ERTMS on SATELLITE Galileo Game Changer

Deliverable 5.1: assessment report of the enhanced functional ERTMS architecture

Due date of deliverable: 31/05/2019

Actual submission date: 16/06/2019

Leader/Responsible of this Deliverable: Bureau Veritas Italia

Reviewed: Y

Document status		
Revision	Date	Description
00	May, 30 -2019	First issue.
01	May, 31 -2019	Revision 01 collects remarks from RINA consulting and AST
02	June, 16 -2019	Revision 02 collects remarks from June, 13th -2019 DRS (author Aleš Filip)

Project funded from the European Union's Horizon 2020 research and innovation programme		
Dissemination Level		
PU	Public	X
CO	Confidential, restricted under conditions set out in Model Grant Agreement	
CI	Classified, information as referred to in Commission Decision 2001/844/EC	

Start date of project: 01/12/2017 Duration: 24 months

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Stefano Benusiglio	Bureau Veritas	Author
Tommaso Ghiara	Bureau Veritas	Contribution and Reviewer
Veronica Tripodoro	Bureau Veritas	Contribution and Reviewer
Claudio Evangelisti	ITCF	Reviewer

DOCUMENT APPROVAL

Document Code	Rev.	Approved	Authorised	Date
ERSAT-GGC_WP5_D5.1.assessment report of the enhanced functional ERTMS architecture	02	TMT	Massimiliano Ciaffi	16/06/19

EXECUTIVE SUMMARY

This document is the output of WP 5.1 activities and its finality is to assess the “Enhanced Functional ERTMS architecture capable of using GNSS and public Radio TLC Technologies” developed by ERSAT GGC WP2.

The present documents receives as input from WP2 and WP3 the following deliverables:

- D2.1: “Enhanced Functional ERTMS Architecture Capable of using GNSS and Public Radio TLC Technologies”, [Rif. 1],
- D.2.2: “Functional and Not Functional Test specification”, [Rif. 4],
- T 2.1.8: “Definition, Model and Verification in MatLab of Railway RAIM”, [Rif. 2],
- D3.1: “Safety Analysis of ERSAT ERTMS Application over GNSS” [Rif. 5],
- D3.2: “GNSS Quantitative Analysis for ERSAT GGC Project” Rif. 6.

The assessment activity documented by the current deliverable has been carried out comparing the expected functional and safety performances achievable by the “ERTMS enhanced architecture” under evaluation against the targets nowadays requested by the ETCS B3 R2 GSM-R R1 set of specification.

Specificity of the ERSAT project is the introduction in ETCS system of components, GNSS technology and public radio technologies, which are out of the railway application control. For this reason, one of the goal of this report is to evaluate the adequacy of the safety measures identified by WP3 to protect the railway application also against failure of parts out of his control.

Another finality of this report is to evaluate the impact of proposed architecture on the framework of the ETCS interoperability specifications trying to identify:

- the upgrade to be applied on the specifications in order to allow the development by the suppliers of interoperable solutions
- the functional blocks of the architecture candidate to be introduced in the specification as “interoperability constituents” or that can be independently certified as generic product.

TABLE OF CONTENTS

LIST OF FIGURES

ACRONYMIS AND DEFINITIONS

Acronym	Description
ATPE	Along Track Position Error
ATPL	Along Track Protection Level
BG	Balise Group
BTM	Balise Transmission Module
DB	Database
ERSAT-GGC	ERTMS on SATellite – Galileo Game Changer
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETS	Eurobalise Transmission System
FDE	Fault Detection and Exclusion
FMECA	Failure Mode, Effects, and Criticality Analysis
GAD/TV	GNSS Augmentation Dissemination/ Trackside Verification
GNSS	Global Navigation Satellite System
HW	Hardware
LOS	Line of Sight
MA	Movement Authority
MDE	Minimum Detectable Error
MI	Misleading Information
MLCP	Multi-Link Communication Platform
MTCP	Multipath Transmission Control Protocol
NLOS	Non Line of Sight
PBG	Physical Balise Group
PL	Protection Level
PR	Pseudo-range
PVT	Position, Velocity, Time
QoS	Quality of Service
RAIM	Receiver Autonomous Integrity Monitoring
RBC	Radio Block Center
SIL	Safety Integrity Level
SIS	Signal In Space
SoM	Start Of Mission
SOW	Scope of Work
STI	Standard for Technical Interoperability
THR	Tolerable Hazard Rate
TLC	Telecommunication
TMS	Traffic Management System
VB	Virtual Balise
VBR	Virtual Balise Reader

1. INTRODUCTION

Finality of this report is to supply an independent safety evaluation of the technical solutions proposed by the ERSAT GGC WP2 in order to introduce in the ETCS system the virtual balise capability using the GNSS technology and public radio TLC technologies.

The finality of introduction of the virtual balise concept is to reduce the need of physical fixed Eurobalises along the lines equipped for operation in ETCS Level 2 and, as consequence, to increase the availability of the lines reducing the need of maintenance and the installation costs.

The ERSAT GGC functional architecture is not intended to operate in ETCS Level 1, that because the Euroradio link is not present in the ETCS level 1, while, also with the aim to avoid the introduction of new interfaces, the ERSAT GGC project makes use of the Euroradio link to disseminate the satellite augmentation system information.

In a future prospective, ERSAT GGC project has also the finality to gain the necessary experience on the use of the GNSS technique in a railway context to use this technique for the ETCS L3 context.

Since the introduction of the virtual balise concept brings innovative concepts into the ETCS system that are not nowadays regulated by the TSI, the present assessment cannot be carried out applying a standard approach that would require the evaluation both of compliance of the system against the functional requirements and the evaluation of the achievement of the tolerable hazard rates regulated by the TSI.

Nevertheless, the present assessment is always focused on the evaluation of the proposed solution against the current applicable regulations highlighting the situations on which, for the specificities of the project, the current regulations are not fully applicable and evaluating, for these cases, the presence of additional measures able to assure an equivalent train protection.

With the aim to get this goal the report is organized in the following sections:

- §2: introduction to ERSAT GGC project. Finalities of this paragraph are:
    - to supply an overview of virtual balise concept,
    - to introduce the system architecture proposed by the ERSAT GGC project,
    - to evaluate the impact of the proposed solution on the ETCS L2 interoperability interfaces,
    - to introduce the constrains given by railway context that could impact on the applicability of the GNSS technology inside a Train Control System.
- §3 physical balise versus virtual balise functional comparison: the aim of this paragraph is to supply for the functions impacted by the introduction of the VBR, a functional comparison between the current ETCS L2 functionalities and the ETCS L2 system integrated with the virtual balise capabilities.

- §4 safety target achievement: aim of this paragraph is to evaluate if the proposed solution is adequate to assure the compliance against the ETCS THR nowadays defined by the UNISIG subsets

2. INTRODUCTION TO ERSAT GGC PROJECT

2.1 VIRTUAL BALISE CONCEPT

Physical Eurobalise are nowadays used by ETCS level 2 to send to the on board system a packet of data whenever the data shall be safety referred to a specific location on the infrastructure.

Physical Eurobalise are used:

- to support the first localization on the train at the start of mission;
- as repositioning, to supply a fixed and safe space references during the run in order to reset the odometric errors;
- to localize specific points on the line such as a “change of voltage”, “change of phase” or RBC and the level transition as well as related text messages for displaying on the DMI.

It must also be taken into account that ETCS level 2 makes mainly use of fixed Eurobalise which telegrams are defined at the moment of the design of the line.

The virtual balise concept moves from the consideration that the on-board system could be fed with an absolute space reference given by a Global Navigation Satellite System (GNSS), instead of the fixed balises, and that the fixed information now acquired by the physical balises could be stored on a data base up-loaded by the on board system before the mission.

The main advantage of this solution is the possibility to reduce the complexity of the lines removing the majority of the Eurobalise and therefore to reduce the need of maintenance along the lines.

It must also be highlighted that:

- the “virtual balise concept” is complementary and it is not intended to replace all the physical balises nowadays present on the stations/lines (see [Rif. 3]). The criteria to identify the balises that can be virtualized on the base of their function and position are introduced later in this report.
- the proposed solution does not introduce new ERTMS/ETCS levels or operative modes and does not impact on the “train detection and train integrity supervision” which are still in charge of the trackside equipment as defined by SUBSET 026-2 for ERTMS/ETCS level 2.
- the virtual balise concept is applicable for operation on ERTMS/ETCS Level 2 and it is conceived to assure the backward compatibility of the trains equipped with this capabilities also on existing lines.

- the presence of the virtual balises does not prevent the use of the line by “ETCS trains not equipped for VB detection” under the condition of the presence of at least of the physical balises necessary to assure an acceptable performance level.
- the finality of the GNSS technique inside the ERSAT GGC project is confined to realize an alternative way to make available to the on-board system the LRBG position, with a known and safe position accuracy, without the need to install physical balises along the path.
- the use on-board of the GNSS is not intended to replace the odometric subsystem which shall be always responsible to supply to the EVC core the travelled distance from the LRBG and the train speed.

