A FRAMEWORK FOR CERTIFICATION OF TRAIN LOCATION DETERMINATION SYSTEM BASED ON GNSS FOR ERTMS/ETCS

ALEŠ FILIP[1], SALVATORE SABINA[2] & FRANCESCO RISPOLI[2]
[1]University of Pardubice, Pardubice, Czech Republic
[2]Ansaldo STS (A Hitachi Group Company), Genoa, Italy

ABSTRACT

The Virtual Balise concept has been demonstrated and shared among the ERTMS community as a mean to replace the physical balises by implementing a train Location Determination System (LDS) based on GNSS. It is evidenced both by the results of recent and current EC-supported R&D projects (e.g. 3InSat, ERSAT EAV, STARS, RHINOS, NGTC), the Sardinia Trial Site (Cagliari – San Gavino double track lines) equipped with a ERTMS Level 2 based system with Virtual Balises and the Ansaldo STS Freight SIL 4 ERTMS Level 2 system based on GPS L1 positioning system in commercial service in Australia.

In order to introduce the safe high-integrity LDS system into ERTMS/ ETCS and use it in railway operations in EU member states (MSs), it is necessary to develop and to authorize it according to relevant European and national regulations. It means that this LDS and its integration into ERTMS must pass through a certification and authorization process compliant with the applicable CENELEC standards and EU regulations.

This article deals with a possible certification process of a train LDS as a new subsystem of the ERTMS/ETCS interoperability constituents. Special attention is paid to a possible certification strategy in case of external GNSS safety-of-life service employment via an augmentation network. A possible certification framework for the whole LDS comprising on-board and trackside subsystems is outlined as well. Since the introduction of GNSS into ERTMS/ETCS represents a significant change within EU railway network, then the required common safety method must be applied. In this framework, a new pilot line has been launched by RFI with Ansaldo STS aiming to contribute to the identification of a possible certification process for deploying an ERTMS Level 2, baseline 3 with GNSS localization and public telecom solutions by 2020.

Keywords: certification, EGNOS, Galileo, GNSS, GPS, railway signalling, safety, safety case.

1 MOTIVATION

In order to introduce a safe high integrity train Location Determination System (LDS) based on GNSS into ERTMS/ ETCS and use it in railway operations in EU MSs, it is necessary to develop and to authorize it according to relevant European and national regulations. It means that this LDS as a new subsystem to be integrated in the ERTMS/ETCS interoperability constituents (ICs) and its integration into ERTMS Specification must pass through all the CENELEC development phases and also a certification process [1–12]. It is evident that a return of experience from aviation sector's certification process is important whenever GNSS augmentation networks are used so that the rail sector can assess and eventually cross-accept procedures already adopted. A certification framework for the whole LDS has to comprise of both on-board subsystem including GNSS receiver and trackside subsystems including GNSS service. Since the introduction of GNSS into ERTMS represents a significant change within EU railway network, then the common safety method (CSM) must be applied [1, 12, 13].

ISSN: 2058-8305 (paper format), ISSN: 2058-8313 (online), http://www.witpress.com/journals
DOI: 10.2495/TDI-V2-N3-284-297

2 SAFETY REGULATORY FRAMEWORK

2.1 Common safety method

Although innovation is encouraged, especially when it will enable the utilization of the ERTMS, a risk analysis is mandatory to evaluate eventual additional risks brought by the new technologies and the proper mitigation solutions. In fact, each intended change in railway signalling represents a risk, which could endanger safety. In order to control the risk on an acceptable level, new instruments called common safety targets (CSTs) and CSMs have been introduced in the Railway Safety Directive (EU) 2004/49/EC [14] and also in the revised Directive 2016/798 [1]. In 2009, a new regulation regarding safety management has been implemented by the European Commission (EC) and ERA (formerly European Railway Agency, now European Union *Agency* for *Railways*) to harmonize risk assessment process for the European railway industry [15]. This new approach is called common safety method for risk evaluation and assessment (CSM-RA). The CSM-RA approach is described in the revised Commission Regulation (EU) 402/2013 [13].

This Regulation shall facilitate the access to the market for rail transport services through harmonization of [13]:

- The risk management processes used to assess the impact of changes on safety levels and compliance with safety requirements;
- The exchange of safety-relevant information between different actors within the rail sector in order to manage safety across the different interfaces which may exist within this sector;
- The evidence resulting from the application of a risk management process.

The CSM on risk assessment shall be applied by the person in charge of implementing the change under assessment. This person, referred to as the 'proposer', can be one of the following actors [1, 7]:

- The railway undertakings (RUs) and infrastructure managers (IMs) which implement risk control measures in accordance with Article 4 of the safety directive 2004/49/EC [14] and its revision 2016/798 [1];
- An entity in charge of maintenance (of vehicles) which implements measures in accordance with the directive 2016/798 [1];
- The contracting entities and the manufacturers, when they invite a conformity assessment body to apply the 'EC' verification procedure in accordance with Article 15(1) of the interoperability directive 2016/797 [2];
- The applicant of an authorization for placing in service of vehicles.

