CERTIFICATION OF EGNOS SAFETY-OF-LIFE SERVICE FOR ERTMS ACCORDING TO IEC 61508 AND EN 50129

ALEŠ FILIP
Faculty of Electrical Engineering and Informatics, University of Pardubice, Czech Republic

ABSTRACT

A number of research projects are currently focused on the replacement of track balises (used for safe train position determination) with Virtual Balises (VBs) detected by GNSS to increase the efficiency of the European Rail Traffic Management System (ERTMS). The exploitation of the EGNOS Safety-of-Life (SoL) service, which is the European GNSS wide-area augmentation developed for aviation, for Virtual Balise Reader (VBR), should further strengthen the interoperability of ERTMS. In order to meet the high Safety Integrity Level required for VB detection (SIL 4), EGNOS-based train position determination in combination with other on-board sensors must be used. The adoption of EGNOS, which was not designed according to CENELEC railway safety standards, shall pass through a railway certification process to demonstrate that all demands on safety, dependability and interoperability have been met. This article proposes certification of the EGNOS SoL service for ERTMS via a so-called "pre-existing" item in the sense of the IEC 61508 and EN 50129 standards. The pre-existing item means an item that already exists and that was not specifically developed for the current project. The proposed solution starts with the use of Common Safety Method for Risk evaluation and Assessment (CSM-RA) that must be applied according to the EU Regulation No. 402/2013, because the safety change in ERTMS is significant. Since EGNOS alone is not able to meet the safety integrity requirement for VB detection, then EGNOS shall be correctly integrated within the VBR constituent. This article suggests that all essential information on EGNOS required for its integration into the VBR subsystem would be contained in the EGNOS Safety Manual. The Safety Manual, together with its assessment report, would be then referred in the section entitled "Related Safety Cases" of the overall Safety Case according to EN 50129.The presented results contribute to the introduction of EGNOS into ERTMS.

Keywords: certification, EGNOS SoL service, ERTMS, pre-existing item, safety case, virtual balise.

1 INTRODUCTION

The European Train Control System (ETCS), which is a part of ERTMS, employs track balises with known position for safe train position determination. These physical balises are detected on board of train by means of a so-called Balise Transmission Module (BTM). Besides Europe, ERTMS/ETCS has also become successful in Asia – especially in China, Turkey, Taiwan and South Korea. However, additional installations of ETCS with classical track balises on heavy haul and other lines may not be in some countries efficient (Australia, Russia, China, etc.) – mainly due to high investment and maintenance cost of ETCS balises.

The European Commission is aware of these ETCS limitations and therefore gradually initiated different R&D projects oriented on the use of Global Navigation Satellite System (GNSS) for signalling and ERTMS, such as 3InSat (2012–2015), ERSAT EAV (2015–2017), RHINOS (2016–2018), STARS (2016–2018), ERSAT GGC (2018–2020), STEMS (2018–2020), HELMET (2020–2022), etc. The exploitation of the European Geostationary Navigation Overlay Service (EGNOS), which is the European GNSS wide-area augmentation developed for aviation, for Virtual Balise Reader (VBR) within Virtual Balise Transmission Module (VBTM) is critical in this concept. The common objective of the above projects is to integrate the two large pan-European infrastructures (ERTMS and EGNOS) and, in addition to greater operational efficiency, to further enhance the interoperability of ERTMS.

WIT Transactions on The Built Environment, Vol 199, © 2020 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/CR200111

The interoperability is a key feature of ERTMS. It ensures the correct technical interaction among on-board and track-side subsystems shared between different stakeholders, mainly Infrastructure Managers and Railway Undertakings. High safety and dependability requirements (i.e. RAMS: Reliability, Availability, Maintainability and Safety) for ERTMS must be met; also in cases when track balises are replaced with virtual balises and detected by GNSS – see e.g. ERSAT GGC project [1]. Therefore, it is necessary to pass the certification and approval process that guarantees all requirements for ERTMS (i.e. safety standards CENELEC EN 5012x [2]–[5], EN 50159 [6], Technical Specifications for Interoperability (TSIs), EU regulations, directives, etc.) are met. The EU Directive 2016/797 [7] extends authorization process of Control Command Systems (CCS) to the entire railway system – it supports concept of “cross-acceptance” as a steppingstone to the interoperability within the Trans European Network.

