General requirements for the provision of air navigation services;
- Specific requirements according to the type of service provided;
- A competent authority is required to verify an organisation's compliance with the common requirements before issuing a certificate to it;

10.3.2 Acceptance of the performances guaranteed by the Service Provider

It is foreseen that ERA, or initially a railway NSA, would accept the performances guaranteed by the service provider through a Service Definition Document for Railway SoL Services, published by the EC.

The EC declaration of verification of System for Air Navigation Services should demonstrates the compliance with the ICAO Standards and Recommended Practices (SARPs) for Aeronautical Telecommunications (Annex 10, Volume 1, Radio Navigation Aids)

In order to ensure applicability of the EC declaration of verification to the railway SoL service, a reinterpretation of the SARPs applicable for railways would be required, ensuring that there is no deviation on requirements for SBAS, i.e. consistent with the principle of using EGNOS as-is. The reinterpreted SARPs would need to be developed by industry and accepted by ERA.

Figure 10-1 illustrates the relationships and dependencies in the described approach.

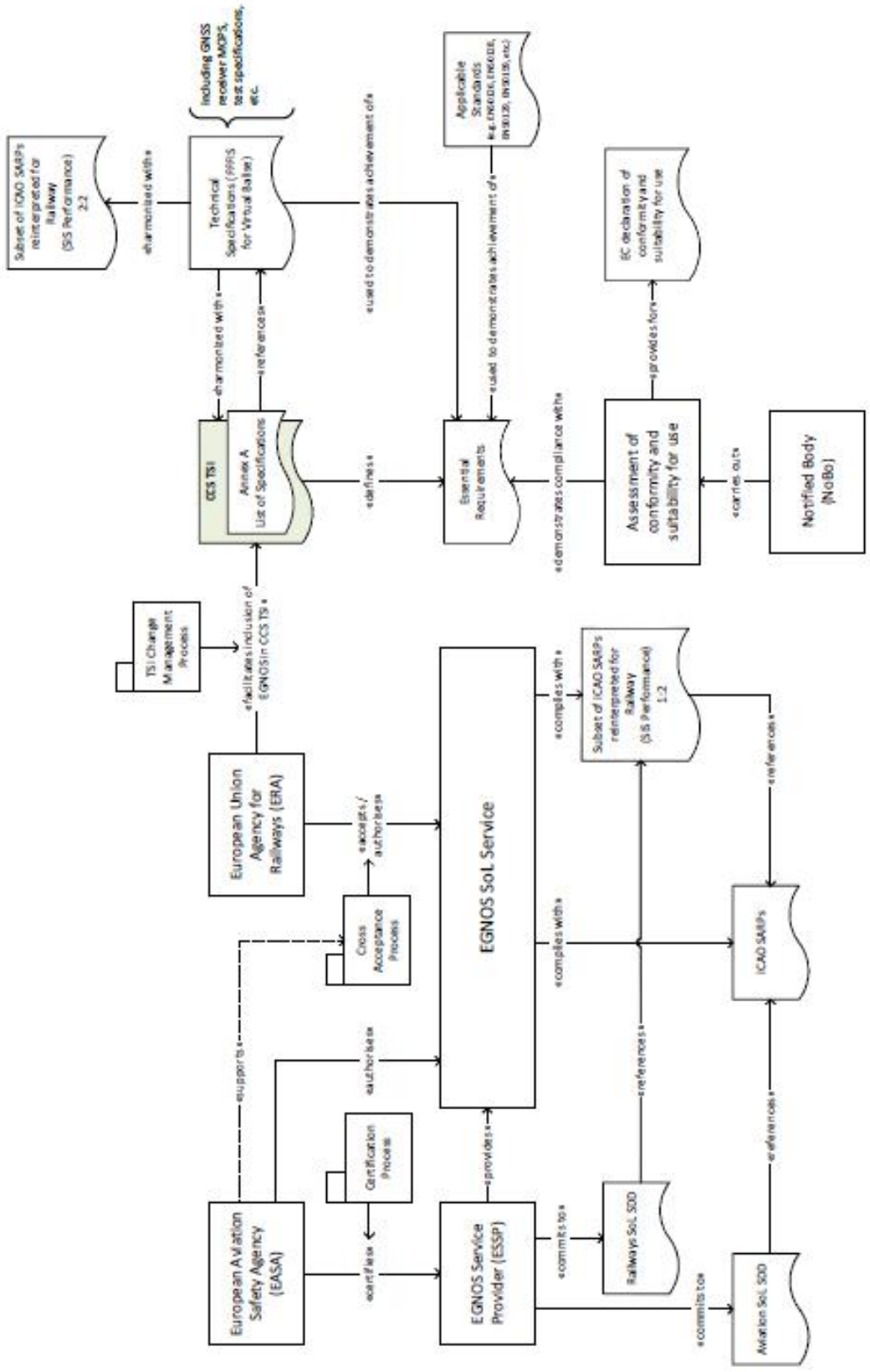

Figure 10-1. High-level certification approach

10.4 AVIATION REQUIREMENTS VALIDATION TECHNIQUES

10.4.1 Integrity and Continuity Fault Trees

A standard approach to hazard risk assessment is to sub-allocate the allowed risk into the possible hazard causes and then assign a probability to each while demonstrating that mitigations exist for each cause so that each sub-allocation is met and, therefore, the total hazard risk requirement is met. These allocations are commonly performed and documented by fault trees. In civil aviation requirements, fault trees are used to sub-allocate and demonstrate compliance with both integrity and continuity risk requirements.

Figure 10-2 is an illustration of the system-level integrity fault tree proposed for the GBAS application to CAT I precision approaches in the RTCA MASPS of 2004 [16]. It starts with the overall CAT I integrity risk requirement and sub-allocates it among the sources of integrity risk: loss of integrity under nominal conditions (H0), loss of integrity due to a single ground reference receiver fault (H1), and all other fault cases (not H0 nor H1). Because the former two categories are easier to model and bound using protection level equations, only 25% of the total integrity risk was allocated to them, while the remaining 75% was allocated to a host of satellite faults and atmospheric anomalies that are not so easily modelled or bounded. In GBAS, one of the satellite faults (ephemeris) is bounded by a specific protection level equation, thus a specific sub-allocation to it was required, but the sub-allocation among the other “not H0 nor H1” fault conditions was