If the proposer is an IM or a RU, sometimes it may be necessary to involve other actors in the process. In some cases, the IM or the RU might sub-contract, partly or completely, the risk assessment activities. The CSM on risk assessment shall apply to any change of the railway system (technical, operational or organizational nature) which is considered to be significant. It is the introduction of GNSS into ETCS. If the change in signalling system is significant, than the proposer has to evaluate the associated risk according to the six criteria [13]:

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

The analysis should consider worst cases, not just the likely or expected case. When the change is significant, a CSM Assessment Body (CSM AB) must be appointed by the proposer. Independent assessment in Regulation 402/2013 [13] is different from notified body (NoBo) work, because NoBo checks formal conformity of a structural subsystem vs. all requirements defined in relevant TSIs, whereas CSM AB makes judgements.

It is evident from Fig. 1 that, in addition to the basic CSM-RA, the significance of the change should also be assessed taking into account all safety-related changes affecting the same part of the product/subsystem/system under assessment. The purpose is to assess whether or not the totality of such changes amounts to a significant change requiring the full application of the CSM for risk evaluation and assessment. Furthermore, RUs, IMs and the proposer must include audits in their recurrent auditing scheme for the safety management system (SMS).

2.2 Safety management system

RU and IM have a duty to establish a SMS – Directives 2004/49/EC [14] and 2016/798 [1]. It shall demonstrate that all mandatory functions required for interoperability have been

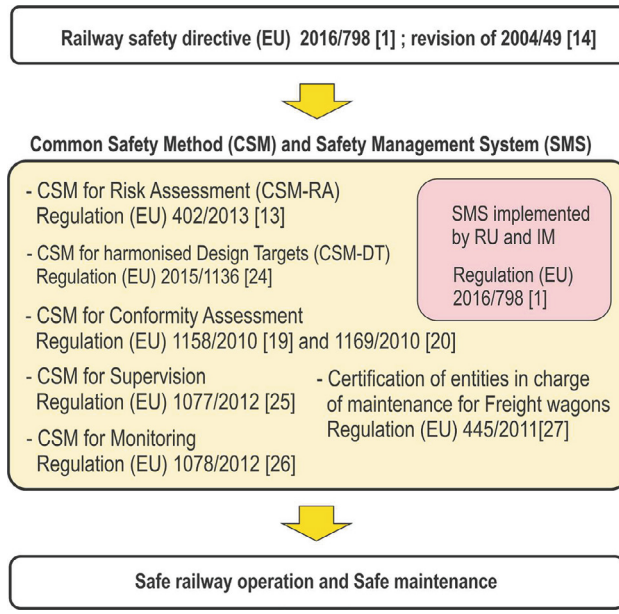

Figure 1: EU regulations in safety regulatory framework.

implemented. The SMS shall ensure the control of all risks associated with activities of IM and RU, including maintenance.

The risk management process covered by the CSM can be represented within the EN 50 126 [16] V-Cycle (life cycle) that starts with the preliminary system definition and finishes with the system acceptance. However, CSM does not cover performance monitoring and operation and maintenance. These two phases are covered by the RU and IM SMS – see Fig. 1.

3 CERTIFICATION PROCESS WITHIN ERTMS: PURPOSE AND STEPS

Certification ensures that the required interoperability among on-board and trackside subsystems is shared among many independent actors, mainly IMs and RUs. The corresponding certificate comprises either the assessment of the conformity of an IC, considered in isolation, to the technical specifications to be met, or the assessment of the suitability for use of an IC, considered within its railway environment, in relation to the technical specifications.

Directive 2016/797 [2] extends authorization process of Control Command System to entire railway system as defined in the Directive – it supports the concept of 'Cross-Acceptance' (mutual recognition) in different MSs as a stepping stone to the interoperability within the Trans-European Network. Certification process for railway safety-related systems includes three steps:

- Review reports on all evidence elaborated by system manufacturer for communication between the manufacturer/applicant and the NoBo;
- Technical report detailing requirements to be met by the system, and how and why they are fulfilled and
- Issue of the certificate as top-level summary for potential customers. It is often a single page stating that the system requirements/standards have been met.

IMs have a key responsibility for the safe design, maintenance and operation of their rail network. IMs are subject to a safety authorization by the National Safety Authority (NSA) concerning their SMS and to other provisions so as to meet safety requirements. In order to be allowed to manage and operate a rail infrastructure, the IM shall obtain a safety authorization from the NSA in the MS where the rail infrastructure is located.