2.2 PHYSICAL ARCHITECTURE

In order to include the virtual balises capability, the current ETCS architecture shall be integrated with the here below introduced subsystems:

(for a more detailed description of the system architecture proposed by the ERSAT project refer to [Rif. 1] §6.1)

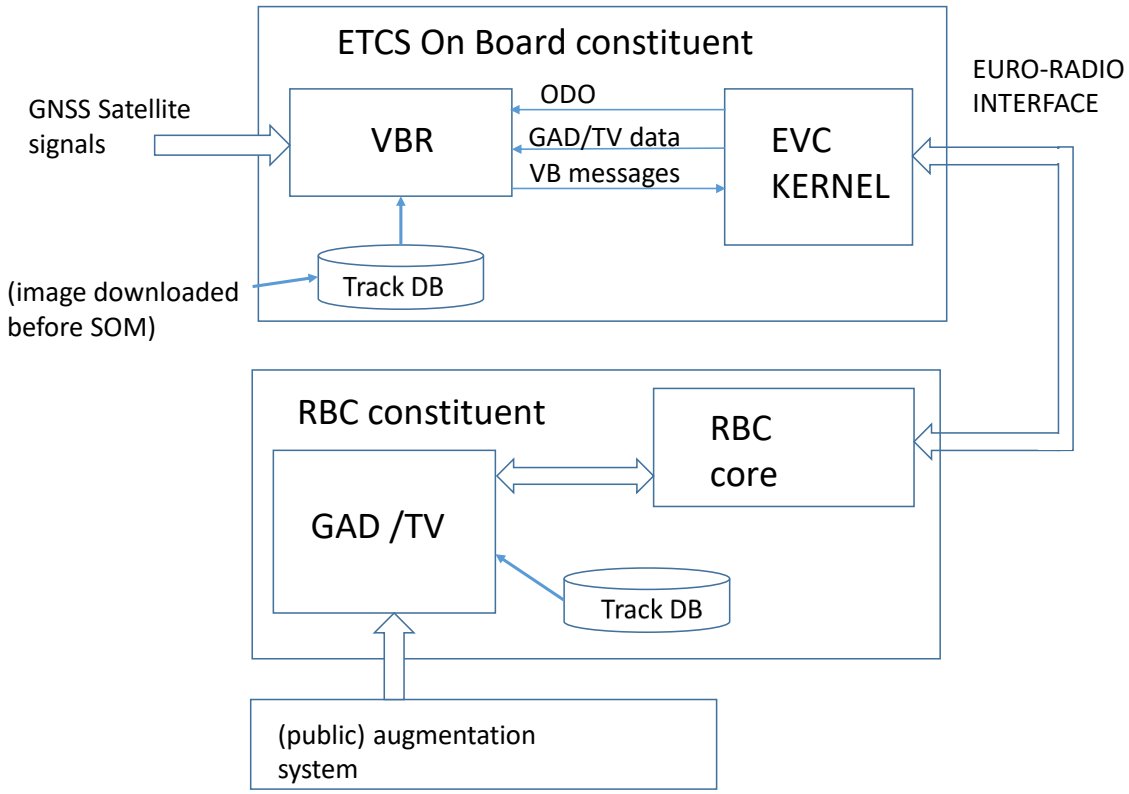

Figure 1 ETCS enhanced architecture

Trackside system

1. Track database.

   The track DB is a repository built at the time of design of the line and frozen once the last version is available for commissioning.

   The track DB in stored by the Track side constituent, while an image of track DB shall be make available to the on-board subsystem before the Start of mission.

   The track DB shall include:

   - the geographical position of all the virtual balises designed for the line and, for each balise, its own telegram. It must be noticed that the introduction of the virtual balise concept does not require any change of the rules now applied to assign the values of the telegrams variables. The way EVC processes the information is equivalent there is no functional distinction between physical and virtual balises
   - geographical reference of the tracks;
   - additional information about the track layout in order to allow, in cooperation with the trackside system, the identification of the track engaged by the train.

   The first time the track DB shall be uploaded by the on-board subsystem, from the track side sub-system before the start of the mission or, in any case, in advance with respect to a RBC handover. When the track DB is already available on board, a check for consistency with the trackside DB shall be always performed before the start of mission.

   The trackside / on-board communication link identified to upload the track DB is the Euroradio link already present in the ETCS architecture. It must also be underlined that in order to assure the trackside / on-board interoperability, the structure of the messages which allow the OB system to upload the track DB shall be regulated by an interoperability specification.

2. The augmentation system (or reference station). The task of the augmentation system is to monitor at a well know location the signals supplied by the satellites in order to calculate corrective factors that, once made available to the on-board systems, permit to increase the GNSS location accuracy. Specifically the use of an augmentation system reduces significantly the effects of the tropospheric propagation, which can be assumed constant in area of some tens of kilometres from the reference station, on the location accuracy.

   A second mission of the reference station is the detection of unreliable satellites to be excluded by the on board system during the PVT (position, velocity time) evaluation. The reference station can perform this task more easily that an On-board receiver because working into a fixed position it knows the expected PVT solution.

   The corrective factors and the satellite integrity data calculated by the reference stations shall be collected by the augmentation and dissemination system and then broadcasted by means of the Euroradio channel to the on board systems in order to increase the measurement accuracy.

Note: the augmentation system data are considered in this ERSAT project as input for enhanced RBC constituents.

3. The GAD/TV (GNSS Augmentation Dissemination/ Trackside Verification). Mission of this components are:
    - GAD: to collect and to disseminate to the on-board systems the satellite error correction and satellite integrity data.
    - TV: check the localization of the train on the tracks merging the data supplied by the train, for example when a non connected train requires a new connection, against the information available on the trackside RBC and TMS equipment

On-board system

4. The On–board GNSS based virtual balise reader. The Virtual balise reader can be split in two stages : “Antenna / GNSS receiver” and “PVT computation and balise detection”

   While the first stage has in charge the acquisition and demodulation of the satellite signals, the second stage shall:

   - calculate the PVT solution and the location accuracy, also taking into account the error correction factors broadcasted by the augmentation and dissemination system,
   - determine when the train position matches the next virtual balises expected along the train route;
   - acquire from the track DB the correspondent telegrams, correlate the telegram with the current space/time and send the data, including the safety confidence interval, to the EVC core exactly as expected by the current implementations.

2.2.1 IMPACT ON THE INTEROPERABILITY FRAMEWORK

2.2.1.1 INTEROPERABILITY CONSTITUENTS

The ETCS enhanced architecture proposed by the ERSAT GGC project (see [Rif. 1] figure 2) includes the GAD/TV sub-system inside the RBC constituent and the VBR inside the ETCS On board constituent.

Therefore the proposed ETCS enhanced architecture does not introduce new interoperability constituents.

Nevertheless it must be noticed that the functions in charge of the VBR and GAD-TV subsystem are well defined and independent from the other functions allocated to the interoperability constituents. Therefore VBR, GAD/TV could be developed, verified and certified as “generic products” whenever a CENELEC 50126 / CENELEC 50129 life-cycle is applied.

2.2.1.2 INTEROPERABILITY INTERFACES

The proposed architecture impacts only on the definition of the messages exchanged by means of the EURORADIO interface because the system architecture makes use of this interface for the following functions:

- to upload to the OBS the track DB and to verify the consistency of an already present track DB;
- to disseminate to the ON_BOARD systems the GNSS error corrections and GNSS satellites integrity status;
- to assist the track verification function.

Therefore the ETCS messages definition shall be updated including new dedicated packets, however no changes are necessary to the EURORADIO communication protocol up to the safety layer included (note: for trial tests it is planned to include these data in packet 44 “Data used by applications outside the ERTMS/ETCS system”).

The proposed architecture does not require any change on the other existing interfaces because:

- no changes are requested to the existing Eurobalise and Euroloop interface;
- the GNSS Signal In Space (SIS) interface is already regulated by the GNSS standards and does not need to be included in the interoperability specification;
- because the on-board interface between the VBR and the EVC core is, according to the [Rif. 1] setup, defined as an internal interface of the EVC on board constituents it does not need to be regulated by additional interoperability specification.

In the same way the trackside interfaces between RBC, GAD/TV and Public augmentation network, are defined as a RBC constituent internal interfaces and therefore do not need to be regulated by the interoperability specifications.

2.3 INTRODUCTION OF THE GNSS TECHNOLOGY AND RAILWAY CONSTRAINTS

As well known the main finality of all GNSS is to make available, by means of low cost receivers, an accurate localization of the receiver on an Earth referred coordinate system. Moreover the GNSS is also able to supply accurate UTC time information and receiver velocity.

Nowadays many GNSS are operative as: GPS (developed and maintained by United States), GLONASS (Russia), Galileo (European community) and Beidou (China) as well as different satellite based and ground based augmentation systems are available.

The main questions to be clarified in order to introduce the GNSS concept in the railway train protection system are:

- is the GNSS measurement accuracy suitable for the railways needs?
- is the GNSS measurement availability suitable for the railways needs?
- is the GNSS measurement integrity suitable for the railways needs?

Purpose of the followings paragraphs is to supply a first introduction about how the approach applied by the ERSAT answer to these questions.

2.3.1 GNSS ACCURACY (FAULT FREE CONDITIONS)

As widely debated in literature, the GNSS accuracy, in fault free conditions, depends on many factors including, but not limited to:

- the number of the available satellites;
- the position on the sky of each satellite and the angular space between them (geometrical factor);
- the ionospheric and tropospheric condition;
- the presence of interference, including the electromagnetic interference generated by traction system;
- the presence of obstacles able to create multipath;
- the noise figure of the receiver.

It must be observed that all these factors give contribution to the measure accuracy and that, almost all, change both over the time and over the position.

A conservative approach to determinate the worst accuracy that can be assured by a GNSS taking into account the worst condition for each of these factors is really not feasible because it would lead to a really pessimistic and useless result.

On the other hand it must be observed that most of the here above recalled factors are directly evaluable by receivers at the time of the measure or their effect can be predicted by a fixed reference station (augmentation system) and broadcasted to the receivers as corrective factors.

For example:

- once that also an approximate PVT solution is known, the satellite positions are known to the receiver by the ephemerid data and the receiver is able to estimate the geometrical factor.
- corrective factors, able to take into account the tropospheric propagation effects, which can be supposed to be invariant in an area around the station, can be evaluated and broadcasted to the receivers by a ground fixed reference station.

