A safety regulatory framework for certification and authorization process of self-driving cars: experience from European railways

Ales Filip
University of Pardubice, Czech Republic. E-mail: ales.filip@upce.cz

Francesco Rispoli
Hitachi Rail STS S.p.A, Italy. E-mail: francesco.rispoli@hitachirail.com

Roberto Capua
Sogei S.p.A, Italy. E-mail: rcapua@sogei.it

Safety improvement represents a key driver in the development of self-driving cars (SDCs). It is currently assumed that safety of SDCs should be approximately at the same level achieved by trains or airplanes. For example, the European Railway Traffic Management System (ERTMS) which oversees train speed and stopping position is compliant with a Tolerable Hazard Rate (THR) of 10^{-9}/h/train. To guarantee this high level of safety, it is necessary to have a clearly defined regulatory framework for certification and safety approval process for SDCs with Automatically Commanded Steering Functions (ACSF). Nevertheless, many car manufacturers are relying on extensive experimental campaigns to demonstrate the achievable level of safety. This paper describes a framework for certification of SDCs based on the experience of the ERTMS authorisation process adopted for train control in Europe and accepted world-wide. This framework is built on a so-called Common Safety Method for Risk Assessment (CSM-RA) that was originally set up for management of significant safety changes in a railway system. Furthermore, the CSM Design Targets are introduced to harmonise safety requirements for SDCs with ACSF. We believe that a synergy between train and car automation leveraging on the safety primacy of the ERTMS and the mass market potential of cars is a stimulus to achieve the highest safety standards at lower costs.

Keywords: Automated car driving, certification, CSM-RA, ERTMS, RAMS, risk assessment, standardization.

1. Background

At present many cars have already implemented some kinds of driver assistance functions and the race between automotive companies globally is heading towards fully self-driving cars (SDCs). Safety becomes out of doubt a fundamental issue in this development.

A risk acceptance criterion, which is a measure of the required safety, represents a critical attribute reflecting a consumer trust in SDCs. It enables to estimate whether and when the driverless vehicles will be mass-produced and put into operations. How much safe should driverless vehicles be to be accepted by society? Respondents of one latest survey expect that self-driving vehicles should be four to five times safer than human driven vehicles – see Liu et al. (2019). It also implies that the responders expect the global road traffic fatality risk (TFR) should be reduced by about 2 orders. The current TFR is estimated as 17.4 fatalities per 100,000 population and year (~ 10,000 hours). It implies that the responders also assume that the acceptable risk associated with a driverless car should approximately correspond to the safety level currently guaranteed on railway or in civil aviation.

Railway traditionally belongs to a regulated and very safe transport sector. From the very beginning railway safety is based on conservative principles and worst-case approach. The worst-case approach takes into account many scenarios and assumptions that are unlikely to occur simultaneously. Excepting safety, a great attention is also paid to efficiency of railway operations. Railway technical systems shall be safe enough but shall be not safer than actually required, otherwise they would be more expensive and no one would use them.

The European Railway Traffic Management System (ERTMS) is a standardised commanded and control system conceived to intervene in case of driver's errors by supervising the maximum allowed speed and stopping position of the train. ERTMS is in operation by more than 20 years and it ensures the highest safety level ever achieved in the transport sector. Since it is not clear so far how the generally acceptable certification and safety approval process for SDCs should look like, the framework for certification and safety approval process used for the ERTMS has been proposed in this paper as an example for certification process for SDCs operated on a road-side digital infrastructure.

Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Published by Research Publishing, Singapore.
ISBN/DOI: 978-981-14-8593-0

Section 2 of the paper briefly summarises the existing type-approval process and regulations for road vehicles in Europe. Functional railway certification and safety approval process, which could be served as an example for SDCs, is outlined in Section 3. Section 4 then describes the proposed concept of the safety regulatory framework for SDCs based on that railway experience. Finally, main results and conclusions are summarised in Section 5.

2. Type-approval framework for cars in EU

Before a new model of vehicle is to be placed on the EU market, it must pass through a so called type-approval process, i.e. homologation. Within this process national authorities in EU Member states certify that the model of a vehicle (or its part) satisfies all EU safety, environmental and production requirements. This type-approval process has to be performed according to the Regulation (EU) 2018/858 of May 2018 which establishes the harmonised framework for approval of motor vehicles.

The manufacturer shall submit according to the above regulation the application accompanied by the information folder to the *approval authority* in a given Member State. If all relevant requirements are met, the national authority delivers an EC type-approval

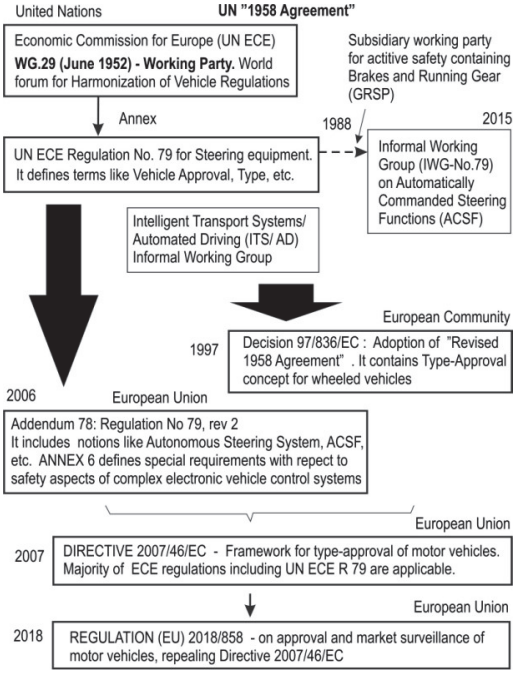

Fig. 1. Chronology of regulations towards type-approval process of vehicles with ACSF in Europe.