Railway stakeholders have to safely manage changes of the European railway system – including GNSS/EGNOS integration with ERTMS. Except Verification and Validation (VaV) and Safety Case development, system compliance with Control Command and Signalling Technical Specifications for Interoperability (CCS TSIs) should be checked – see [7]–[9]. VaV reports and Safety Case including assessment reports are important inputs for the certification process. The European railway sector utilises Common Safety Method for Risk evaluation and Assessment (CSM-RA) [10], [11] for harmonisation of risk assessment. CSM-RA harmonises in fact the whole Risk Management Process. It also creates a framework for certification and safety approval process of railway technical systems. It is evident that EGNOS shall also pass the certification process to ensure that all requirements for ERTMS safety and interoperability are met.

The safe exploitation of the aeronautical EGNOS SoL service in railway signalling primarily means that the SoL service must be employed according to CENELEC railway safety standards (EN 50126 [2], EN 50128 [4], EN 50129 [5], etc.). However, this has been a major obstacle to the EGNOS cross-acceptance for ERTMS for many years, since EGNOS was developed according to aviation safety standards and not according to railway CENELEC safety standards.

This article proposes that the EGNOS SoL service could be cross-accepted and certified for ERTMS via a so-called “pre-existing” item in the sense of the IEC 61508 [12] and EN 50129 [5] safety standards. It is further suggested that all essential information regarding EGNOS required for its integration into the ERTMS VBR subsystem would be contained in the EGNOS Safety Manual that would be then referred in the overall Generic Safety Case.

Section 2 describes basic requirements for safety assurance of railway Control Command and Signalling (CCS) systems. The cross-acceptance process according to CENELEC standards used in railway signalling is outlined in Section 3. The EGNOS cross-acceptance for ERTMS according to EN 50129 via pre-existing item is suggested in Section 4. Finally, the achieved results are summarised in Section 5.

2 SAFETY ASSURANCE OF RAILWAY SIGNALLING SYSTEMS

This section outlines a methodology to apply the current safety assurance procedures used in the railway sector to the exploitation of EGNOS and its related safety services for the application of the ERTMS Virtual Balise concept as explained in this article. It suggests that there should be an interface established between the current application of EGNOS in the aviation sector and its application in the railway sector. The approved EGNOS service provider then has the same relationship with the railway sector as with any aviation services. The adoption of EGNOS SoL service for ERTMS is then narrowed to the Safety and Risk Management processes of the EGNOS interface. Therefore, there will be an interface document setting out the services to be provided to the railway sector that will effectively be the same for all users of the service.

An important part of the interface document shall be a Safety Manual, which is a user guide for designers and systems integrators enabling safe EGNOS integration with ERTMS without compromising safety. The EGNOS Safety Manual is the fundamental document enabling cross-acceptance of EGNOS in the railway sector. The idea of the safety manual describing EGNOS interface and enabling safe EGNOS integration with ERTMS represents the main topic in this paper.

The safety manual shall be developed and approved in line with the railway Safety Management Process according to railway CENELEC standard EN 20129 [5] and also used within Risk Management Process according to CSM-RA, as it is required by the EU Regulation 402/2013 [10], [11]. The differences between the Safety and Risk Management processes are outlined in sections below.

2.1 Safety management and CENELEC standards

2.1.1 EN 50129 [5]

The standard EN 50129 is applied in conjunction with EN50126:2017 (part 1 and part 2; [2], [3]) which addresses safety-related requirements applied to the whole railway system. EN 50129 addresses the measures required to provide confidence in the safety of safety-related electronic system to be used in railway signalling systems. The interface between the two standards consist of two subjects; the overarching RAMS context, and the development of the safety case and the life cycle. Intrinsic to both these subjects is risk assessment, which is the subject of the CSM-RA regulation [10]. EN 50129 defines the conditions that shall be satisfied in order that a safety-related electronic railway system/sub-system/equipment can be accepted as adequately safe for its intended application. The conditions for safety acceptance are the following:

- Evidence of quality management;
- Evidence of safety management;
- Evidence of functional and technical safety.

All of these conditions shall be satisfied, at equipment, sub-system and system levels, before the safety-related system can be accepted as adequately safe. The documentary evidence that these conditions have been satisfied shall be included in a structured safety justification document, known as the Safety Case. The Safety Case forms part of the overall documentary evidence to be submitted to the relevant safety authority in order to obtain safety approval for a generic product, a class of application or a specific application.