An applicant (e.g. a natural or legal person requesting an authorization, be it a RU, an IM or any other person or legal entity, such as a manufacturer) can place a vehicle on the market only after having received the vehicle authorization for placing on the market issued by the Agency or by the NSA. In its application for a vehicle authorization, the applicant must specify the area of use of the vehicle and include evidence that the technical compatibility between the vehicle and the network of the area of use has been checked.

The safety authorization and the vehicle authorization must thus also be obtained for ERTMS systems based on the GNSS positioning. Therefore, the certification and authorization for placing in service new IC, e.g. GNSS based, is expected to include three main activities (see Fig. 2):

- EC declaration of Conformity (issued by Applicant) with respect to specifications (e.g. new interoperable specification that will also include such a new technology) – i.e. certification of IC's conformity assessed by NoBo;
- EC declaration of verification of a subsystem (performed by Applicant) – i.e. certificate of verification assessed by NoBo;
- Authorization for the placing in a service of a new system/subsystem by MS/railway NSA.

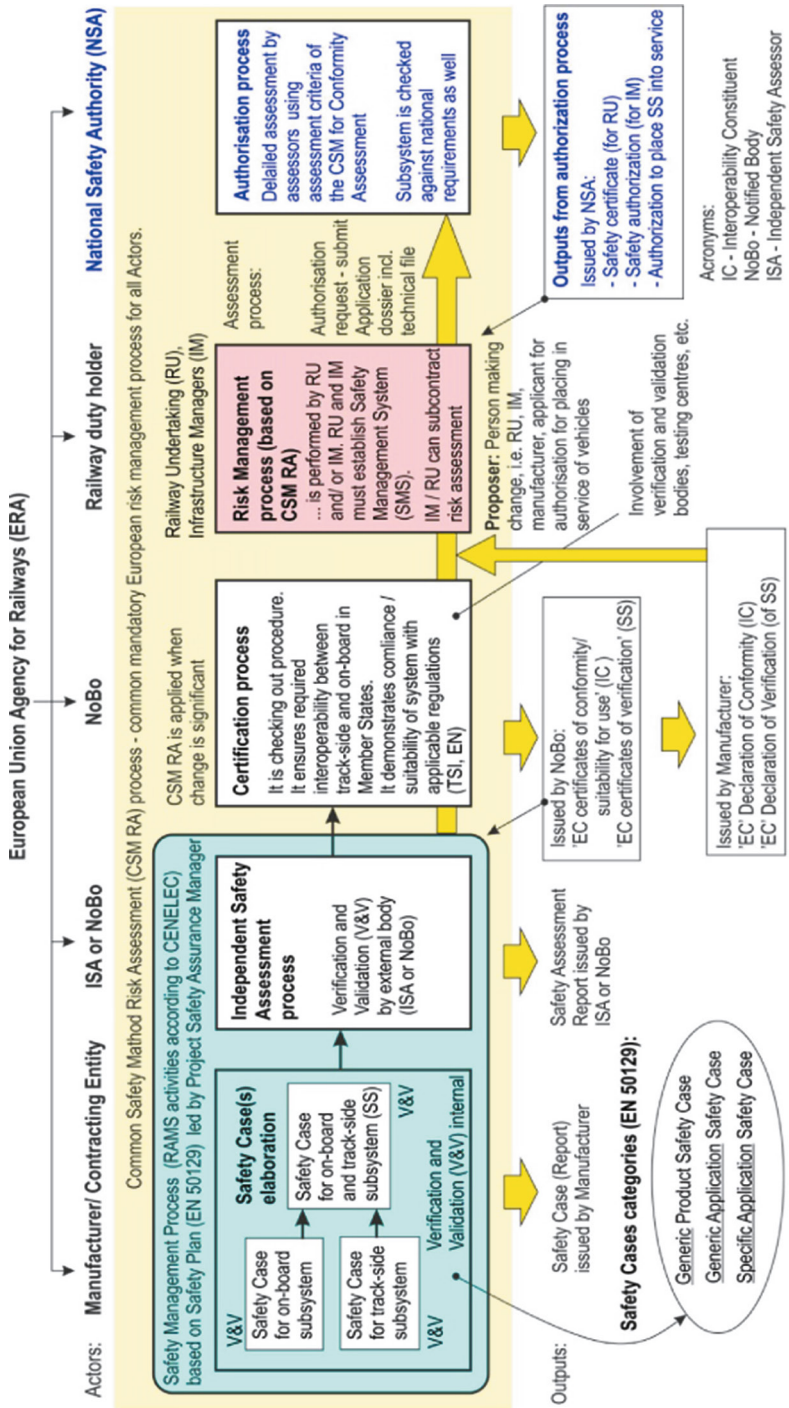

Figure 2: Elements of authorization process for train LDS based on GNSS.