certificate to the manufacturer authorizing the sale of the vehicle type in EU. After that the manufacturer issues a Certificate of Conformity, which accompanies every produced vehicle. The certification process is based on a mutual recognition, i.e. cross-acceptance of approvals by national approval authorities in EU Member States.

The above EU regulation has been formulated in accordance with the 1958 United Nations Economic Commission for Europe (UN ECE) agreement and additional subsequent regulations as it is outlined in Fig. 1.

In next section there is described an efficient certification and safety approval process, which is currently used for railway safety-related systems on European Railways. A harmonised approach for derivation of railway safety requirements for such systems is described as well. The intention of such description is to provide to the automobile sector an inspiration for a similarly effective type-approval process for self-driving cars.

3. Certification of railway safety systems

3.1 *Description of whole authorization process*

Certification and safety approval for ERTMS is retained as a reference. 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).

The ERTMS is a centralised command and control system which authorizes the train to move until a predetermined point once the train position has been detected and all the safety conditions are fulfilled. Train positioning is determined by a SIL 4 on-board odometer whose errors are reset periodically with transponders (balises) deployed along the railways. This architecture is well consolidated and operational since more than 20 years, cumulating billions of Km travelled without accidents. Nowadays the ERTMS is evolving by adopting the GNSS positioning, hybrid telecom networks and autonomous driving operations (ATO), making it similar to the Connected car architecture. These changes will undergo the approved certification and authorization process in order to guarantee the safety levels. Furthermore, hybrid positioning systems (GNSS + IMU) are being developed in order to increase the availability of the vehicle's positioning. The objective is to reach a THR better than 10^{-9}/ h or even than 10^{-10}/ h. To achieve this goal a cross-check with an independent non-GNSS localizer, i.e. IMU as the Function B shown in Fig. 2, has been defined in the RHINOS

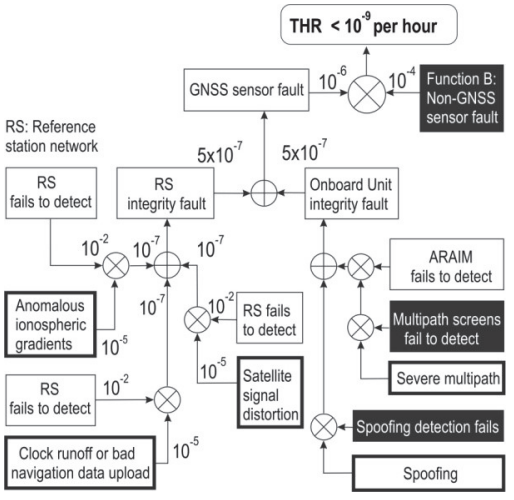

Fig. 2. Example of THR allocation for GNSS-based train position determination.

project – see Rispoli et al. (2018).

A key feature of the ERTMS is to ensure the interoperability among on-board and track-side subsystems shared between different actors, mainly Infrastructure Managers (IM) and Railway Undertakings (RU). A similar scenario is foreseen between different car manufactures and smart road infrastructure managers. High safety and dependability requirements RAMS – Reliability, Availability, Maintainability and Safety are one of the pillars of the ERTMS certification and must be met also when track balises are replaced with virtual balises and detected by GNSS positioning – see e.g. ERSAT GGC project (2019). Therefore it is necessary to pass the certification and approval process that guarantees all requirements for ERTMS (i.e. safety standards CENELEC 5012x,Technical Specifications for Interoperability (TSIs), EU regulations, directives, etc.) are met. The EU Directive 2016/797 extends authorization process of Control Command Systems (CCS) to the entire railway system - it supports concept of "Cross Acceptance" as a stepping stone to the interoperability within the Trans European Network. The framework for certification and safety authorization of ERTMS based on GNSS has been described by Filip et al. (2018).

Excepting Verification and Validation (V&V), Safety Case elaboration (for on-board, track-side and integrated track-side and on-board equipment) and Independent Safety Assessment (ISA), the system compliance with ERTMS TSIs should be checked within the certification process. Railway actors have to manage safely all changes of the European railway system – including GNSS positioning, hybrid GNSS positioning and other sensors integration with ERTMS. A Common Safety Method for Risk evaluation and Assessment (CSM-RA) must be used according to the European railway regulation No 402/2013 if a safety-related change in a system is significant – see Fig. 3.