The knowledge of these factors at the measurement time allows the receiver, as demonstrated by the scientific literature, to evaluate in run time together with the PVT solution also the current accuracy of the measure.

The location accuracy is usually calculated as standard deviation (the area of the error distribution function which includes the 68 % of the measurements) but because, as demonstrated by the scientific literature, the error distribution is Gaussian, the measure accuracy can be recalculated at any integrity level by means of a fixed multiplicative factor as 2 sigma (95%), 3 sigma (99.7%).

In order to evaluate the possibility to use a GNSS in a railway context it is necessary to take into account that:

- the respect of a pre-defined measure accuracy can not be assured by any GNSS receiver;
- the standard deviation of measure changes continuously because of many reasons but it can be calculated by the receiver at the same time of the measurement;
- several techniques are nowadays available to increase the GNSS measurement accuracy as augmentation systems, low noise receiver or multi constellation systems.
- It is up to the railway applications that use the measure:
    - starting from the standard deviation of the measure calculated through the satellite data analysis techniques, evaluate the accuracy at the requested integrity level requested for the safety of the railway application[1] ;
    - integrate, if necessary, the GNSS measure with other direct or indirect measurements supplied by other independent sources (like odometric data or inertial data) of measure which integrity shall be well known
    - take in charge the estimated accuracy at the requested integrity level to assure the safety of the train.

A first idea about the use of a GNSS system as virtual balise reader inside the ETCS level 2 system could be to verify if the satellite technology can assure the same location accuracy requested by the UNSIG specification for a physical balise detection but it is evident that the safety location accuracy of ±1m requested by subset 036 §4.2.10.2 (accuracy for vital purposes) cannot be assured by a GNSS.

Therefore it is necessary to identify the reasons of this requirement, and when possible, ask to the EVC functions that need the location data, to keep into account the GNSS safety accuracy supplied by the Virtual balise reader together with the location measure.

Note: With the words “safety accuracy” is meant a VBR location accuracy calculated at the sigma level that assures an “invalid position” probability compliant with the THR allocated to the GNSS localization system by the ERSAT quantitative analysis [Rif. 6].

The reasons of the physical balise accuracy requirement are different:

1. avoid balise inversion inside a balise group (the minimum distance allowed between 2 consecutive balises is between 2.3m and 5m, depending of the allowed speed (Subset-036, 5.6.3))
2. for all the balises intended to protect a danger just downstream the balise (as Stop if SR balise): to make predictable the maximum delay of the emergency action requested by the balise in order to define the minimum distance necessary between balise and danger.

[1] More considerations about how much safe shall be the confidence interval for a railway purpose are included at pag 13

3. define the maximum contribution due to the balise localization accuracy to be taken into account to calculate the “safe distance confidence interval” requested by SUBSET 041 §5.3.1.1 for a safety localization of the position of the train.

In addition it must be considered that physical Eurobalise are also used at start of mission to safety locate the train on the correct track while this function could be safety performed by a virtual balise reader only if the safety measure accuracy is less than the distance between parallel tracks. This requirement is nowadays not achievable, with the safety integrity requested for railway applications, with the current GNSS technologies.

According to these considerations in the ERSAT GGC project the virtual balise reader is not intended to:

- discriminate the track engaged by the train. To cover this function at start of mission the ERSAT GGC projects includes the GAD/TV subsystem, whose function is to support the first location of the train on the correct track at start of mission, merging different data made available by other systems as: On-board, RBC, Interlocking and TMS if present. Note: for the evaluation of the impact of the introduction of the VBR on SOM refer to §3.1;
- replace balises whose function is protect a danger just downstram the balise as Stop if SR balises;
- replace balises whose function is to identify transition, change of voltage or change of phase transitions because these balises are in any case necessary to allow the access on the line of trains not equipped with the Virtual balise reader.

while the main finality of the introduction of the Virtual balise reader is :

- to eliminate, or at least reduce significantly, the physical Eurobalise nowadays present on the line intended to supply to the train a safety travelled space reference.

Because, the accuracy of the balise localization gives contribution to the safety of the train location, the ERSAT GGC project requires to take into account in the calculation of the safe travelled distance confidence interval requested by SUBSET 041 §5.3.1.1 all the dynamic GNSS accuracy (that shall be calculated at the requested integrity level) instead of the ±1m accuracy nowadays assured by a physical balise reader.

Therefore, and just with reference to the calculation of travelled distance confidence interval, the assessor agrees that the accuracy requirement of ± 1m request for the Eurobalise is not mandatory for the VBR context under the condition that the full GNSS accuracy (calculated at the requested integrity level) is taken into account by the EVC function to calculate the travelled distance safe confidence interval.

Also if during normal behaviour it is expected that the safety accuracy given by the GNSS will permit to improve the accuracy given by the odometric subsystem, it could be useful to note that also in situation of very poor GNSS accuracy (VBR location uncertain > current Odometry location uncertain), and also if the GNSS safety accuracy is used to determinate the safe min/max front of the train, the protection assured to the train with respect to the danger will be always present without any discontinuity. In the case that the train front end is overestimated with respect to the active safe train front end (calculated by the odometry) a speed limitation could occur, but because

the real train position is surely inside the safety confidence interval, the respect of the danger is always assured.

About the respect of the performance requirement required by SUBSET 041 §5.3.1.1 of ±5m+5%s the assessor agrees that VBR technique, allowing a more frequent recalibration of the odometric errors, because more VB can be included in the line, should be able to assure at least the same average accuracy performances also if at the time of VBR detection (s= 0) the accuracy of ±5m can not be assured.

GNSS accuracy safety integrity requirement

Once clarified that the location accuracy, starting from the standard deviation, can be calculated at any integrity level just applying a multiplicative factor, the next question in order to evaluate the impact of the introduction of the VBR is:

- how can be established the requested Virtual Balise accuracy integrity (in absence of failures) requested to safely introduce the Virtual Balise concept in the ETCS level 2 context?

The answer of this question can be found in the ERSAT GGC quantitative safety analysis [Rif. 6] §9.2 which allocates to the event TRANS-BALISE-3-SR (insertion, which also includes the case of a longitudinal error on the balise position) the hazard rate of 0.66 E-9 h-1.

It must also be highlighted that a critical point for the certification of the applications could be the demonstration of the achievement of the safety requirement here above recalled and therefore of the correctness of the calculation of GNSS accuracy standard deviation, with the only sharable assumption that the distribution of the error measurement is Gaussian, allows to calculate the location accuracy at the requested integrity level.

Different on–board suppliers can indeed use different solutions to get the PVT solution and to calculate its standard deviation using different techniques as mono or multi constellation systems, different front-end or calculating the absolute error or just the component of the error along the track.

In this context, to support the certification process it seems necessary to introduce and develop in detail for the “space interface” a new test specification focused to make possible a uniform evaluation of the safety performances of the PVT algorithms including the calculation of localization safe confidence interval.

For this purpose, and taking into account that the current GNSS technology makes available to the GNSS developers adequate tools able to reproduce both the nominal signals of the satellite and to inject errors, the test specification could be mainly based, but not only, on the definition of scenario synthesizable in laboratory.

Running these scenarios, which shall also involve the augmentation system interface, it shall be possible to compare the localization error, with respect to the position defined by the scenario, against the calculated standard deviation. In this way the calculation of the standard deviation performed by the different suppliers, applying different techniques, could be positively certified whenever the location error is lower of the standard deviation evaluated by the on-board system for at least the 66% of the measurements.

Once that the calculation of the measurement standard deviation is verified it will be easier also to certify the achievement of the safety requirement verifying how the safe confidence interval is calculated from the standard deviation.

2.3.2 GNSS INTEGRITY (PRESENCE OF FAULTS)

As introduced by [Rif. 2] §3:

> "*Integrity and Continuity characterise the system response to rare natural events or system failures*".

Where in the context of the project "failures" must include in addition to the space segment failures also the ground control stations failure, the on board receiver failures and the augmentation system failure.

The ERSAT project has evaluated the effect of the failures with the support of a set of functional Failure Mode Effect Analysis (see [Rif. 5]). As result the functional Failure Mode Effect Analysis has identified a set of safety requirements, identified by [Rif. 5] with the identifier "req. nnn".

The identified safety requirement can be classified in the categories here below identified[2]

	category	requirement (refer to [Rif. 5])	identified protection techniques	note
1	Protection of communications	REQ.012 (ERTMS/ETCS EVC-VBR interface) REQ.014 (GNSS Receiver - PVT Computation Block interface) REQ.015 (GAD/TV-RBC interface) REQ.016 (Augmentation System - GAD/TV interface) REQ.005, REQ.008 (VBR and GAD/TV shall avoid the communication of undue messages	Use of safety protection layer compliant with CENELC 50159	The requirements intended to verify the freshness of the information are not included because already included in the safety layers finalities.
2	Hardware redundancy	REQ. 009	Redundancy of the on board GNSS chain	

[2]For simplicity the table does not includes all the requirements intended to assure a safety reaction in case of lack of fresh data

3	Consistency checks based on the SIS information redundancy	REQ. 033	Use of RAIM techniques	It includes the protection against multipath
4	Check of the SIS quality	REQ. 020	Measure and check against of a predefined threshold of the S/N ratio.	
5	Self-test (as memory test, CPU test, track db consistency check, initialization complete checks...)	REQ. 006 REQ. 017 REQ. 018 REQ. 010 REQ. 032	Internal self-test	VBR GAD/ TV
6	Consistency check of the PVT solution based on different data	REQ. 029 The PVT solution shall be always crossed-check with other information	To be defined	

Table 1

As appears from Table 1 some of the mitigation techniques identified by the safety analysis (see 1,2,and 5) are already widely applied to protect safety critical railway systems while, the mitigation techniques 3,4 and 6 have been introduced specifically in order to validate the SIS (Signal in Space) and therefore the part of the GNSS system out of boundary of the railway applications.