4 ELEMENTS OF CERTIFICATION AND SAFETY APPROVAL PROCESS

4.1 Verification and validation

During the development of safety-related systems, it is important to document that the system meets requirements and that it works correctly. It can be proven by means of the verification and validation (V&V) process, which must start early in the development life cycle – see Fig. 2. The verification is the process evaluating element or system during a given development phase and saying whether it meets the specified requirements for that phase. In other words, if the element or system was built correctly in accordance with the applicable specification for that phase. On the other hand, the validation checks for errors in the specification and demonstrates that the system works as it required. The V&V activities are to be carried out by verifiers and validators in accordance with the recommendations given by CENELEC EN 50128 [17] and EN 50129 [18] to guarantee the required independence (see Fig. 6 of [18]). The role of external specialists, e.g. independent safety assessors (ISAs) or NoBos, is also included – see Fig. 2.

4.2 Safety case

The application of V&V process alone does not still provide sufficient evidence that the safety requirements for the system have been met. More comprehensive safety evidence in the document named Safety Case must be provided. A Safety Case can be a Generic Product Safety Case, a Generic Application Safety Case or a Specific Application Safety Case as defined in EN 50129 and EN 50126. The type(s) of Safety Case(s) elaborated shall be suitable to meet the scope of the product, system or process. Moreover, when the integration of subsystems is required (in particular, when these subsystems are provided by different suppliers), the Safety Case of the Integration is also required.

The safety case is based on (1) safety requirements, (2) safety argument and (3) safety evidence. A safety case shall include a structured argument supported by analytical and experimental evidence including simulations that provide a comprehensive and valid case that a generic product/system is safe for the intended application in the given environment.

The safety case has to be elaborated by the manufacturer of the generic product/subsystem/system and assessed by the ISA – ISA or NoBo. It is elaborated early in the development life cycle. In the safety case, the safety assessor verifies that safety requirements have been met, all potential safety hazards have been identified and risks associated with them have been carefully evaluated. It is also verified that appropriate safety guards with a sufficient quality have been designed as protection against the hazards. In addition, the safety case must also demonstrate that the quality and safety management controls adopted within the life cycle are suitable for the required safety integrity level, and appropriate development techniques have been adopted and they have been performed correctly.

Safety case is the structured document and its content is specified in detail in EN 50126 [16] and the EN 50129 [18]. The ISA elaborates the safety assessment report. The safety assessment report is a key deliverable that summarizes the safety case at a particular instant of time. It is one of two major outputs (excepting V&V) forming the certification process. In contrast to the safety case, the structure and contents of the safety assessment report is not defined in standards – its content is defined in Article 15 and Annex III of [13] so as to valid across different MSs of the Union.

4.3 Role of safety case in certification process

In some cases, even the safety case for the individual system/subsystem and its approval by the independent assessor is not able to justify the required operational behaviour and the safety at a system level. For example, it is when the system requires both on-board unit and infrastructure parts for its proper functioning. Such examples can be found in aviation or on railway. Currently, the management of the railway system is shared between independent actors, namely IMs and RUs. Each of them is responsible for their part of the railway system. The situation can be further complicated if the system is also required to operate in several countries – i.e. to enable a so-called cross-border operations. It is just the case of ERTMS/ETCS or the possible future ERTMS/ETCS based on GNSS positioning technology, which shall provide the required safe and dependable operations of trains throughout Europe or in other regions. ETCS on-board units from different manufactures must be able to properly function on trackside infrastructures also from different suppliers. In other words, the required interoperability within such large-scale system must always be assured [2]. The interoperability means in fact the correct interaction between different interoperable constituents as defined in point (7) of Article 2 of Directive (EU) 2016/797. In order to guarantee the interoperable, safe and dependable operations, it is necessary to provide certification of individual constituents, which is required by law [2, 5]. The safety case is important part of the certification process – see Fig. 2.

It is obvious that certification cannot prove correctness of the system. If a system receives certification, it simply means that it has met all the requirements needed to be met for certification. It does not mean that the product is error free. The safety assessment does neither replace own competence or knowledge nor does it guarantee for 100% correctness of the project's work in all details. Therefore, the manufacturer is finally responsible for its legal or moral obligations.

4.4 Role of safety case in conformity assessment

Conformity assessment means the process demonstrating whether specified requirements relating to a product, process, service, subsystem, person or body have been fulfilled. With regard to the interoperability of the rail system within the European Union, NoBos must carry out conformity assessments in accordance with the conformity assessment procedures provided for in the relevant TSI. It is the demonstration that specified requirements relating to a system are fulfilled. The certificate is outcome for this process.

The purpose of the conformity assessment is to verify that mandatory/optional and any additional functions applicable to interoperability have been implemented. In case of verification, the task of the NoBo selected begins at the design stage and covers the entire manufacturing period through to the acceptance stage before the subsystem is placed in service. The certification is valid in all EU MSs, or only in a specific MS, depending on conditions. Generally, the concept of 'cross-acceptance' (mutual recognition) among MSs is a stepping stone to full interoperability, which is supported by the EC.