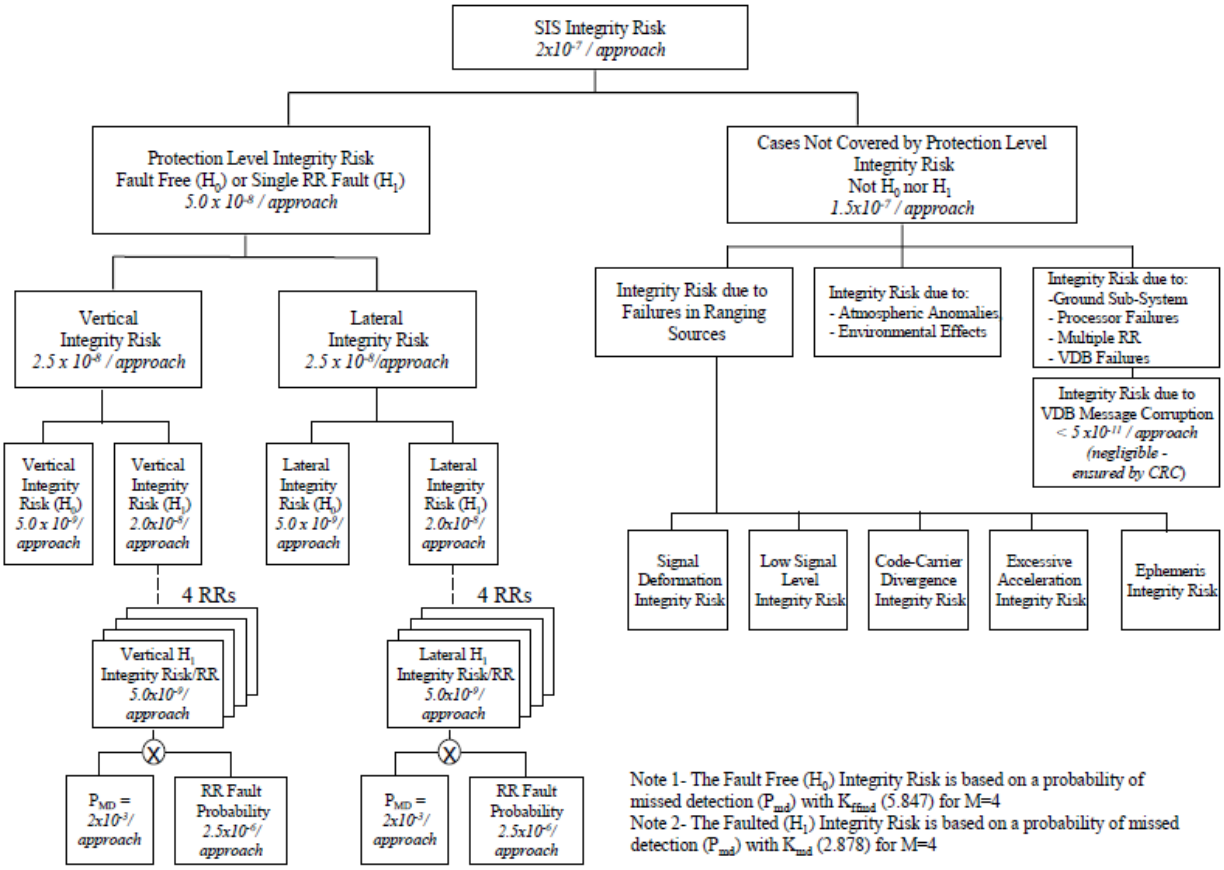

Figure 10-2. GBAS CAT I System-Level Integrity Fault Tree from RTCA MASPS (DO-245A, 2004)

left to each ground subsystem manufacturer (this changed over time as more specific requirements were created to bound the effects of these conditions).

Figure 10-3, also from the 2004 MASPS [16], shows a proposed (not mandated) allocation of the CAT I (also known as “GSL C”) continuity risk requirement, meaning the risk that an operation would need to be aborted unexpectedly. Most of this risk comes from what is called a “configuration change”, meaning the loss or removal of one or more satellites that causes the protection level computed at the airborne to suddenly exceed the allowed safe level (known as the “alert limit”) when it did not before. This can be caused by reference receiver failures, fault-free alerts in ground monitoring (in