Specifically the Technique 3 (RAIM), which works thanks to the redundancy of the information supplied by the satellites when more than the minimum set of satellite requested to fix the PVT are in LOS (Line of Sight), is a powerful help to protect the systems both against failures and against multipath.

In general to fix a PVT solution in three dimensional space, and considering that also the Time is unknown, is necessary the visibility of at least four satellites of the same constellation.

If the solution is constrained (i.e. the context of the application assures that the solution is on a well-known subset of the three dimensional space as a surface or a line) less satellites are requested. In the context of a railway application, where the PVT solution is constrained on a 1 dimension railway track the number of the necessary satellites can be reduced to 2 also if, in this case, the accuracy of the measure could be really poor in condition of bad alignment.

The purpose of RAIM techniques is to validate the SIS by means of the redundancy of the information available when more satellites are in visibility. Specifically, considering a mono-constellation GNSS and context, 5 satellites are sufficient to assure the fault identification capability (i.e. un-validate the solution in presence of failures) while 6 satellites are necessary to assure also the fault exclusion capability (get a safe PVT solution, which exclude the satellite in fault condition).

In general if satellites from different constellations are visible (as GPS and GALILEO) at the same time the number of satellites necessary to apply the RAIM technique is respectively[3]:

- fault identification: four satellites in visibility plus the number of used constellations.
- fault exclusion: five satellites in visibility plus the number of used constellations.

The number of necessary satellites reduces in case of a constrained context and specifically in case of 1 D constrained application, as a railway path, the number of necessary satellites became:

- fault identification: two satellites in visibility plus the number of used constellations.
- fault exclusion: three satellites in visibility plus the number of used constellations.

The requested number of satellites in LOS to execute the RAIM algorithms for a virtual application does not represent a significant constrain because, as more deeper introduced at §2.3.3, the possibility to locate the virtual balises only in specific location[4] assuring a good sky visibility together with the possibility to uses satellites from different constellations reduces the risk that the RAIM algorithms could not be executed because of a lack of satellites.

The potentiality of the RAIM technique are evaluated at [Rif. 2]. This activity was carried out synthetizing in laboratory the expected GNSS signal for a realistic railway scenario and then testing the performances of RAIM techniques following the injection of random noise and/or injecting a known error on the signal of a satellite.

The activity introduced by [Rif. 2] wants to demonstrate the capability of the tested constrained and un-constrained RAIM algorithms, to:

- Avoid false alarms also in presence of random noise.
- Identify the presence of a failure satellite following the injection of the error
- Isolate correctly the satellite affected by the failure.
- Identify the unreliable satellite data because affected by multipath,

The RAIM algorithms was tested against this parameters:

- Random noise: average 0m, standard deviation 0.8m;
- Error injection: bias 15m or ramp 0.5m/s bias 11m.

[3] the number of satellites increase because each constellation uses its own system time
[4] the identification of a method able to identify the best location for the virtual balises also assuring a high sky visibility is the object of Working Package 4

- Multipath: to simulate a multipath condition, considering that the peculiarity of this type of error is to be really discontinue on the space, a random (according to a statistical distribution) alternation of error (10m) and non-error, is synthetized.
- False alarm threshold: 1E-3

The performed tests well demonstrated:

- The capability of both the constrained and unconstrained algorithms to identify the fault condition and to isolate the faulty satellite also if a random noise is injected at the same time of the satellite error.
- The robustness of the both the constrained and unconstrained algorithms to avoid false alarm in presence of random noise. Just a false alarm (undue satellite exclusion) was detected (see [Rif. 2] fig 46).
- The capability to identify the presence of multipath also if in presence of multipath more false alarms (undue satellite exclusion) were observed for the un-constrained algorithm.

In order to evaluate the applicability of the proposed RAIM techniques in the railways context it is also necessary to take into account the "miss detection probability" assured by the RAIM algorithm that can be calculated (see [Rif. 2] appendix A, (17)) starting from the assigned detection threshold.

Therefore in order to be used in the railway context, a possible approach could be:

1) calculate the detection threshold that assures "miss detection probability" compliant with the THR nowadays allocated, as already introduced at §2.3.1, to the hazard: actual train position outside the estimated travelled distance confidence interval .
2) take into account the detection threshold as additional contribution to evaluate the travelled distance confidence interval.

The approach followed by the current project is slightly different but always correct. In the approach applied by the project the requested THR is reached (refer to [Rif. 6] §11.3.2 H7-SR Apportionment[5]) allocating a HR target of 7.5E-06/h (how evaluated as technical feasible) on the event "lack of GNSS position integrity" and an additional contribution of 4E-05/h allocated by the safety analysis on the event "Independent checks integrity risk" that shall be based on independent position system.

Therefore it shall be highlighted that the ERSAT project does not state the technical solutions to be applied to assure the requirement of "Independent checks integrity risk" and each supplier is free to apply different method using also different source of data as, for example, odometer and inertial sensors.

[5] the scenario analysed at §11.3.2 H7-SR Apportionment refer to a Start of Mission on line with position unknown but it is also applicable to determinate the residual risk of a wrong localization

2.3.3 GNSS AVAILABILITY

The third parameter that shall be taken into account to evaluate the introduction of the GNSS in the railway system is the GNSS availability that, in general, can be defined as the fraction of the time where the PVT solution is available over the mission time.

However taking into account the context of the virtual balise application proposed by the ERSAT GGC project it must be highlighted that the mission of the on-board receiver is not to fix continuously the PVT solution during the whole train mission but it is just to supply the solution in the area where a virtual balise is expected. Therefore lack of GNSS signals between the virtual balises, in the VBR context, has no effect on the availability of the VBR function.

It could be also useful to remind that the virtual balise application has not in charge to supply the travelled distance information to the train protection functions but that this task, also if a GNSS receiver is installed on board, is always allocated on the traditional (based on wheel sensors) odometric function with the only difference that the odometric errors are now reset according the current safe PVT accuracy when a virtual balise is "detected and not fully reset as for a physical balise.

Therefore to assure a high availability for the Virtual balise Reader function is necessary well design the position assigned to virtual balises avoiding proximity of bridges, lateral walls or big buildings that can obscure the GNSS signals. For this purpose the core of ERSAT GGC project includes WP4 focused on the development of tools for detect the area to be avoided for the virtual balises placement.

The concept of the Virtual balise is also fully compatible with the presence of tunnels up to 1-2 km (the current distance between physical balises) without introducing any degradation of the performance.

In any case because the introduction of the Virtual balise reader is not intended to replace the BTM function that shall be always assured by the on-board system, longer tunnels, series of adjacent tunnels or urban areas, when poor reception is expected for a large area, could be always equipped with physical balises.

According to these considerations and also taking into account that:

- the VBR availability mainly depends on the virtual balise location and that ERSAT GGC WP4 is in charge to define a method to avoid wrong position,
- physical balises can be used, where necessary, to cover specific area where the GNSS signal is missing,
- the lack of GNSS signal between two virtual balises has not effect on the VBR availability;
- the event "missed virtual balises" has not safety effect, because as identified by the quantitative safety analysis (see: [Rif. 6] §9.1 [ERSAT_GCC_D3.2_01]) "*to prevent hazardous consequence in case of VB deletion, the safety-critical information is not delivered by VBG*"
- the PVT solutions and RAIM integrity checks availability can be increased using multi-constellation

- the simulations performed considering a realistic railway scenario included in [Rif. 2] gives evidence of a good and really redundant satellite coverage.

The assessor agrees that the ERSAT GGC project includes adequate countermeasures against the expected and unavoidable lack of availability GNSS signals that can be experimented along the track.

Nevertheless the assessor recommends to estimate, combining the results of WP4 and experimental tests, the frequency of the event “virtual missed balise”. This data could be significant in order to build useful indication and to define the distance between virtual balises.

3. PHYSICAL BALISE VERSUS VIRTUAL BALISE FUNCTIONAL COMPARISON

Finality of this chapter is to supply a functional comparison between the current ETCS L2 functionalities and the ETCS L2 system integrated with the virtual balise capabilities.

The following analysis is focused on the functions impacted by the introduction of the virtual balise concept and specifically on the localization function because the function of the Eurobalise inside the ETSC L2 is to “trigger” the on-board protection functions with a safe distance reference point.

Physical balises are used by ERTMS L2 with the following finalities:

1. to support, when the train position is not valid, the first localization of the train at start of mission;
2. to protect or to announce fixed points just downstream the balise (e.g Stop in SR, System or Level boundary, Change of Phase, Change of Voltage);
3. to supply a safe location reference point that can be used by the trackside to refer the next movement authority.
4. to transfer to the OBS not safety related information (as for example text messages)

Because, as discussed at §2, the VB concept is not intended to replace physical balises intended to protect or to announce fixed points just downstream the balise, only the impact on the following functions shall be analysed:

- localization of the train at the start of mission (see §3.1);
- localization of the train during the mission (see §3.2).

Moreover, considering the contribution given by the linking function to the mitigation of the hazards “physical (or virtual) balise deletion , the impact of the introduction of the Virtual Balìse on the linking function is evaluated at §3.3.

The following evaluation assumes that:

- the contents of the “telegrams” of the VBR stored in the track DB are equal to the same telegrams if stored by a physical balise placed at the same position;
- The VB accuracy location calculated by the VBR and sent to the EVC protections functions, as for example including the VBR contribution in the variable Q_locacc, is safe.

3.1 LOCALISATION OF THE TRAIN AT START OF MISSION

The ERSAT GGC project is well aware that the currently available GNSS technology is not yet able to supply, with the safety integrity requested for a railway purpose, a safety discrimination of the train position between adjacent tracks.