In order to be granted access to the railway infrastructure, a RU must hold a safety certificate. The safety certificate may cover the whole railway network of a MS or only a defined part thereof [19]. If a company is considered as an IM, it shall have a safety authorization to be authorized to carry out its maintenance activities on the infrastructure [20] – see Fig. 2.

Detailed safety case has been replaced with higher level safety certificates (for RUs) and authorization (for IMs). Applicants need to describe how their SMS [1] allows them to run their transport system safely, but they have to provide less detail than in a safety case on the individual processes they use. It means that a safety case is still a very important set of arguments documenting the achieved safety level.

4.5 Cross-acceptance among member states

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 subsystems and equipment by the different national railway authorities is necessary [18, 21, 22].

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). It is evident that the issue of cross-acceptance becomes also critical in the area of exploitation of the aviation EGNOS safety-of-life service (as CENELEC Generic Application) within ERTMS.

A product is not only described by a set of interfaces, but also by a set of assumptions and restrictions. Thus, as a general rule, the design of a railway system requires the verification of the compatibility of the interfaces and of the assumptions and restrictions. In addition, the quality and safety management controls adopted within the life cycle used for the aviation application domain must also be suitable for the railway application domain. Otherwise, ad hoc mitigations must be identified and set up. If the industrial standard used for safety assessment/certification is not that of the railway domain, e.g. RTCA DO-229 for SBAS [23], we also need to verify that the standards are compatible or that the way of EGNOS integration within ERTMS is compliant with CENELEC [16–18], etc.

4.6 Suitability of GNSS/SBAS for cross-acceptance by railway safety authorities

Nowadays, the GNSS positioning has been certified only for the aviation domain which differs from the railway's one in terms of safety targets, operational scenario, and climatic, EMC, mechanical and insulation requirements. For example, hazards tolerated by the ERTMS are set to 10E-9/hour per function versus the 10E-7 and 10E-9 per operation for, respectively, airport approach and landing. Moreover, the railways operative scenarios significantly differ from the aviation environment regarding GNSS local hazards caused by multipath, spoofing and electromagnetic interference (EMI).

For these reasons, the certification process for cross-acceptance of safety case should first start by assessing the suitability of SBAS (Satellite Based Augmentation System, e.g. EGNOS) networks to mitigate the system faults that have already evaluated by the aviation case (e.g. SV faults, ionosphere and troposphere effects and SV geometry orbit error); in addition, the assumptions used for the aviation application domain should be reviewed and their validity for the railway environment should be assessed. However, it is also necessary to mitigate the failures that arise in the immediate neighbourhood of the train (local errors). Multipath propagation is the most significant integrity challenge to the GNSS positioning for rail, and, in many R&D projects such as ESA 3InSat, H2020 ERSAT-EAV, and H2020 RHINOS, significant effort has been devoted to the hazards associated with local feared

events. In particular, the RHINOS strategy to cope with local feared events uses two levels of multipath detection. The first level is a set of multipath screens that isolate and discard most of the measurements that contain serious multipath defects. The second level is an end-around integrity check based on Advanced Receiver Autonomous Integrity Monitoring that catches the multipath defects not flagged by the first level.

The analysis of SBAS safety and performance in the rail application domain is extremely important for the rail application. Such an analysis should be done on the basis of (a) the real EGNOS SoL service in terms of railway RAMS, (b) recommended EGNOS utilization within ERTMS/ETCS solution with virtual balises and (c) the consolidated functional, safety and dependability requirements for virtual balise detection. This analysis should outline the limitations of existing SBAS, SBAS receivers, the mechanisms and the safety guards to cope with both systematic faults and random failures and assumptions done for avionics that imply railway applications conditions to be properly managed to meet all ERTMS/ETCS requirements for virtual balise detection. The Shift2Rail TD 2.4 Fail-Safe Train Positioning System initiative foresees the definition and the delivery of the Railway Minimum Performance Operational Standards required to guarantee the interoperable use of the GNSS positioning technology into ERTMS/ETCS solutions.

Further, the suitability analysis about the introduction of the GNSS positioning technology will also include the evaluation of the allocation of the responsibilities among railway and GNSS stakeholders when services of SBAS provider are used. The use of an external GNSS service for safe railway applications is a challenge aspect because railway IMs and undertakings usually currently manage all systems they use on their own.