2.1.2 Purpose of safety management process

Safety management process is that part of the RAMS management process which deals specifically with safety aspects – see EN50126-1 [2]. The above-mentioned evidence of safety management represents one of three basic conditions for safety acceptance of the railway safety-related system. The use of this safety management process is mandatory for Safety Integrity Levels (SILs) 1 to 4 inclusive. However, the depth of the evidence presented, and the extent of the supporting documentation should be appropriate to the SIL of the system/sub-system/equipment under scrutiny.

The documentary evidence to demonstrate compliance with all elements of the safety management process throughout the life cycle shall be provided in the Safety Management Report, which forms Part 3 of the Safety Case [5]. The purpose of this process is to further reduce the incidence of safety-related human errors throughout the life cycle, and thus minimise the residual risk of safety-related systematic faults.

2.2 Risk management process according to CSM-RA

Single implementation of Safety Management process in accordance with CENELEC safety standards is not enough for application of an EGNOS service in railway signalling and train control. Since the introduction of an EGNOS service into ERTMS/ETCS represents a significant change within the European railway network, then a so-called Common Safety Method for Risk evaluation and Assessment (CSM-RA) according EU legislation must be applied [10], [11].

CSM-RA (Regulation (EU) 402/2013 [10]) covers the following activities: 1) Risk assessment process and demonstration of compliance with the safety requirements, 2) Hazard Management and 3) Independent Assessment by CSM Assessment Body (AsBo).

CSM risk assessment is compliant with the CENELEC life cycle. However, the safety monitoring during real system operations is not covered by the harmonised risk assessment within CSM-RA. In order to achieve full compliance of CSM-RA with the CENELEC life cycle, CSM-RA requires a separate Safety Management System to be implemented and provided within activities of the proposer of the significant change. The proposer can be i.e. a railway undertaking, an infrastructure manager, an entity in charge of maintenance, etc.

CSM-RA enables mutual recognition of results including harmonization of risk acceptance and safety requirements in EU Member States. Harmonization and mutual recognition of safety requirements is performed via Risk Acceptance Principles (RAP) and Risk Acceptance Criteria (RAC). CSM-RA is in fact the iterative process. The iterative risk assessment process is completed when it is demonstrated that all safety requirements are fulfilled, and no additional reasonably foreseeable hazards have to be considered.

Widely acceptable Codes of Practice (e.g. CCS TSIs, CENELEC standards, etc.) such as Risk Acceptance Principles enables one to harmonise risk and thus also safety requirements across Europe. Both Codes of Practice and similar Reference Systems as RAP can be considered at the same time also as RAC.

In case of GNSS/EGNOS application for railway signalling including ERTMS, Codes of Practice (mainly ERTMS/ETCS subsets and CENELEC standards) have been utilized for derivation of safety requirements for Virtual Balise detection.

3 CROSS-ACCEPTANCE IN RAILWAY SAFETY CONCEPT

The aim of European railway authorities and European railway industry is to develop compatible railway systems based on common standards. Therefore cross-acceptance of Safety Approvals for sub-systems and equipment by the different National Railway Safety Authorities (NSA) represents basic approach in the system development and approval process. The issue of cross-acceptance also becomes critical in the area of exploitation of the aviation EGNOS SoL service within ERTMS.

3.1 Safety cases according to EN 50129

The cross-acceptance in the field of railway safety-related systems can be achieved and demonstrated via a so-called Generic Product and Generic Application. For a generic product, i.e. independent of application, and for a generic application, i.e. class of applications, it should be possible for safety approval granted by one safety authority to be accepted by other safety authorities (i.e. cross-acceptance or mutual recognition).

The CENELEC EN 50129 standard identifies three different kinds of safety cases:

- Generic Product Safety Case (GPSC) – independent of railway safety application;
- Generic Application Safety Case (GASC) – for a class of (ERTMS) applications;
- Specific Application Safety Case (SASC) – for a specific application.

The cross-acceptance can be achieved by means of the GPSC and GASC. The SASC is required for a specific application and will depend on mutually recognized GPSA and GASC. The Safety Case for a system may depend on the Safety Cases of other sub-systems or components. In such circumstances, safety acceptance of the main system is not possible without previous safety acceptance of the related sub-systems/components. If an Independent Safety Assessment/Assessor (ISA) report has been obtained for a generic product, or for a generic application, a reference may be made to this for safety acceptance of a specific application; it is not necessary to repeat the generic ISA process for each specific application. It is mandatory according to CENELEC that verification and validation (VaV) activities and development of the safety case for a product or application shall start at the early phases of the system life cycle (EN 50126 [2]). It is also required for GPSC and GASC.