which the ground subsystem unnecessarily excludes a healthy satellite), or actual satellite failures. A satellite whose exclusion (due to either actual failure or fault-free alarm) leads to the protection level exceeding the alert limit where it did not before (with the satellite included) is known as a “critical satellite.”

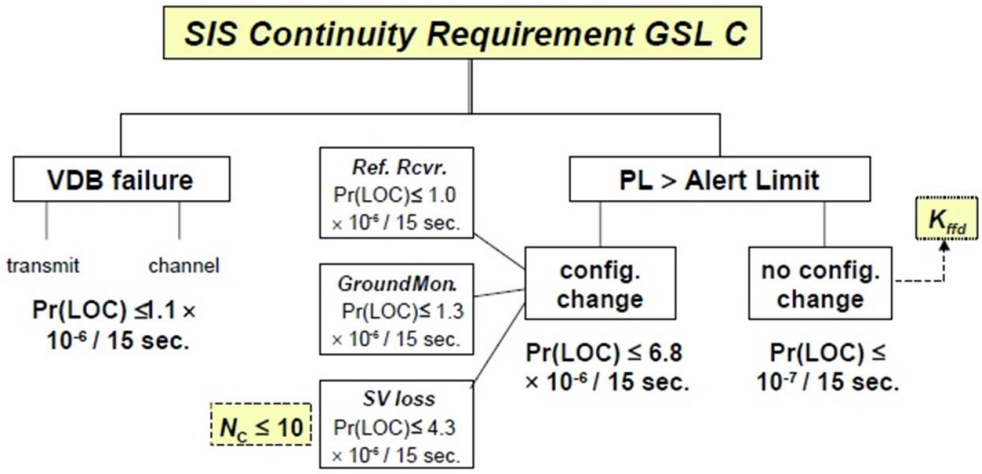

Figure 10-3. Example GBAS CAT I System-Level Continuity Fault Tree from RTCA MASPS (DO-245A, 2004)

Protection levels, which are the key to verifying GNSS user integrity in real time, must bound errors under anomalous as well as nominal conditions. Bounding errors under nominal conditions to the very low probabilities required is not easy, but large samples of measured data can be collected. Anomalous conditions occur rarely by definition and thus are hard to limit solely based on the statistics of empirical data.