4.7 A possible preliminary methodology for building a suitable safety case for SBAS use in ERTMS/ETCS solutions based on the virtual balise application

The ERTMS/ETCS functions and the related functional architecture also based on the GNSS positioning must be described in a standard new functional specification document set, named System Requirements Specification (SRS) to be agreed and accepted by the Railway Community. The implementation of this new solution must meet all the recommendations provided in the applicable CENELEC standards, such as EN 50129, EN 50128, EN 50126 and the related standards. Therefore, the use of the GNSS positioning technology must be assessed with respect to these standards and the related evidences must be described in the railway safety cases (Generic Product, Generic Application and Specific Applications), Independent Safety Assessment Report and the Safety Qualification Test Report.

All of these conditions shall be satisfied, at equipment, subsystem and system levels, before the safety-related system can be accepted as adequately safe. All documentary evidence that these conditions have been satisfied shall be included in a structured safety justification documents, known as Safety cases.

The methodology for building safety case for SBAS exploitation within the ERTMS/ETCS virtual balise concept will be elaborated with respect to the structure defined in the standard EN 50129 as follows: Definition of System (or subsystem/equipment), Quality Management Report, Safety Management Report, Technical Safety Report, Related Safety Cases and Conclusion.

The content of each of sections is described in EN 50129 [18]. It is obvious that in this development phase of GNSS-based LDS should be focused a special attention (but not only) on Part 4: Technical Safety Report. The Technical Safety Report is mandatory for SIL 1–4.

It shall explain the technical principles which assure the safety of design, including all supporting evidence (e.g. design principles and calculations, test specifications and results, and safety analyses). Large volumes of detailed evidence and supporting documentation need not be included, provided that precise references are given to such documents in the safety cases.

The proposed methodology for safety case related to the SBAS employment in ERTMS reflecting the necessary requirements for cross-acceptance (of safety case) should be elaborated according to EN50129 for the following three safety case categories:

- ***Generic Product Safety Case*** (*independent of railway safety application*) – covering SBAS on the basis of (a) the determination of real SBAS performance in terms of railway RAMS (EN 50126) – i.e. suitability analysis, (b) the identification all gaps in safety provisions due to SBAS imperfections, railway environmental effects (multipath, EMI), potential intentional attacks e.g. spoofing (security gaps) – from viewpoint of railway high-safety integrity requirements;
- ***Generic Application Safety Case*** (*for a class of ERTMS applications*) – related to efficient use of SBAS within ERTMS for virtual balise detection taking into account all existing ETCS and newly introduced safety barriers;
- ***Specific Application Safety Case*** (*for a specific application*).

The proposed methodology for the elaboration of three safety case categories will take into account the following aspects:

- Fundamental railway safety pillars, i.e. functional safety, technical safety and high dependability;
- 'Reasonable' worst-case approach. The EC Regulation 402/2013 [13] regarding mandatory use of CSM-RA requires to use among others the following criterion for risk assessment: 'Failure consequence: credible worst-case scenario' – see Section 2.1. The safety analysis must consider worst cases, not just the likely or expected case. The credible worst-case scenario in the event of failure of the system under assessment has also to take into account the existence of safety barriers outside the system. A 'reasonable' worst-case approach introducing a 'reasonable' measure of conservatism done on the basis of best estimates is critical for efficient use of EGNOS within ERTMS/ETCS;
- Integrity fault-tree allocations – specific to GNSS faults and anomalies that affect safety;
- Integrity/functional responsibility allocation between trackside and on-board;
- Defined subsystem elements responsible for mitigating events in fault trees;
- Functional processing requirements measurement and calculation procedures that must be standardized between trackside and on-board;
- Models for bounding nominal error parameters of probability distributions that bound trackside and on-board errors;
- Interface control document to describe the messages related to GNSS information (e.g. integrity) to be exchanged between trackside and on-board;
- Protection level equations assumed by trackside and calculated on-board;
- Railway RAIM (Receiver Autonomous Integrity Monitoring);
- Knowledge on difference between aviation-specific risk used in GNSS and railway safety integrity concept can be used for evaluation of impact of exposure time, safe down time (EN 50129) and other effects – see Fig. 3;
- Proper use of fail-safe techniques within the SBAS-based LDS architecture;