Note: If a CSM-RA Assessment Body (AsBo) fulfils also the competence requirements of a CENELEC ISA, then the independent safety assessment carried out by such an AsBo can include also all necessary independent safety assessment activities that should be fulfilled by the CENELEC ISA. The objective is to avoid unnecessary duplication of independent safety assessments by different conformity assessment bodies and unnecessary duplication of inherent costs.

3.2 Role of generic safety case in certification and proposed solution

The interoperability means correct interaction between different interoperable constituents as defined in point (7) of Article 2 of Directive (EU) 2016/797 [7]. In order to guarantee the interoperable, safe and dependable operations, it is necessary to provide certification of individual constituents. A safety case is an important part of the certification process because it simplifies the process by providing a modular approach. It is assumed that the railway cross-acceptance approach based on generic safety cases (GPSC and GASC) would be utilised for demonstration of the essential safety requirements related to a Virtual Balise Reader (VBR) based on EGNOS. It can significantly simplify the certification of Interoperability Constituents implementing the VBR function.

As it is explained above, it is not considered that GPSC would be developed for EGNOS according to CENELEC and utilised for the cross-acceptance process since it is not practically possible. In addition, it seems it is not necessary to focus the attention on a generic safety case development, since as it is mentioned in Section 1 not always a safety case is required according to IEC 61508/EN50129:2018, especially for systems or services which already exist, such as EGNOS. Instead the EGNOS SoL service would be cross-accepted through mutual recognition of EGNOS SoL Service provider for railway usage based on the ICAO SARPs (International Civil Aviation Organization Standards and Recommended Practices) and GNSS MOPS (Minimum Operational Performance Standards) interpretation in terms of railway RAMS and elaboration of the Railway EGNOS SoL Service Definition Document (by EGNOS SoL service provider supported by rail industry). This document would also describe how EGNOS shall be used by designers and system integrators within the ERTMS VB concept in order to achieve safe integration of EGNOS with ERTMS. It represents a fundamental step in the EGNOS adoption for ERTMS. This would be then followed by the development of subsequent generic and also specific safety cases. The exact structure and contents of a safety case for railway safety-related systems is defined in EN 50129 [5]. The same structure is also required for generic safety cases.

The certified EGNOS SoL service for aviation already exists (since 2011) and it is compliant with ICAO SARPs. The EGNOS safety case has been already developed according to aviation safety standards and not according to CENELEC. Therefore, the major problem related to the EGNOS SoL service cross-acceptance for ERTMS is that EGNOS cannot be considered as a Generic Product from the CENELEC standards point of view. EGNOS as it is without additional supporting safety evidence and guarantees must not be used for safety applications in the rail sector. It is because the essential condition regarding VaV, safety case development and other activities to be performed during CENELEC safety life cycle was not fulfilled.

Aviation and railway safety regulations (i.e. ICAO SARPs, GNSS MOPS, CENELEC, CCS TSIs, etc.) are different and therefore it would be unrealistic to develop the EGNOS safety case according to CENELEC and use it as a basis for certification of EGNOS based ERTMS solutions. Therefore, another approach for the EGNOS SoL Service cross-acceptance should be utilised. It seems that the EGNOS SoL service could be adopted and certified by means a so-called “pre-existing” item that was originally defined in the standard IEC 61508 (2nd ed., 2010) [12].

This is the fundamental idea in this article that could open the door to the EGNOS cross-acceptance for ERTMS. The idea is further developed in Sections below.

4 EGNOS CROSS-ACCEPTANCE FOR ERTMS VIA PRE-EXISTING ITEM

This section deals with a possible EGNOS SoL service cross-acceptance for ERTMS through its certification as a pre-existing item, which is specified in detail in IEC 61508 [12] and CENELEC EN 50129 [5] standards.

Firstly, a common practice regarding certification of supporting services which are considered as critical elements of safety-related systems is described. Then the concept of a supporting service as a pre-existing item which was originally introduced in the standard IEC 61508 and subsequently adopted by the railway specific standard EN 50129:2018 is outlined. Finally, the possibility of EGNOS SoL service cross-acceptance for ERTMS via the IEC 61508/EN 50129 pre-existing item is discussed.

The analysis performed below is fully in line with the Return Experience (REX) [13] of the European Union Agency for Railways (ERA) with the use of CSM-RA (402/2013 and 2015/1136). The REX says that apart from widely used CENELEC EN 5012x standards within the CSM risk management process, the risk acceptance is also managed according to the standard IEC 61508 and Tolerable Hazard Rates (THRs), especially regarding generic components design for the Control Command Signalling (CCS) sub-system.