The approach taken by GNSS applications in civil aviation is to build “threat models” (TMs) for each faulted or anomalous condition that is of non-negligible probability and may lead to unbounded errors exceeding the alert limits for a given application. No official methodology for developing threat models exists, but Figure 10-4 from [21] illustrates the concept and its application. Each threat model is composed of a simplified mathematical model with a relatively small set of parameters that represents the essentials of each threat condition without trying to capture all possible variations in detail (since these are generally unknown).

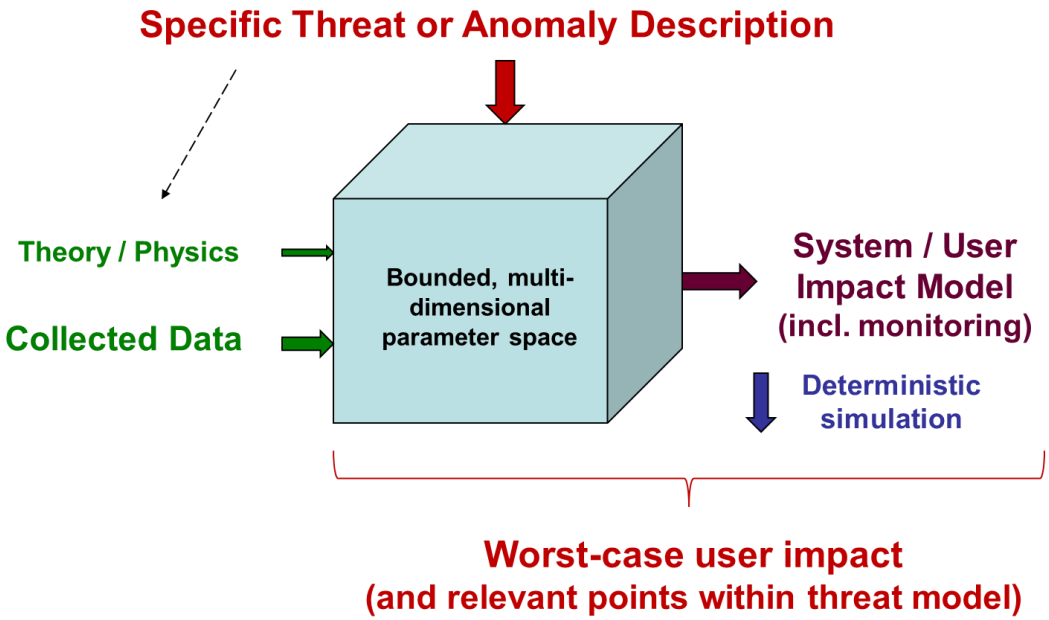

Figure 10-4. Threat Model Development and Utilization Concept

A combination of whatever theory and observed data are available is used to generate the form of this model and bounds on each of the numerical parameters. Events that have been observed and confirmed (e.g., by comparison among multiple parties) in the past, once reduced to the framework of the simplified model, must be included within these bounds, and reasonable margin for variations in these events and measurement error should be added. The resulting bounded set of faults or anomalies is represented by the green box in the centre of Figure 10-4, and the resulting threat model is comprised of the mathematical model driven by all combinations of parameters that fall within this box.

The impact of the threat model on GNSS user performance is assessed either analytically or by simulation in which all possible parameter combinations are exercised. In most cases, each parameter combination is assigned the same prior probability of occurrence as the event for which the threat space is designed. In other words, the overall event probability is not further divided up among the possible parameter combinations unless there is strong reason to believe that the particular combination of parameters that occurs is random and unknowable (this is one of the principles of the “specific risk” approach used in aviation integrity assessment – see [22]. As a result, every point (combination of parameters) within the threat model must be shown by analysis or simulation to meet the integrity requirements sub-allocated to this fault or anomaly condition, assuming that the prior probability that applies to the condition as a whole applies to each point within it.

The consequence of this approach to threat model assessment is that a search is conducted over all points within the threat model to find any that violate the integrity requirements. An integrity violation means that the probability of producing unsafe errors (exceeding either the protection level or the alert limit, depending on the fault-tree layout) after mitigation by ground and airborne monitoring exceeds the sub-allocated integrity risk in the fault tree. If such points exists, a subset of them typically is “worst” or hardest to mitigate with the existing design, and design focus is naturally placed upon them.