For this reason:

1) The virtual balise concept is not intended to support the first train localization at start of mission and to replace the balises intended to assure the safety of the system during this phase.

2) Before that the Virtual balise reader could identify the next virtual balise, the reader shall be initialized with:

   - the track_DB; which includes the position of the virtual balises related to each track and the related telegrams;
   - the track currently engaged by the train and the planned route.

   Only under these conditions, the Virtual Balise Reader is able to select, among the balises stored in the track DB, only the balises related to the track engaged by the train.

Therefore, it is important to assure that VBR is correctly initialized at the Start of Mission in each operative scenario and also in presence of degraded conditions.

According to this principle the start of mission phase, in addition to the operation already requested for ETCS L2 start of mission, shall also include the following operations to support the VBR initialization;

- the upload, or if already uploaded a consistency check, of the portion of the track DB necessary for the mission from the trackside equipment.

  Note: the trackside track DB cannot be changed after commissioning during service time while connected trains are using an already uploaded section of the DB.

- the initialization of the Virtual balise reader with the identification of the track engaged by the train.

Upload of the track DB

According to the ERSAT GGC project setup if a consistent copy of the Track DB is not already available on board, it can be uploaded by the trackside equipment using the Euroradio interface as soon as the train is accepted by the RBC.

The possibility to use the already available Euroradio interface for dynamically upload the Track_DB has been positively evaluated because the safety of the communications on this interface is already assured by a CENELEC 50159 compliant safety layers. However, it must be highlighted that, in order to assure the interoperability, the details of the messages to be used for this operation shall be defined and included in the ETCS message definitions.

In both cases, Track DB already stored or dynamically uploaded, the validity and the integrity of the track DB shall be safety checked before the SOM. To avoid any movement before the track DB is available and validated, the functional safety analysis has identified the need (see [Rif. 5] Req.001, Req.002, Req.003) to introduce a feedback toward the RBC of the completeness of the upload / verification operation.

This feedback makes the RBC able to avoid sending any movement authority to the train until the track DB is uploaded and checked for consistency.

Initialization of the VBR

The ERSAT GGC project includes different modalities to assure the initialization of the VBR at the start of mission which differ according to the current operative scenario (terminal station,

intermediate station) and to the availability of the current position (i.e value of the variable Q_Status)

To be confident that the VBR could be successfully initialized in all the possible, nominal and degraded, conditions the ERSAT GGC project has identified, analysed and defined within the test specification [Rif. 4] all the possible operative scenarios where the start of mission can take place.

This activity assumes, as nowadays ERTMS L2 applications, the presence of physical balises at terminal and intermediate stations to:

- assist the first train localization when the train position is UNKNOWN or INVALID;
- protect the railway system against undue movement in Staff Responsible mode.

The easiest scenario is when the train position is known (Q_Position = Valid). In this case the LRBG is known and therefore the train is located on the track.

To assist the localization of the train on the correct track, and therefore the VBR initialization, when the train position is unknown / invalid the ERSAT GGC architecture introduces the GAD/TV trackside subsystem. Purpose of this system is to identify the track engaged by the train at the moment of the request of the connection merging the information available from the interlocking (track status), the RBC (last NID_engine on the tracks engaged by a non connected trains) and the TMS (last NID_Operational on the tracks engaged by a non connected train).

It must be also noticed that the ERSAT GGC project does not mandatory ask for the presence on-board of the “Cold Movement detector” also if, when present, the presence of this device could help to Validate the current train position following the train Power–up.

Document [Rif. 4] gives evidence that, with the support of the functions planned to be included in the GAD/TV subsystem, the VBR can be successfully initialized in almost all the scenarios before the Start of Mission request and therefore before any movement of the train. The only scenario that does not allow the VBR initialization before to the Start of Mission is SoM9 ([Rif. 4]). SoM9 is degraded situation where:

- Q_Status: UNKNOW or INVALID
- RBC not able to associate the train to the track by means on the NID_ENGINE.
- TMS-RBC connection is NOT available.

In this scenario, and because according to [Rif. 5] REQ.017 must be prevented to provide any MA to the train before the VRB initialization, an authorization to “OVERRIDE” is requested to move the train on Staff Responsible modality. In this scenario the VBR will be initialized as soon as the first physical balise is reached.

As demonstrated by [Rif. 4] in all the other scenarios the train localization on the correct track, and therefore the VBR initialization, is always possible before the Start of Mission. After the SoM, if the train position is Valid, the RBC could send the first MA (OS/LS modes), otherwise if the train position is not VALID, and the location of the train along the track will be only approximate, the movement of the train can be authorized only in SR mode up to the next physical balise.

A special scenario is the Start of Mission along the line at the moment of the request of reconnection. In this case the identification of the engaged track, and therefore the VBR initialization is assured by the knowledge of the track engaged by the same train (same NID_Engine) before losing the connection.

In this scenario, because the next Virtual balise is known while the linking distance is not known, the safety analysis (see [Rif. 5] req.029) and [Rif. 6], H7-SR Apportionment, event: INDEP-CHK) has identified the need to validate the GNSS localization along the track with an independent source of localization.

Therefore it shall be noticed that the modalities to be applied to assure these mitigations are left open to the different implementations.

During the activities the assessor has analysed the results supplied by the ERSAT GGC project and agrees that, under the hypothesis of the presence of the physical balises in the stations to protect the railways system against undue movement in Staff Responsible mode, the modalities identified to assure the VBR initialization are safe and able to cover all the possible scenarios, without introducing additional constrains or limitation to the service.

3.2 LOCALIZATION OF THE TRAIN DURING THE MISSION

To evaluate the adequacy of the virtual balise reader to assure a safety localization of the train along the railway path during the mission are applicable all the considerations already developed at §2.3.1 (fault free conditions) and § 2.3.2 (presence of faults) about the GNSS accuracy and here below summarized:

1) The VBR reader is involved in the evaluation of the localization of the train along the path only at the moment of the detection of a virtual balise because the Virtual Balise localization accuracy shall be taken into account in the evaluation of the “safe distance confidence interval” requested by UNISIG SUBSET 041 §5.3.1.1 for the train localization.
2) The integrity of the Virtual Balise localization accuracy (i.e. the risk that the position of the Virtual balise is affected by an error greater that the declared accuracy) shall assure the integrity of the “safe distance confidence interval” as requested by UNISIG SUBSET 041 §5.3.1.1.
3) The ERSAT GGC has allocated to the hazard TRAN-VBALISE-3-SR (virtual balise insertion, which also includes the case the detection of a balise for the correct track but with a longitudinal error) the following THR:

   - THR (TRANS-BALISE-3-SR) = 0.66 E-9 h-1

   Of course it must be noticed that to achieve this target the Virtual balise localization accuracy given by the GNSS technology could be improved, as suggested by [Rif. 1] §6.3 or [Rif. 5] §9.2 “*odometry information based on the multi-sensor technology*”, using independent measurements. In this case the GNSS and the multi-sensor accuracies level shall be combined to calculate the overall location accuracy taking into account their own integrity.

With respect to this last point the assessor also notices that the availability of more independent measurements gives the maximum contribution to improve the overall accuracy when their accuracies (calculated at the same integrity level) are in the same order of magnitude, while a more accurate measure has always a stronger weight with respect to the less accurate measure. Therefore the contribution of the multi sensor odometer techniques could be significant to improve the GNSS accuracy only when its accuracy at the time of the measurement is more accurate, or at least not far, from the GNSS accuracy[6].

4) The achievement of the distance accuracy performance requirement ±(5m +5% s) defined by UNISIG SUBSET 041 §5.3.1.1 should be not critical because the Virtual balise allow to re-initalize the odometric errors more often just adding "virtual balises" in the data base. Also if the target of ±5m should not be reached when the VBR is detected (s=0) the reduction of the space between the balises allow the respect of the "average" accuracy target defined by the requirement.

3.3 LINKING FUNCTION

In the ETCS L2 system the linking function is intended to protect the system against the hazard "deletion of a balise group" and assures a protection with respect to:

- Trackside failure: silent balise groups;
- On board failure: loss of the BTM capability[7].

The introduction of the Virtual Balise Concept does not require any change on the linking function requirements and implementations but it has a significant effect on the BTM failures detection capability assured by the linking function.

In the VBR context the linking function will be always able to protect the system against loss of detection of Virtual balises both because failures of the VBR equipment or lack of the availability of the GNSS signals.

On the other side it must be noticed that the introduction of the VBR concept reduces the capability to detect failures of the BTM equipment nowadays assured each 2.5 km by the linking whenever a physical balise is met.

To overcome this problem the following approaches could be possible:

1) Update the "reference infrastructure" proposed by UNISIG subset 088-3 introducing an "average distance between physical balises". As consequence the THR nowadays allocate to the On-board equipment against the hazard "physical balise deletion" shall be also reviewed.

[6] this consideration could also help to define a criteria to define the optimal distance between the virtual balises

[7] according to the "reference infrastructure" proposed by UNISIG subset 088-3 some (1/1000) of the balise groups present on the line could be Unlinked. For this reason the loss of the BTM capability to detect a balise group is a hazardous condition.

2) Take into account the hazard at the moment of the design of the VBR equipped lines reducing the number of unlinked physical groups.

The first approach is the one applied by the ERSAT GGC safety analysis (see [Rif. 6] §5 "… *Then each on board supplier shall verify that this condition does not impact negatively the BTM safety performances considering the specific trackside project [ERSAT_GGC_D3.2_07]*) but it shall be noticed that this approach could impact the current BTM implementation which were designed according to THR nowadays introduced by the UNISIG specifications.

Contribution of the linking to the GNSS location accuracy

In the VBR context the linking function could also be used as consistency check of the GNSS location, or to improve the VB location accuracy given by GNSS, verifying if the travelled distance calculated by the Odometry function at the time of the detection of a new VB is compliant with the linked expected window.