4.1 Certification of generic supporting services and utilities in industry

Generally, in the control systems market, manufactures’ products are often certified for functional safety applications against IEC 61508. This is mostly done by a Certification Body (CB) which is accredited to do this work by an Accreditation Body (AB). Important element of the certification process is a safety case, which provides a systematic and complete way to show compliance to one or more functional safety standards. The IEC 61508 safety case demonstrates the fulfilment of the functional management requirements of the IEC 61508-1 to 3. This also applies to supporting services/utilities such as electricity, gas, pressure steam, etc. It is usually required to develop a safety case for such supporting services in the process industry to show that the supporting services that are needed to implement any measure defined in the safety case shall have suitable reliability and availability. To meet this criterion, the safety case relating to the safety services shall according to the Safety Case Assessment Guide [14] show:

- that the role and significance of the supporting services has been considered in design, construction, operation and maintenance to ensure that these supporting services and facilities will be available in the required quality when it is needed;
- the effect of the loss of key supporting services has been considered as part of a hazard identification and risk analysis process. This shall ensure that safety systems fail to a safe state and that the consequence of supporting service failure does not act as a major accident initiator;
- the reliability of services for safe shutdown and emergency response have been specified and independent back-up supplies provided where necessary, and
- those supporting services that are essential for operation of key safety systems and its back-up system.

However, it is not always possible to develop a safety case for a system or item according to required standards, e.g. IEC 61508 [12], CENELEC EN 50129 [5], etc. This also applies to the EGNOS system whose safety case was developed according to aviation standards because it was primarily designed for safety operations in aviation.

In order to utilise EGNOS SoL service for the ERTMS virtual balise concept, it should be adopted and certified according to railway specific standards and regulations. In sections below there are discussed possibilities to adopt and certify EGNOS for ERTMS as a supporting service via an IEC 61508/EN 50129 pre-existing item.

4.2 IEC 61508: Supporting service within safety-related system

The standard IEC 61508 [12] applies to safety-related systems that incorporate Electrical and/or Electronic and/or Programmable Electronic (E/E/PE) devices. It specifically covers hazards that occur when safety functions fail. The main goal of the safety standard is to reduce the risk of failure to a tolerable level. IEC 61508 is built on two fundamental pillars:

- the Safety Life Cycle intended to reduce or eliminate failures due to systematic causes; and
- the Safety Integrity Levels (SILs) to address dangerous random HW failures.

The safety life cycle is defined as a process that includes all necessary steps to achieve the required functional safety. It is also called Functional Safety Management. A Safety Integrity Level is one of four levels (i.e. SIL 1, 2, 3 and 4), each corresponding to a range of target average dangerous failure frequencies of a safety function. SIL is a measure of performance of a safety function, which is designed as a safety guard (safety provision) against the specific hazard. SIL 4 is used to protect users against the highest risks. SIL, according to IEC 61508 [12], is determined by the average frequency of dangerous failure per 1 hour (PFH) for systems working in continuous or high demand mode of operation – i.e. also computer-based railway signalling systems. Note that a SIL is a property of a safety function rather than of a system or its part.

IEC 61508 defines that a safety-related system is a designated system that both:

- implements the required safety functions necessary to achieve or maintain a safe state for the Equipment Under Control, and

- is intended to achieve, on its own or with other safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions.

Note 6 of IEC 61508-4 [12] says that a safety-related system includes all the hardware (HW), software (SW) and supporting services (e.g. power supplies) necessary to carry out the specified safety function (sensors, other input devices, final elements, etc. are therefore included in the safety-related system). Therefore, IEC 61508 supporting services and related IEC 61508/EN 50129 pre-existing items could also represent a way to the EGNOS SoL service acceptance for the ERTMS Virtual Balise concept.

4.3 Pre-existing item according to IEC 61508 and EN 50129

The second edition of IEC 61508, [12] introduced a notion "pre-existing item" (for both HW or SW elements), which means an item or element that already exists (e.g. EGNOS) and that was not developed specifically for the current project (e.g. ERTMS). It is required by IEC 61508 that the compliant pre-existing item, which does not have a safety-case, should have an IEC 61508 certificate together with a certificate report and a safety manual. The safety manual should be developed by the system manufacture or service provider. The concept of pre-existing item was adopted later by CENELEC in EN 50129:2018 [5].