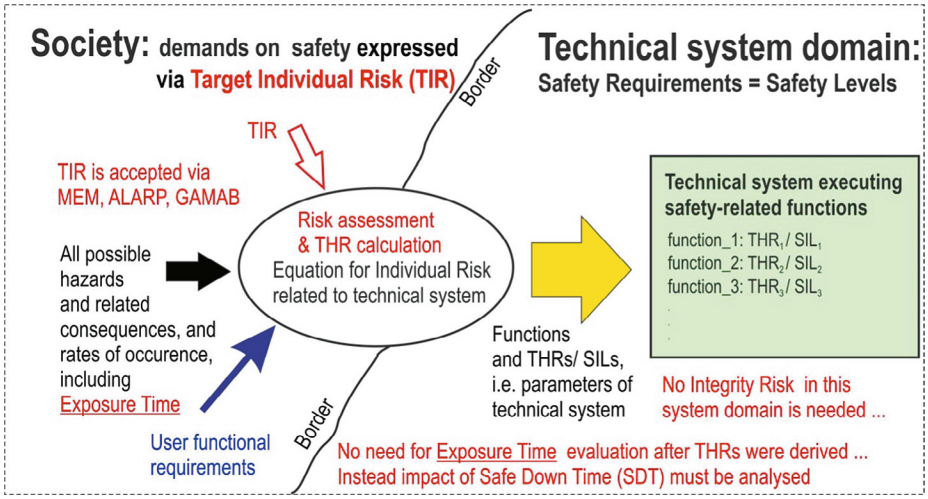

Figure 3: Transition from TIR to THR in railway safety integrity concept.

- Protection against external influences including environmental and other local effects;
- Systematic capability techniques necessary for realization of SIL 4 safety function;
- Real SBAS performance in terms of railway RAMS – not only safety integrity, but also reliability and availability.

The review of GNSS assumptions related to barriers and their applicability in the railway context should start from proper knowledge of aeronautical and railway operational concepts, related safety philosophies and terminology used. Therefore, this review would start with description of differences between aviation-specific risk approach used in GNSS integrity and railway safety integrity concept. It enables to find correct relations among aviation and railway safety and dependability attributes, identify their criticality and relevance and also confirm correctness of terminology used for requirements specification in compliance with CENELEC. For example, clarification of distinctions among quantities such as exposure time (aviation, rail), response time (ERTMS), time to alert (GNSS) and safe down time (EN 50129) – see Fig. 3. This detailed analysis will also enable to unambiguously justify why THR instead of integrity risk must be used, why continuity risk should be replaced by dependability attributes, etc.

5 THE PINEROLO–SANGONE PILOT LINE

RFI (Rete Ferroviaria Italiana) and Ansaldo STS are deploying the Pinerolo–Sangone pilot line (a regional line in the north-west of Italy) to contribute to the identification of the certification process of an ERTMS/ETC solution based on the GNSS positioning technology after the positive test campaign in Sardinia with 3InSat and ERSAT EAV (Fig. 4). In this context, RFI has developed a preliminary hazard analysis that after having been reviewed by an Independent Notify Body was submitted to the ANSF (Italian Railways Safety Agency) and to GSA, ESA and ERA. All these entities are now involved and working together, including the Shift2Rail, with the goal to agree and share the path to allow ANSF to express its opinion before starting the formal authorization process. This initiative (the first one in Europe)

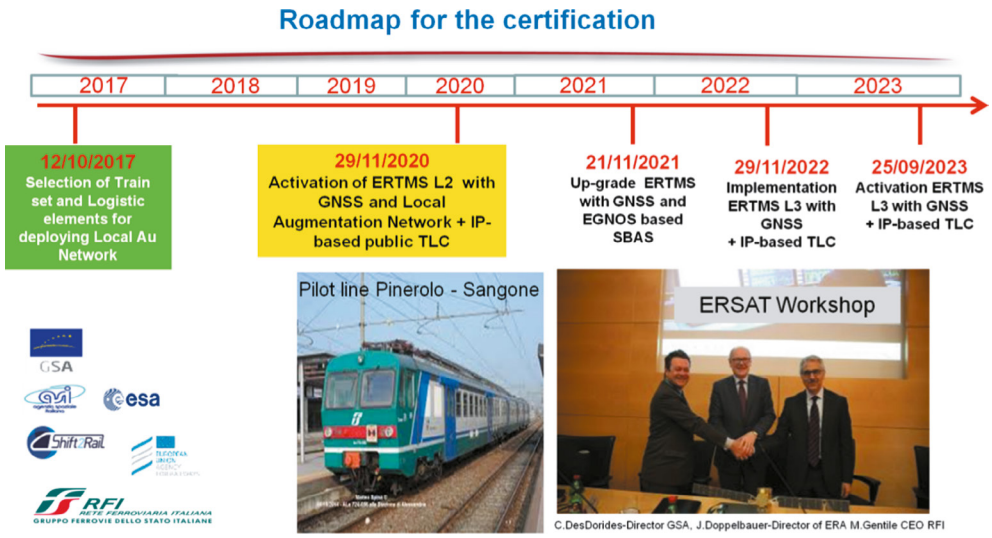

Figure 4: Roadmap for supporting the certification process.

represents an important step forward to build the consensus for introducing the GNSS positioning technology into an ERTMS/ETCS-based solution. The ambition of this initiative is also to exploit the GNSS infrastructures already developed and under development for the aviation sector.

6 CONCLUSION

GNSS positioning technology represents a step-change innovation for the evolution of ERTMS and to encourage its adoption is necessary to agree a process for the introduction of this technology that may lead to update the TSI to enable the use of this innovative solution.