This test could be useful to reject wrong GNSS measurements but, as already introduced at §3.2 it could give useful contribution to increase the GNSS accuracy only when the accuracy of the odometric measurement is more accurate, or at least of the same order of magnitude, of the accuracy supplied by the GNSS measurement but, in this case, the VB would not give any useful contribution to the re-initialization of the odometric errors.

4. SAFETY TARGET ACHIEVEMENT

Finality of the following paragraph is to supply an independent evaluation of the capability of the proposed "enhanced ERTMS architecture" (refer to [Rif. 1]) to assure the THR defined for the ETCS application by the UNISIG SUBSET 091 ver 3.6.0.

The current evaluation assumes "as fully and correctly managed" all the safety requirements identified by the ERSAT safety analysis [Rif. 5].

The chapter is organised according to the same approach proposed by the UNISIG SUBSET 091 which has been also applied by the ERSAT GGC project for the quantitative safety analysis [Rif. 6] and therefore the ETCS hazard is split into the following contributes:

- transmission hazard (THR allocated by UNISIG SUBSET 091 = 0.67 E-9/h);
- on board hazards (THR allocated by UNISIG SUBSET 091 = 0.67 E-9/h);
- trackside hazards (THR allocated by UNISIG SUBSET 091 = 0.67 E-9/h).

4.1 TRANSMISSION SUB-SYSTEM

According to the SUBSET 091 setup the "transmission" hazard is intended to collects all the contribution due to the non-trusted parts of the trackside<->on-board communications to the ETCS failure rate.

Therefore the TRASMISSION hazard receives contribute from: the radio sub-system and from the balise sub-system.

Radio sub-system

SUBSET 088-3 V 3.6.0 allocates to the RADIO sub system a contribution of 1E-11/h and therefore negligible with respect to the TRASMISSION THR. As consequence, the full THR available for the TRASMISSION event (0.67 E-9/h) is fully allocated to the balise subsystems.

This apportionment can also be considered valid for the enhanced ETCS architecture proposed because:

- the introduction of the GNSS technology to add the VB capability does not require any Hw or Sw changes on the radio subsystem which, in VBR context, will be also used to make available to the on-board and trackside sub-systems the additional data, as the track DB, the GNSS augmentation and the Track Verification, necessary to realize the VBR capability.
- the safety analysis has not identified additional hazards applicable to the RADIO sub system, due to the specificity of the VBR application, in addition to the hazards already identified by SUBSET 088-3 for the RADIO sub system.

Balise subsystem

SUBSET 088-3, FOR ETCS L2, allocates to the balise sub system the full THR available for the TRASMISSION (0.67 E-9/h). The BALISE sub system THR is split in the SUBSET in the following contributes:

- TRANS- BALISE-1 (corruption), THR = 1E-11 (contribute negligible);
- TRANS-BALISE-2 (deletion), THR = 3.3E-10;
- TRANS-BALISE-3 (insertion), THR = 3.3E-10.

Because of the introduction of the VBR capability, and in order to leave unchanged the overall hazard rate due to the transmission subsystem, the here above hazards shall also collect the contribution given by the VBR capability.

The effect of the introduction of the VBR capability on the here above recalled event hazard rate is evaluated in the following paragraphs.

4.1.1 TRANS-BALISE-1

Top hazard	TRANS-BALISE-1 (corruption) Incorrect balise group message received by the on-board kernel functions as consistent (Subset 088-3 §4.1.1.1, ver 3.6.0).
SUBSET 091 safety requirements	ETCS_OB06
THR allocated by SUBSET 088-3	THR 1E-11 (against failure of the untrusted part).

Hazard TRANS-BALISE-1 represents the contribution to “transmission function” HR given by an undetected corruption of a balise telegrams.

The introduction of the Virtual Balise does not impact on the mitigations already applied to assure the integrity of the Physical balise as: code strategy of the Eurobalise airgap and of the BTM <-> EVC core communication but a new initializing event, corruption of the virtual balise telegram, shall be taken into account for the virtual balise context.

According to the performed safety analysis, possible causes of corruption of a virtual balise message could be:

a. loss of Integrity of the image of the track DB upload on-board
b. lack of consistency of the on-board image of the track DB with the trackside track-DB
c. start of mission without valid and updated track DB
d. loss of integrity on the internal VBR / EVC Core interface

which appears to be fully mitigated by the safety requirements identified by [Rif. 5] here below recalled:

a. all the interfaces involved in the track DB upload, if not already preloaded, (EURORADIO interface and GAD/TV –RBC) are protected according to EN 50159 standard (see: REQ.015);
b. the version of the track DB is verified as soon as the RBC-EVC communication is established (see: REQ.004);
c. GAD/TV requires an acknowledge of the track DB verification before to allow the RBC to send any MA or allow train movements (see: REQ.001, REQ.002, REQ 003);
d. protection of the internal VBR – EVC core interface according to EN 50159 standard (see: REQ.012) (as assured by the on board suppliers for the BTM <-> EVC core interface).

The assessor, taking into account the identified mitigations, agrees that the contribution to TRANS-BALISE-1 hazard rate introduced by the VBR technology can be evaluated as negligible as evaluated by the ERSAT GGC quantitative safety analysis [Rif. 6] table 7.

4.1.2 TRANS-BALISE-2

Top hazard	TRANS-BALISE-2 (deletion) Balise group not detected by on-board kernel functions (Subset 088-3 §4.1.1.1 ver 3.6.0).
Related SUBSET 091 safety requirements	ETCS_OB07
THR allocated by SUBSET 088-3	TRANS-BALISE-2 < 3.3 * 10-10 dangerous failures hour-1(Subset 088-3 §11.2.1.2 ver 3.6.0). Note:

	Starting from the TRANS-BALISE-2 THR, SUBSET 088-3 also allocates the maximum contributes due to the information point and on board failure according to following equation: ➢ $R_{NL} = r_{NL}$* PDR *((λIP * 24h) +(λONB * T_{NL}) (SUBSET 088-3 Ver 3.6.0 §11.2.1.2) Where T_{NL}: is "the duration of an on-board failure when on-board linking checks are not active". and specifically allocates to the Onboard system failure rate contribution 1E-7 failure/h It must be noticed that, because the T_{NL} parameter depends of the medium time to next link with a physical balise, the introduction of the VB could impact the allocation of the THR supplied by sebset 088-3.

Hazard TRANS-BALISE-2 represents the contribution to "transmission function" HR given by the loss (i.e. the kernel does not receive the expected packet) of a balise, that in the ERSAT-GGC context, could be both physical or virtual.

The main mitigation applied by ETCS L2 to mitigate the loss of physical balises is the linking. Additional contributions applicable to the mitigation against "physical balise deletion" are the continuous integrity test of the on-board BTM equipment and the redundancy of the physical balises. These additional mitigations are necessary in ETCS L2 to cover the scenario of unlinked physical balises that is included in the SUBSET 088-3 reference infrastructure.

However the scenario of unlinked balises (i.e next expected Vb unknown) is not applicable for the VB context because, according to the constraints identified by the functional safety analysis, the VBR, to acquire a VB shall be initialized and the next expected balise shall be always known (see [Rif. 5] REQ.018)

With reference to the scenario of "next expected virtual balise known" the countermeasure which assures the mitigation of the balise deletion hazard is the linking function that is fully applicable both to the loss of physical and the virtual balises. The introduction of the virtual balise does not introduce changes because VBR is fully transparent to the linking function and specifically to the modalities applied by the on-board to calculate the linking window and to verify the congruence between the balise position and the linking window. The only matter relevant to the VB context is that, when the link is established by a virtual balise, the linking window extension shall also take into account the safe location accuracy of the LRBG that establishes the linking.

Specifically the VBR does not supply any contribution to the computation of the travelled distance between two BG and as consequence the VBR does not play any role either in:

- the generation of the "link error" when the train exits from the linking windows before that a new balise, physical or virtual is detected.
- the verification of the consistency of the travelled distance with respect the linking window when a new physical or virtual balise is detected;

Therefore, thanks to the independence between the VBR and the linking function, the mitigation assured by the linking function to the hazard “balise detection” is fully applicable also to the VB context.

Moreover additional mitigations, based on continuous VBR integrity check, have been introduced by the functional safety analysis to strengthen the protection against the VB deletion event (see [Rif. 5] REQ.006, REQ.007, REQ.010, REQ.011, REQ.019).

Unlinked balises

Because VB are not intended to support the first train localization at terminal or intermediate stations, the only scenarios of ”virtual balise with unknown linking distance” to be taken into account is the “Start of Mission in line with unknown position”. This is a rare scenario conceivable only following the management of a failure. The deletion of a virtual balise in this scenario must considered a hazard because, until the first balise is acquired, FS mode can not be assured to the train. The contribution due of this hazard to the system hazard is taken into account by the quantitative hazard analysis [Rif. 6] by the event TRANS-VBALISE2-SR (see §11.3.1 scenario start of mission in line).

The THR allocated by the quantitative hazard analysis to this event is 1E-10/ h (see [Rif. 6], table 8). The value of 1E-10 is defined by [Rif. 6] §11.3.1 in order to reach, jointly to the contribution allocated to the other applicable hazards (see §4.1.3) the THR allocated on the balise subsystem.

The allocation of THR = 1E-10 h/1 for the hazard TRANS-VBALISE2-SR could be appears as a severe requirement but it must be noticed that it just applies to situation of deletion of the first VB present after a start of mission. Therefore, the exposure to the risk is significant low.

Impact of the introduction of the virtual balises function versus physical balises deletion hazard.