EN 50129 admits that safety of the system under consideration (e.g. ERTMS based on EGNOS) can rely on the specific properties of elements that have their own life cycle independent of the system safety life cycle. In this sense the EN 50129 pre-existing item is considered as an item which has been already developed (e.g. EGNOS) and cannot be changed for the system under consideration (e.g. ERTMS). EN 50129 further assumes that pre-existing items

- are complex (in their sense that a complete and deterministic functional model of the item is not possible or not completely available), and
- have not been developed in accordance with this document (EN 50129) or its previous versions.

It is further stated in EN 50129:2018 how pre-existing items shall be used within the railway safety-related systems, what are requirements for use of complete pre-existing systems (Section 6.2.2 of EN 50129:2018) and requirements for use of pre-existing elements, that performs only part of a safety-related function (Section 6.2.3 EN 50129:2018).

4.4 Role of IEC 61508 safety manual in safety acceptance process

The IEC 61508 [12] safety manual, which is not explicitly mentioned in the EN 50129 [5] standard, represents an important source of information regarding the pre-existing items for designers and system integrators. The manual includes all information about the compliant item, which is required for correct integration of the compliant item in the safety-related system or subsystem in order to meet the system or subsystems requirements without compromising safety. Development of the safety manual for the pre-existing item and its certification represents the required evidence which shall be contained in the overall Safety Case.

4.5 Contents of IEC 61508 safety manual

The content of the safety manual for the pre-existing is specified in detail in IEC 61508 [12]. For every compliant item, the safety manual shall contain (IEC 61508-2, Annex D, 2010):

- a description of the functions capable of being performed;
- identification of the hardware and/or software configuration of the compliant item to enable configuration management of the E/E/PE safety-related system;
- limitations regarding the use of the compliant item and/or assumptions on which analysis of the behaviour or failure rates of the item are based.

For every function, the safety manual shall contain according to [12] information on:

- the failure modes of the compliant item (in terms of the behaviour of its outputs) that:
  - o are not detected by diagnostics internal to the compliant item;
  - o are detected by diagnostics internal to the compliant item;
  - o result in a failure of the diagnostics to detect failures of the function;
- estimated failure rates for the identified random/hardware failure modes including failure modes of the diagnostics internal to the compliant item;
- specification of the diagnostic test interval for every failure mode in that is detected by diagnostics internal to the compliant item requirements on any periodic proof test and/or maintenance;
- specification of outputs of the compliant item initiated by the internal diagnostics;
- requirements for any periodic proof test and/or maintenance;
- detailed information on the external diagnosis capable to detect identified failure modes of the compliant item;
- the hardware fault tolerance, etc.

For every function in terms of protection against systematic failure, the manual shall contain:

- the systematic capability of the compliant item that provides the function;
- any requirements or constraints relating to the application of the compliant item, relevant to the function, that should be observed in order to prevent systematic failures of the compliant item.

For additional requirements relating to software compliant items see 7.4.2.12 and Annex D of IEC 61508-3 [12].

4.6 Contents of safety evidence for pre-existing elements according to EN 50129

The standard EN 50129 [5] does not explicitly require that a “Safety Manual” for supporting elements having potential impact on functional safety shall be developed. Nevertheless, a very similar/same safety evidence of their contribution shall be documented in the overall Safety Case. EN 50129 states that pre-existing equipment performing only part of a safety-related function (like EGNOS), shall be correctly integrated in the technical and procedural safety management. The supporting safety evidence, which should be referred in the overall Safety Case, shall according to EN 50129 (Section 6.2.3) mainly include:

- a minimum set of information shall be available: described functionality; interfaces; hardware and/or software constraints; failure rate of the equipment; environmental conditions and other conditions of use;
- the pre-existing item shall be identified, included in the overall system definition and put under configuration control;

- the hazardous functional failure modes shall be identified. These failure modes should be identified by an interface hazard analysis. Note: This is particularly important for a complex system such as EGNOS;
- for each hazardous functional failure mode identified at the interface of the equipment, that would require a safety-related function with a safety integrity level from 1 to 4, the failure mode shall be externally (independently) negated and a safe state shall be enforced within the required time to fulfil the required safety target at the system level;
- failure modes observed at the boundary of the equipment are not always traceable to their actual causes. Therefore, for any equipment performing a SIL function, when it is not possible to identify the components of the equipment having a failure mode contributing to the hazard, the full failure rate of the equipment (e.g. EGNOS service) is used. This failure rate shall be demonstrated to be compatible with the TFFR (Tolerable Functional Failure Rate) required for the complete function;
- at the system level, when the pre-existing equipment is integrated in the system under consideration, all design, safety verification, safety validation and assessment activities shall be performed encompassing the pre-existing equipment as a black-box;
- for all SILs, a strategy shall be defined to manage the possible effects of product changes (e.g. disable automatic software updates).