Because of the limited information present when threat models for faults and anomalies are created, bounds on the parameters that describe them must be conservative to minimize the possibility that possible conditions are not excluded. (Note that conditions outside these bounds need not have zero probability, but their probability must be small compared to the integrity risk allocation to this fault

hypothesis.) However, this conservatism sometimes leads to subsets of unusual parameter combinations that violate the integrity requirements. It is not always possible to reduce this conservatism over time, as unusual events that have been observed even once in the past cannot be excluded later if they do not recur. Despite this, continued observations of faults and anomalies that play important parts in the integrity validation of a particular system or application are needed to check against “negative surprises” (new events that violate previous assumptions) as well as collecting experience that, over time, may allow the safety community to reduce its level of conservatism regarding particular rare-event assumptions.

11 REFERENCES

[1] STARS Grant Agreement, Annex I - "Innovation Action", 25th of November 2015.

[2] STARS Consortium Agreement of 6th November 2015.

[3] Koichi Chino;Dinesh Manandhar, Ryosuke Shibasaki, "Authentication technology using QZSS", Position, Location and Navigation Symposium PLANS 2014, 2014 IEEE/ION, 5-8 May 2014.

[4] C. Wullems,"A Spoofing Detection Method for Civilian L1 GPS and the E1-B Galileo Safety of Life Service", IEEE TAES 2012.

[5] Sherman Lo, Sam Pullen, Stanford University; Veronica Palma, Maurizio Salvitti, CosimoStallo, RadioLabs, Italy; Juan Blanch, and Per Enge, Stanford University," Projected Performance of a Baseline High Integrity GNSS Railway Architecture under Nominal and Faulted Condition", ION GNSS+ 2017 • September 25-29, 2017• Portland, Oregon.

[6] Cosimo Stallo, Alessandro Neri, Pietro Salvatori, Andrea Coluccia, Roberto Capua, Giorgia Olivieri, Luca Gattuso, Lukasz Bonenberg, Terry Moore, "GNSS-based Location Determination System Architecture for Railway Performance Assessment in presence of local effects", IEEE ION PLANS 2018 Conference, April 23-26, 2018, Monterey, California.

[7] *Pietro Salvatori, Cosimo Stallo, Sam Pullen, Sherman Lo, and Per Enge,* "Use of SBAS Corrections with Local-Area Monitoring for Railway Guidance and Control Applications", IEEE ION PLANS 2018 Conference, April 23-26, 2018, Monterey, California.

[8] Juliette Marais, Julie Beugin, Jean Poumaillouxc, Marc Gandara "EGNOS service evaluation in railway environment for safety critical operations", Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria.

[9] E. Barker and A. Roginsky, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths," NIST Special Publication,800-131A, Jan. 2011.

[10] European Network and Information Security Agency (ENISA),"The Algorithms, Key Size and Parameters Report," Nov. 2014.

[11] NSA, "Fact Sheet Suite B Cyber Security Analysis"

[12] Igor Lopez and Marina Aguado, "European Train Control System Cryptography", Sept. 2014.

[13] C.W. Johnson, A. Atencia Yepez,"Cyber security threats to safety-critical, space-based infrastructures".

[14] Ali, K., Pini, M., & Dovis, F. (2012). "Measured performance of the application of EGNOS in the road traffic sector. GPS solutions", 16(2), 135-145.

[15] International Civil Aviation Organization (ICAO), Standards and Recommended Practices (SARPs) Volume 1 – Annex 10, 2006

[16] RTCA Special Committee 159, "Minimum Aviation System Performance Standards (MASPS) for Local Area Augmentation System (LAAS)," DO-245A, Dec. 2004

[17] RTCA Special Committee 159, "Minimum Operational Performance Standards for GPS Local Area Augmentation System Airborne Equipment," DO-253D, July 2017

[18] RTCA Special Committee 159, "GNSS-Based Precision Approach Local Area Augmentation System (LAAS) Signal-in-Space Interface Control Document (ICD)," DO-246E, July 2017

[19] EUROCAE Working Group 28, “Minimum Operational Performance Specification for Global Navigation Satellite Ground Based Augmentation System Ground Equipment to Support Category I Operations,” ED-114A, March 2013