As already introduced at §3.3, the introduction of the virtual balises also impacts on the hazard “unlinked physical balise deletion”. The introduction of the VB impacts on this hazard because the time to detection of BTM on board failures could increase as consequence of the reduction of linking with physical balises which assure the complete test of BTM capabilities.

As consequence the reference scenario assumptions[8] applied by SUBSET 088-3 to establish the THR of on-board failures able to lead to the event “physical balise deletion” shall be reviewed, taking also into account an updated reference structure. After that the current on-board implementations should be re-checked against the updated THR (see also ERSTAT GGC safety analysis (see [Rif. 6] §5). To avoid this problem, the assessor also recommends to evaluate also other possibilities as the introduction of infrastructure design rules able to avoid the presence of unlinked physical balises, as TSR set by balises, on the line equipped with virtual balises.

Virtual balise deletion hazard conclusions

Taking into account that the working modality of the VBR requires that:

[8] specifically the parameter T_{NL}, “duration of an on-board failure when on-board linking checks are not active” should be reviewed because it depends on the number of physical balises met by the train

- the next expected VB is always known;
- the expected linking distance is always known with the only exception of the scenario of SOM in line;
- the availability of the VBR function is continuously monitored,

it is possible to confirm that the Hazard “virtual balise deletion” is fully mitigated and that its contribute to the “transmission function” can be evaluated as negligible in agreement to the result of [Rif. 6] §9.1.

As conclusion, the assessor agrees that the proposed architecture and safety requirements should assure an adequate mitigation against the event virtual or physical balise deletion, and that the contribute of the VBR given to the hazard TRANS-BALISE-2 due to a virtual balise deletion could be evaluated as negligible

4.1.3 TRANS-BALISE-3

Top hazard	TRANS-BALISE-3 (insertion / cross talking) Inserted balise group message received the on-board kernel functions as consistent (Subset 088-3 §4.1.1.1 ver 3.6.0).
Related SUBSET 091 safety requirements	ETCS_OB08
THR allocated by SUBSET 088-3	The maximum tolerable rate for cross talk leading to the ETCS Core Hazard from adjacent information points encountered in 1 hour TRANS-BALISE-3 < 3.3 * E-10 dangerous failures hour-1 (Subset 088-3 §5.2.4.3 amended apportionment for the TRANS-BALISE-3)

Hazard TRANS-BALISE-3 represents the contribution to “transmission function” HR given by the insertion of a balise, that in the VBR context, could be both physical or virtual.

Possible causes of balise insertion could be the acquisition of a balise related to an adjacent track (cross talking), the acquisition of the undue messages because the coupling with Euroloop cables (scenario not applicable to Virtual balises) or also a longitudinal error along the track while the position of balise along the track is determined.

Insertion because cross talk

The first cause of balise insertion, “cross talking”, is protected by ETCS L2:

- For linked balises: by means of the linking function and by all the other measures applicable for unlinked balise.
- For unlinked balise: by means of the antenna irradiation patterns, the limitation of tele-powering and by the check of consistency of the telegrams acquired by different balises of the same group.

In the Virtual Balise context, and because as already recalled at §4.1.2 the VBR initializations assures the identification of the next expected VB, unexpected (because intended for other tracks) VB will not detected by the VBR.

It must be noticed that the VBR initialization is assured by the GAD/TV also in the scenario SOM of mission in line comparing the NID_engine and/or NID_Operational of the train supplied at the moment of the re-connection with the data stored by the track side equipment related to the tracks engaged by a non-connected trains.

This procedure assures the VBR initialization also in this scenario also if the distance to the next VB is not known because the train position inside the track section is only approximately known

The contribute of the SOM in line scenario failure rate due to VBR initialization process is taken into account by the quantitative safety analysis by the event H9-SR (THR 0.33 E-9/7h) (see [Rif. 6], figure 6)

To demonstrate also by experimental tests the immunity of the VBR with respect to the cross-talk hazard the functional and not functional test specification [Rif. 4] had included a set of tests focused on specific potential cross talking scenario as:

- the presence of a virtual balise related to the adjacent track but inside the GNSS accuracy radius,
- little reverse movement next to the virtual balise position,
- double passages on the balise because of a turn-out.

Insertion because longitudinal error

The second cause of balise insertion is the occurrence of a longitudinal error when the balise location is established. In the VBR context, this event occurs whenever a balise is detected and its telegram is sent to the EVC core but the distance between the actual train position and the nominal position of the VB is larger than the declared safety accuracy.

The protections assured by the ERSAT design against this hazard are:

- the calculation of the safety of accuracy given by GNSS (that shall include both the contribution to the localization error in fault free conditions and the contribution due to the failures)
- the linking window, this because VB detected outside the linking window can be ignored.

With reference to the effectiveness of linking window to protect against the hazard “Insertion because longitudinal error” it must be noticed that:

1) the mitigation supplied by the linking window is not applicable to the scenario “start of mission in line” because, in this scenario, the distance to the next VB is unknown. This condition is taken into account by the quantification of the hazard rate of the scenario “SOM with Q_STATUS= “Unknown” in line (see [Rif. 6], §11.3).
2) the presence of an active linking window:

- when the GNSS measurement falls out of the linking window permits the rejection of wrong GNSS measurements,
- when the GNSS measurement ± GNSS accuracy falls inside the linking window, the linking window can only confirm that the actual position is included in the window while cannot confirm the correctness of GNSS accuracy (which could be significant closer than the linking window).

  In this case to improve the GNSS accuracy, the accuracies given by the odometry and by the GNSS measurements, should be combined taking into account their error probability or, in alternative, the fully extension of linking windows should be taken into account as safety confidence interval.

SOM with Q_STATUS= "Unknown" HR allocation

According to the result of the hazard analysis the only scenario which gives contribute to the hazard "insertion because longitudinal error" is the scenario SOM with Q_STATUS= "Unknown" because in this scenario, also if the next expected VB is known, the linking distance is not known.

The tolerable hazard allocation for this scenario is available at [Rif. 6], §11.3.

The quantitative analysis ([Rif. 6], table 8) allocates to this scenario the whole Tolerable Hazard rate assigned by Subset 088-3 to the "balise Subsystem hazard (TRANS-BALISE-1, TRANS-BALISE-2, TRANS-BALISE.3) and therefore allocates to this scenario a THR of 0.67 E-9 /h.

This choose could be misunderstood because it seems that does not take in account the contribution given to the "balise sub system" hazard rate due to the BTM failures and shall be reviewed, as already agreed by the D3.2 leader (see [Rif. 12] question 5), in the next D3.2 release

However, considering that virtual and physical balises are mutually exclusive, and that their contributions shall be weighted, the difference appears not significant.

The next step performed by the hazard analysis is the allocation of the available THR (0.67 E-9/h) on the sub-hazards (TRANS-VBALISE-1-SR, TRANS-VBALISE-2-SR, TRANS-VBALISE-3-SR).

Considering that the contribution of TRANS-VBALISE-1 (corruption) can be evaluated as negligible because of the available protections, the quantitative analysis distributes the available THR between TRANS-VBALISE-2, TRANS-VBALISE-3 in following way:

- TRANS-VBALISE-2-SR (deletion): THR = 1.0 E-10 /h
- TRANS-VBALISE-3–SR (insertion): THR = 0.66 E-9 /h.

AS already introduced at § 2.3.2, the hazard "deletion" has been taken into account in this scenario because in this scenario the event does not permit to assure full supervision. The THR allocated to TRANS-VBALISE-2-SR appears to be reasonable considering that the event "VB deletion" is hazardous only in this scenario and considering the low frequency of the scenario.

The TRANS-VBALISE-3–SR (insertion) THR is then split between:

1. Longitudinal error (H7-SR); THR = 0.33 E-9 /h.
2. Cross talk error (H9-SR); THR = 0.33 E-9 /h .

With reference to the longitudinal error hazard (labelled by [Rif. 6] as H7-SR) considering that:

3) the GNSS integrity (which, according to the GNSS_MI event development included at §11.3.4, also includes the fault-free error contribution) according to the current state of the GNSS technology and taking into account the contributions of the RAIM algorithm and the augmentation system is about 7.5 e-6 failure/h,

4) the THR allocated to this event is 0.33 E-9.

the hazard analysis has identified the need to improve the safety by means of an independent check able to assure a risk reduction of 4 E-5 h-1 (see event INDEP-CHK). Therefore it must be noticed that the modalities to assure this independent check are not defined by the proposed ERTMS enhanced architecture and are demanded to the on-board – trackside equipment suppliers.

4.2 ONBOARD-SUBSYSTEM

According to the THR apportionment, method applied by SUBSET-088-3 V 3.6.0 the event “ETCS On-board failure” is intended to collect all the contributions to the ETCS hazard rate given by the failures of the trusted parts of the ETCS on-board sub-system.

The target allocate to the ETCS On-board constituent is 0.67E-9 dangerous failures / hour (SUBSET-088-3 §7.1.1.2and §7.3.1.1)

The SUBSET-088-3, also if does not develop a more accurate apportionment of the ETCS On-board THR, requires that at least the hazardous events listed by the standard at §7.1.1.3, are taken into account by the suppliers in order to prove the achievement of the assigned hazard rate.

The ERSAT GGC quantitative safety analysis (see [Rif. 6] §7.1.1) is fully compliant with the standard guidelines including all the contributions already requested by the standard, while to take into account the contribution due to the introduction of VBR, the analysis adds:

- adds a new basic event ‘VBR-H4’ which represents the contribution due to the failures of trusted parts of the on-board subsystem able to deliver an erroneous telegrams interpretable as correct to the failures list of the VBR function

  note because a balise could be either Physical or Virtual the event VBR-H4 is, for each balise, exclusive to the event ‘BTM-H4’.

- modifies the definition of the event OB-EUR-H4 just to specifies that this contribution shall also take into account the radio messages related to the GAD/TV capabilities.