EN 50129 does not explicitly give a specific name to the safety evidence file for the pre-existing item, for which it is impracticable to develop a safety case according to CENELEC. Nevertheless, it is obvious that the requirements regarding the contents of the IEC 61508 Safety Manual and the EN 50129 supporting safety evidence for the pre-existing item are practically the same. So why not name the supporting safety evidence required by EN 50129 as the Safety Manual. This Safety Manual as a safety evidence related to the pre-existing item shall be referred in the overall Safety Case (EN 50129).

4.7 Cross-acceptance of EGNOS for ERTMS

If the existing aviation EGNOS SoL service would be considered as a supporting service/utility and pre-existing item according to IEC 61508/EN 50129 for ERTMS Virtual Balise detection (generic application), then development of an additional EGNOS safety evidence would not be required. In this specific case only a supporting evidence (EN 50129)/Safety Manual (IEC 61508) describing all EGNOS SoL service features and characteristics, which are important for safe integration of the item into the ERTMS would be elaborated. Such guidance for designers and systems integrators is exactly what manufactures need.

It is assumed that the EGNOS Service Provider (currently it is ESSP) would develop in collaboration with the European Space Agency (ESA), European GNSS Agency (GSA), ERA and industry EGNOS SoL Service Definition Document (SDD) for Rail in compliance with the interpreted ICAO SARPs for Rail. The safety evidence/manual (EN 50129/IEC 61508) for EGNOS considered as the pre-existing item would be then important part of the EGNOS SDD for Rail. The EGNOS Safety Manual would be elaborated using EGNOS Usage Railway Requirements Document. The existing EGNOS safety case developed for safety operations in aviation would be used in this cross-acceptance process as well. Important fact is that all requirements for Safety Manual, that also represent a guidance for the safety evidence elaboration, are known. These are specified in detail in EN 50129:2018, Section 6 and Annexes D of IEC 61508-2 and IEC 61508-3, and should be also used as a guidance for development of the EGNOS Safety Manual to be fully in line with CENELEC.

CSM-RA must be used for the EGNOS cross-acceptance process in any case since it represents a significant change in ERTMS. The applicability of CENELEC is within CSM-RA is optional. Nevertheless, the use of CENELEC standards within CSM Risk Assessment Process is generally highly recommended, as it also results from the ERA REX study [13]. The EGNOS Safety Manual including assessment report (i.e. supporting safety evidence in terms of EN 50129) for EGNOS as the pre-existing item shall be then referred in the overall Safety Case, Section named "Related Safety Cases", as it is outlined in Fig. 1.

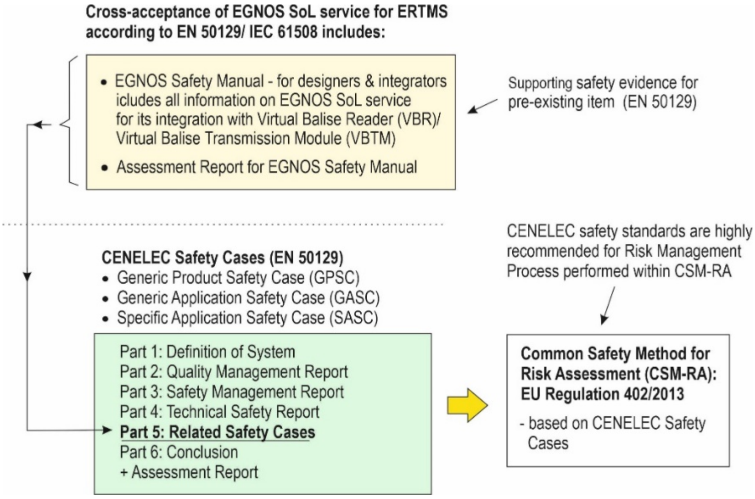
Cross-acceptance of EGNOS SoL service for ERTMS according to EN 50129/ IEC 61508 includes:
• EGNOS Safety Manual - for designers & integrators icludes all information on EGNOS SoL service for its integration with Virtual Balise Reader (VBR)/ Virtual Balise Transmission Module (VBTM)
• Assessment Report for EGNOS Safety Manual
Supporting safety evidence for pre-existing item (EN 50129)
CENELEC safety standards are highly recommended for Risk Management Process performed within CSM-RA
CENELEC Safety Cases (EN 50129)
• Generic Product Safety Case (GPSC)
• Generic Application Safety Case (GASC)
• Specific Application Safety Case (SASC)
Part 1: Definition of System
Part 2: Quality Management Report
Part 3: Safety Management Report
Part 4: Technical Safety Report
Part 5: Related Safety Cases
Part 6: Conclusion
+ Assessment Report
Common Safety Method for Risk Assessment (CSM-RA): EU Regulation 402/2013
- based on CENELEC Safety Cases