This article has described a possible framework for the certification and safety authorization process for a LDS based on the GNSS positioning technology integrated into the ERTMS/ETCS evolution framework. This framework will be developed and tuned for the safety approval process required for the validation of the ERTMS/ETCS-based solution integrated with LDS on the pilot line Pinerolo– Sangone, close to Turin in Italy, around 2020.

ACKNOWLEDGEMENTS

This work was supported from the European H2020 research and innovation programme within the EU-US RHINOS project (2016–2017), by the ESA STPERTMS 9053_PRP_NSL project (2018–2019), by the H2020 ERSAT GGC project (2017–2019) and the Czech national project PosiTrans (2018–2020) within the MSMT CR OP VVV programme.

REFERENCES

[1] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety.

[2] 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.

[3] Guide – Issuing a safety certificate or safety authorization, European Railway Agency, 12 June 2015, 86 pages.

[4] Impact Assessment Report – Accreditation & Recognition schemes: CSM on Risk Assessment. European Railway Agency, 22 May 2012, 49 pages.
[5] Report on the certification of ERTMS equipment. The European Railway Agency, 14 April 2011, Document reference: ERA/REP/2011-08/ERTMS, 51 pages.
[6] Jovicic, D., CSM for risk assessment: Proactive decision making instrument Consequences and benefits of latest changes. Safety Conference of Danish Transport and Construction Agency – Copenhagen, 28 October 2015, presentation, 50 slides.
[7] Jovicic, D., CSM for risk assessment (Reg. 402/2013) & Requirements for CSM Assessment Body. NAB/RB Training Workshop in Valenciennes, April 2016, presentation 63 slides.
[8] Jovicic, D., Explanatory note on the CSM Assessment Body referred to in Regulation (EU) N°402/2013 and in OTIF UTP GEN-G of 1.1.2014 on the Common Safety Method (CSM) for risk assessment, The European Railway Agency. Document reference: ERA/GUI/01-2014/SAF, 17 pages.
[9] Guide for the application of the CSM design targets (CSM-DT). The European Railway Agency. 23 December 2016, Document reference: ERA-REC-116-2015-GUI, version 1, 139 pages.
[10] Issuing a safety certificate or safety authorisation – a guide for national safety authorities. The European Railway Agency, 12 June 2015, Document reference: ERA/GUI/11-2013/SAF V 2.1, 86 pages.
[11] Collection of examples of risk assessments and of some possible tools supporting the CSM Regulation. The European Railway Agency, 06 January 2009, Reference: ERA/GUI/02-2008/SAF, version 1.0, 105 pages.
[12] Common Safety Method (CSM), risk evaluation and assessment. The European Railway Agency, Published in the Official Journal of the European Union on 29th of April 2009, 4 pages.
[13] 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.
[14] Directive 2004/49/EC of the European Parliament and of the Council of 29 April 2004 on safety on the Community's railways (Railway Safety Directive).
[15] Regulation (EC) No 352/2009 of 24 April 2009 on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC.
[16] EN 50126 Railway Applications: The Specification and Demonstration of Dependability Reliability, Availability, Maintainability and Safety (RAMS). CENELEC European standard, 2002.
[17] EN 50128 Railway Applications: Communications, signalling and processing systems – Software for railway control and protection systems. CENELEC European standard, 2003.
[18] EN 50129 Railway Applications: Safety related electronic systems for signalling. CENELEC European standard, 2003.
[19] Regulation (EU) No 1158/2010 of 9 December 2010 on a common safety method for assessing conformity with the requirements for obtaining railway safety certificates.
[20] Regulation (EU) No 1169/2010 of 10 December 2010 on a common safety method for assessing conformity with the requirements for obtaining a railway safety authorisation.
[21] Coenraad, W., Cross-Acceptance of Signalling Systems – The Myths and the Reality. IRSE News Letter, Honk Kong Section, September 2006, Issue 22, 6 pages.

[22] Munck, S., New CENELEC Standards & CSM-RA, RAMBOLL, 2017, presentation 29 slides.
[23] Minimum operational performance standards for GPS WAAS Airborne Equipment. RTCA DO-229D: RTCA, Inc., Washington, 2006.
[24] 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.
[25] Regulation (EU) No 1077/2012 of 16 November 2012 on a common safety method for supervision by national safety authorities after issuing a safety certificate or safety authorisation.
[26] Regulation (EU) No 1078/2012 of 16 November 2012 on a common safety method for monitoring to be applied by railway undertakings, infrastructure managers after receiving a safety certificate or safety authorisation and by entities in charge of maintenance.
[27] Regulation (EU) No 445/2011 of 10 May 2011 on a system of certification of entities in charge of maintenance for freight wagons and amending Regulation (EC) No 653/2007.