[20] RTCA Special Committee 159, “Minimum Operational Performance Standards (MOPS) for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment,” DO-229E, Dec 2016

[21] Sam Pullen, “The Use of Threat Models in Aviation Safety Assurance: Advantages and Pitfalls,” CERGAL 2014, Dresden, Germany, July 2014

[22] Sam Pullen, Todd Walter, Per Enge, “SBAS and GBAS Integrity for Non-Aviation Users: Moving Away from ‘Specific Risk’,” ION ITM 2011, San Diego, California, January 2011

[23] “EGNOS Safety of Life (SoL) Service Definition Document” Revision 3.1

[24] Ali, K., Pini, M., & Dovis, F. (2012). “Measured performance of the application of EGNOS in the road traffic sector”. GPS solutions, 16(2), 135-145.

[25] A.Grant, P.Williams, N.Ward and S.Basker, “GPS Jamming and the Impact on Maritime Navigation”. The Journal of Navigation, 62(2): 173-187, 2009

[26] F.Rispoli, A.Neri, C.Stallo, P.Salvatori, F.Santucci,"Synergies for trains and cars automation in the era of virtual networking2, Journal of Transportation Technologies, Special Issue on "Automated Autonomous Vehicles: Technology Trends and Impacts on Society", 2018, Vol.08 No.03(2018), Article ID:85060,19 pages 10.4236/jtts.2018.83010.

[27] I. Fernandez-Hernandez, V. Rijmen, G. SecoGranados, J. Simón, J. D. Calle and I. Rodríguez, "Design Drivers, Solutions and Robustness Assessment of Navigation Message Authentication for the Galileo Open Service," ION GNSS+ 2014, 2014.

[28] STARS “D5.3 - EGNSS Target Performances to meet railway safety requirement” Deliverable.

[29] “GNSS Initiatives in Shift2Rail: the challenges for EGNOS in the ERTMS evolution”, pag.16.

[30] “Guidelines for ANSP/Airports and Aircraft Operators for LPV implementation”, ESSP

[31] Benoit Roturier, Eric Chatre, Javier Ventura-Traveset - “The SBAS Integrity Concept Standardised by ICAO: Application to EGNOS”.

[32] UNISIG - “On-line Key Management FFFIS”, Subset-137

[33] “EGNOS Service Notice”, Number 015, Version 2.0, release date 14/08/2018.

[34] https://www.gsa.europa.eu/newsroom/news/airbus-awarded-egnos-v3-contract

[35] CEI EN 50129, Railway applications - Communication, signalling and processing systems – Safety related electronic systems for signalling, 2004

[36] D5.3 EGNSS Target Performances to meet railway safety requirements, deliverable STR-WP5-D-ANS-034-06

[37] RTCA Special Committee 159, “Minimum Operational Performance Standards (MOPS) for Global Positioning System/Satellite-Based Augmentation System Airborne Equipment,” DO-229E, Dec 2016

[38] UNISIG SUBSET-041 v.3.2.0, Performance Requirements for Interoperability

[39] UNISIG SUBSET-026 v.3.4.0, ERTMS/ETCS System Requirements Specification

[40] Commission Regulation (EU) No. 1299/2014 of 18 November of 2014

[41] CEI EN 50159, Railway applications - Communication, signalling and processing systems – Safety related communication in transmission systems, 2012

[42] ERTMS/ETCS RAMS Requirements Specification, Chapter 2 – RAM, UIC 1998

[43] Global Positioning System Standard Positioning Service Performance Standard, 4th edition, September 2008.

[44] Galileo Initial Services – Open Service – Service Definition Document, Issue 1.0, December 2016.

[45] EGNOS V3 Phases C/D - Summary Statement of Work, Issue 1.0, June 2016.

[46] Commission Delegated Decision (EU) 2017/1474

[47] ERA (2015), Report on ERTMS Longer term perspective V1.5

[48] Commission Regulation (EU) No. No 402/2013 of 30 April 2013

[49] UNISIG SUBSET-098 v.3.0.0, RBC-RBC Safe Communication Interface

[50] EGNOS Data Access Service (EDAS) Service Definition Document.

[51] UNISIG SUBSET-098 v.3.1.0, EuroRadio FIS


STARS