Figure 1: Cross-acceptance of EGNOS for ERTMS via CENELEC pre-existing item.

5 CONCLUSIONS

This article presents the original idea of the EGNOS Safety-of-Life (SoL) service adoption and certification for the ERTMS/ETCS Virtual Balise concept. The idea consists in fact that the EGNOS SoL service would be adopted and certified via a so-called "pre-existing" item in terms of the standards EN 50129/IEC 61508. Important is that EGNOS can be fully cross-accepted according to CENELEC railway safety standards and so this significant (safety) change in ERTMS can be fully controlled using CSM Risk Management Process in compliance with the CENELEC life cycle. It means that there is no need to develop a new EGNOS safety case specifically for rail safety applications according to CENELEC, which would not even be possible.

The idea of EGNOS certification for rail signalling by way of a pre-existing item is very fresh. This article was written with the intention to 1) show that a possibility of EGNOS SoL service certification according to CENELEC exists, and 2) initiate a discussion on the proposal within the GNSS and railway community. The European railway and GNSS researchers have been looking for a suitable solution to adopt EGNOS for railway safety systems for more than one decade. The imaginary closed loop consisting of the EGNOS safety case developed according to aviation safety standards on one hand and strict CENELEC standards for rail on the other hand did not offer any solution for EGNOS-based signalling. Therefore, it was necessary to untie the loop. In this paper it has been demonstrated that the suggested idea to certify the EGNOS SoL service by way of the pre-existing item offers a suitable solution. It is believed this proposal opens the door to the EGNOS certification for ERTMS/ETCS in Europe. In addition, the idea can be also utilised for GNSS SoL services adoption and certification in other land GNSS-based safety applications, such as self-driving cars, machine control, mobile robots, etc.

ACKNOWLEDGEMENTS

The work was supported: 1) from the ERDF/ESF grant “Cooperation in Applied Research between the University of Pardubice and companies, in the Field of Positioning, Detection and Simulation Technology for Transport Systems – PosiTrans (2018–2022),” No. CZ. 02.1.01/0.0/0.0/17_049/0008394, 2) by the ESA STEMS project (2019–2020), and 3) from the European research programme H2020 within the HELMET project (2020–2021).

REFERENCES

[1] H2020 ERSAT GGC project, 2019. www.ersat-ggc.eu/.

[2] EN50126-1, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process. *European Standard*, CENELEC, 2017.

[3] EN50126-2, Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety. *European Standard*, CENELEC, 2017.

[4] EN50128, Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems. *European Standard*, CENELEC, 2011.

[5] EN 50129, Railway Applications – Safety related electronic systems for signalling. *European Standard*, CENELEC, 2018.

[6] EN 50159, Railway applications – Communication, signalling and processing systems – Safety-related communication in transmission systems. *European Standard*, CENELEC, 2010.

[7] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union, 2016.

[8] Regulation (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the “control-command and signalling” subsystems of the rail system in the European Union, 2016.

[9] Regulation (EU) 2019/776 of 16 May 2019 amending Commission Regulations (EU) No 321/2013, (EU) No 1299/2014, (EU) No 1301/2014, (EU) No 1302/2014, (EU) No 1303/2014 and (EU) 2016/919, 2019.

[10] Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009, 2013.

[11] Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment, 2015.

[12] IEC 61508 (1-7), Functional safety of electrical/electronic/programmable electronic safety-related systems, *European Standard*, 2010.

[13] Jovicic, D., Report on the return experience (REX) with the use of the CSM for risk assessment (Regulations 402/2013 and 2015/1136). *ERA Report, Ref.: 004MRA1100*, 18/12/2018, page 46.

[14] Safety Case Assessment Guide, jointly developed by Ministry of Manpower, National Environment Agency, SCDF and SCIC (Singapore Chemical Industry Council), pp. 40–41, 2017.