Moreover it must also be noticed that the ERSAT GGC quantitative safety analysis does not identify any impact on the other events which give contribution to the ETCS On-board hazard rate and specifically on hazards coming from the odometry constituent.

The approach applied by ERSAT GGC quantitative safety analysis can be agreed because, also if the odometry subsystem receives from the VBR the Virtual balise safe location confidence interval (which shall be taken into account to determinate the “safe distance confidence interval requested by SUBSET 041 §5.3.1.1”), the contribution to the application Hazard Rate given by failures that could impact the safety of this parameter are already taken into account in the evaluation of the

Communication sub-system hazards and specifically on the event TRANS-BALISE -3 (insertion) as already evaluated at §4.1.3.

With respect to the THR hazard allocation the ERSAT GGC quantitative safety analysis does not identify the need to modify the THR nowadays allocated to the on board sub-system because it is confident that the already defined THR is fully achievable by the on-board sub-system also after the integration of the VBR capability.

The assessor agrees on this approach because:

1) the hazardous failure rate of the VBR can be reduced by the on-board suppliers to a negligible contribution including in the VBR design redundancy and self-testing as already identified by the ERSAT safety analysis [Rif. 5] REQ.009 (redundancy) and REQ.006, REQ 010 (self test).

2) the presence of the VBR permits to reduce the number of physical balises present on the line and therefore the contribution due to the basic event BTM-H4 (related to Physical balises) should decrease.

   Note: to perform a more accurate evaluation of the weight of the event BTM-H4 and VBR H4 on a line equipped with virtual balises should be necessary to include this scenario in the reference infrastructure defined by subset 088-3.

3) the management of the Euroradio messages related to the GAD/TV functions is not really complex and does not require new hardware; therefore its contribute appears not significant.

4.3 TRACKSIDE SUBSYSTEM

According to the THR apportionment method applied by SUBSET-088-3 the event “ETCS trackside failure” is intended to collect all the contributions to the ETSC hazard rate given by the failures of the trusted parts of the ETCS trackside sub-system.

The target allocated to the ETCS Trackside constituent is 0.67E-9 dangerous failures / hour (SUBSET-088-3 §8.1.1.3 and §8.3.1.3)

The SUBSET-088-3, also if does not develop a more accurate apportionment of the ETCS Trackside THR, requires that at least the hazardous events listed by the standard at §8.1.1.4, are taken into account by the suppliers in order to prove the achievement of the assigned hazard rate.

The ERSAT GGC quantitative safety analysis (see [Rif. 6] §8.1.1) in order to take into account the contribution due to introduction of VBR capability, includes the contribution to the ETCS hazard rate due to the GAD/TV sub-systems in the event TR-EUR-H4, while the other basic events requested by the standard RBC-2, RBC-3 and RBC-4 are left unchanged.

With respect to the THR hazard allocation the ERSAT GGC quantitative safety analysis does not identify the need to modify the THR nowadays allocated to the trackside sub-system because it is confident that the already defined THR is fully achievable by the trackside sub-system also after the integration of the VBR capability.

The assessor agrees on this approach because:

4) the hazardous failure rate of the GAD/TV can be reduced by the trackside suppliers to a negligible contribution including in the GAD/TV design safety architectures and self-testing as already identified by the ERSAT safety analysis [Rif. 5] REQ.006 and REQ.010

5) the management of the Euroradio messages related to the GAD/TV functions is not really complex and does not require new hardware; therefore its contribute appears not significant.

5. PRODUCT ASSESSMENT AND CERTIFIABILITY ASPECTS

This chapter submit to the attention of the ERSAT GGC project partners some aspects that have to take in consideration for the next steps of the project in order to make assessment and certification possible.

For safety aspect will be considered that:

1) according to ERSAT GGC safety analysis the VBR shall report to the EVC-core train protection functions the virtual balise location accuracy assuring the achievement of a safety integrity compliant with THR allocated on the event TRANS-BALISE-3-SR. The modalities to reach this target, as example integrating the GNSS information with the contribution of a multi-sensor odometry techniques or with the contribution of the linking function, have to be developed in detail.

2) The lack of physical balises along the line could impact on the time necessary to the On board systems to detect failures related to the BTM equipment and, therefore, could also impacts on the BTM THR achievement.

   The BTM failure detection time is a parameter used by SUBSET 091 to evaluate the hazard rate of the following scenarios:

   a) deletion of un-linked information points when the on-Board linking checks are active (subset 091 §6.3.2). The most relevant scenario identified by the subset 091 for this class of scenarios is a TSR set by physical balises. For this scenario subset 091 assumes a BTM detection time of 0.025 h (see §6.5.2.7), detection time that could not be assured by all the implementations without physical linking. To avoid this problem it could be necessary introduce an operative rule in order to avoid the setting of TSR by means of physical balises along lines equipped with virtual balises.

   b) deletion of un-linked information points when the on-Board linking checks are not active (subset 091 §6.3.3). For these scenarios subset 091 assumes a BTM detection time of 1 h (§6.4.2.10). Therefore, to assure the respect of this assumption at least 1 link with a physical balise shall be assured each operative hour.

With reference to the certifiability of the proposed enhanced architecture it is necessary to underline that any proposal of change, or/and introduction of new technologies could not live aside the interoperability aspects and therefore that a certification of a trackside or/and on-board system which implements the VBR concept requires the introduction of the VB concept in the interoperability specifications.

With reference to this context the assessor confirms that the ETCS enhanced architecture submitted to the attention of the assessor allows to leave unchanged the structure of the interoperability specifications, but, to allow the development of interoperability applications by different suppliers, it seems necessary to integrate the interoperability specifications at least for the following:

- It should be introduced the VBR, GAD and TV functions, their safety and functional requirements and test specifications as already available for other function like BTM and odometry.
- The definition of the ETCS messages shall be reviewed, including in the interoperability specifications: the definition of the messages necessary to upload the track database, to disseminate the GNSS augmentation system data and to perform the Track Verification function because these information shall be make available to all the on-board systems in a standardized way.

A further aspect that can be critical at the scope of the certifiability is how to assess the safety performance of the algorithms in charge to validate the integrity of the GNSS system, including the SIS, and in charge to calculate the current position accuracy.

This is a not immediate task also because each on-board supplier could implement different techniques as single/multi constellations receivers or implement either track constrained or track un-constrained solutions. Moreover, it shall also be taken into account that the safety of the VBR outputs depends also on the contribution given by the augmentation systems, contribution that, according to the interoperability principles, shall be supplied in a standard way from any interoperable trackside to any interoperable onboard.

A real help to assist the certification could arrive from the definition of a standard test specification for the “space + augmentation system interoperability interface”. This test specification could be based on different scenarios of the satellite signals including error conditions, deletion of satellites, noise, that, jointly with the expected augmentation system data, could be used to exercise the VBR constituent.

A criteria to evaluate the safety performance of the different implementations could be based on the comparison among the error of the position supplied by the EUT with respect the nominal position given by the scenario and the standard deviation of the position calculated by the equipment itself.

According to this criteria the implementation could be evaluated as safe whenever:

1. the position error is lower that the real time calculated standard deviation for at least 68% of the measurements;
2. adequate evidence about how the location safe confidence interval is calculated from the GNSS standard deviation, also jointly with the contributes of any additional techniques, is supplied

The same test specification could be also useful to evaluate the functional performances evaluating the average safety location confidence interval.

6. CONCLUSIONS

The aim of the present ISA activity was to carry out an independent evaluation of the Enhanced Functional ETCS L2 architecture and of the impact due to the introduction of the Virtual Balise Concept on the ETCS L2 safety and functional performances, while is out of scope of this report the evaluation of Generic Products or Generic Applications.

The project activity was carried out on the base of the ERSAT GGC WP2 and WP3 deliverables and taking into account, as reference, the safety and functional requirements defined by the ETCS B3 R2 GSM-R R1 set of specification.

The performed activities confirm that the proposed “ETCS architecture” well matches with the current ETCS trackside and on-board ETCS architectures and that the changes to be applied to realize the enhanced architecture are well defined.

Moreover the performed activities confirm that the proposed enhanced architecture, when developed according to the identified safety requirements, appears able to assure a significant reduction of the Information Point nowadays present on the lines, assuring the respect of the same safety and functional targets nowadays assumed as reference for ETCS L2 applications.

REFERENCES

Rif. 1 ERSAT GGC_WP2 D2.1, “Enhanced Functional ERTMS Architecture Capable of using GNSS and Public Radio TLC Technologies”, Rev 02.

Rif. 2 ERSAT GGC_WP2 T2.1.8, “Definition, Model and Verification in MatLab of Railway RAIM”, V01.

Rif. 3 ERSAT GGC_WP2 ERTMS operational scenarios, V02.

Rif. 4 ERSAT GGC D2.2 Functional and Not Functional Test specification”, V03.

Rif. 5 ERSAT GGC_WP3 D3.1, “Safety Analysis of ERSAT ERTMS Application over GNSS”, Rev 02.

Rif. 6 ERSAT GGC_WP3 D3.2, “GNSS Quantitative Analysis for ERSAT GGC Project” rev 02

Rif. 7 UNISIG SUBSET-041 Performance Requirements for Interoperability, V 3.1.0.

Rif. 8 UNISIG SUBSET-088-3 ETCS Application Levels 1 & 2 - Safety Analysis -Part 3 - THR Apportionment, V 3.6.0.

Rif. 9 UNISIG SUBSET-091 Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, V 3.6.0.

Rif. 10 UNISIG SUBSET-036 FFFIS for Eurobalise, V 3.1.0.

Rif. 11 CENELEC EN 50126-1 2017 Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part -1 generic RAMS process.

Rif. 12 note ERSAT-GGC D5.1 review RINA-C BVI_20190521.