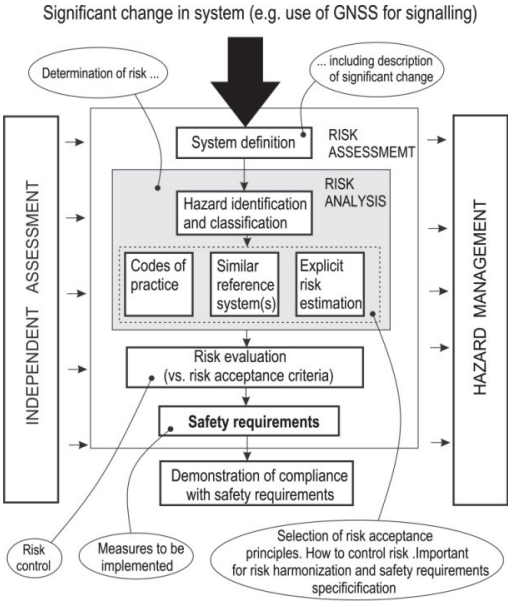

Fig. 3. Common Safety Method for risk evaluation and Assessment (CSM-RA).

The CSM-RA shall cover the whole CENELEC lifecycle including safety evaluation during system operations. The above mentioned activities such as V&V, Safety Case elaboration, Independent Risk Assessment and Conformity Assessment with respect to TSIs (i.e. certification) cover only part of the safety lifecycle according to CENELEC EN 50126. As is it outlined in Filip et al. (2018), CSM-RA creates a framework for the whole certification and safety approval process for European railway systems. The safety monitoring during real system operations is not covered by the activities mentioned above. Therefore CSM-RA requires a separate Safety Management System (SMS) to be implemented and performed within Railway Undertaking (RU) and Infrastructure Manager (IM) activities to fill in the safety gap mentioned above. The European Common Safety Targets for the whole railway system are used for safety evaluation within the SMS.

The aim of European railway authorities and European railway industry is to develop interoperable railway systems based on common

regulations. The cross-acceptance of safety approvals for sub-systems and equipment by the different national railway authorities is essential. The cross-acceptance becomes e.g. also critical in the area of exploitation of the aviation GNSS Safety-of-Life (SoL) service as Generic and Specific Applications for ERTMS. In this sense a Safety Case is a very important part of the conformity assessment documenting the achieved safety levels. The cross-acceptance of GNSS SoL service for ERTMS could be demonstrated via use of CSM-RA supported by following Generic Safety Cases: 1) Generic Product Safety Case – which is independent of railway application, and 2) Generic Application Safety Case - for a class of applications.

3.2 *Risk harmonization for railway systems*

Harmonization of risk acceptance and safety requirements specification in land transport like rail or road is critical not only from viewpoint of the required safety, but also from the required system efficiency. Railways have (compared to automated cars) a long-term experience with harmonisation of risk acceptance including the whole certification and safety approval process for developed Technical Systems (TS). It is because TS shall be safe as it is required by society – but TS must not be exceedingly safe because they would be too expensive and nobody would use them. The European railway sector utilises the above mentioned CSM-RA for harmonisation of risk acceptance. The harmonization and mutual recognition of safety requirements is performed via Risk Acceptance Principles (RAP) and Risk Acceptance Criteria (RAC) – see Griffin and Bearfield (2016).

Widely acceptable Codes of Practice (CoP) such as ERTMS TSIs, CENELEC standards, etc. used as RAP enable to harmonise risk and thus railway safety requirements across Europe. These CoP have been elaborated on the basis of a long-term experience with designing of railway safety-related systems. Reference systems can be used as Risk Acceptance Principles in a very similar way as Codes of Practice because a reference system is a system that has been proven in practice to have an acceptable safety level. Both Code of Practice and similar Reference Systems used as Risk Acceptance Principles can be also considered at the same time as Risk Acceptance Criteria.

If a sufficient experience with the specific safety system design and assessment is missing, which is also the case of high-safety integrity steering systems for SDCs, then explicit risk estimation as RAP must be applied. Then specific railway Risk Acceptance Criteria are also needed – e.g. MEM, ALARP, GAMAB, etc. Problem is that these RACs are not harmonised in Europe. Thus, the related risk cannot be acceptable in all EU countries. It means that resulting safety requirements for TS cannot not be harmonised as well. Widely acceptable harmonised RAC are needed, as it is outlined in next Section.

3.3 *Design safety targets*

In rail domain it was obviously needed to enable mutual recognition of risk assessment of TS when also the explicit risk estimation as 3rd Risk Acceptance Principle is used. In order to harmonise safety requirements for design of E/E/PE (Electric/ Electronic/ Programmable Electronic Safety-related Systems) as TS, Common Safety Method Design Targets (CSM-DT) have been introduced by ERA (EU Agency for Railways) – see Jovicic (2016). The goal of the harmonised CSM-DT is to assure that designed TS will be safe enough, as it is required by society. At the same time TS will not be safer than actually needed.

CSM-DT were derived on the basis of current experience and the best practice with railway safety-related system design. They represent harmonised functional safety requirements for TS, i.e. safety levels. CSM-DT can be used as quantitative safety requirements for random HW failures of E/E/EP technical systems. And how can be the harmonised design targets used? A hazard rate of a specific functional hazardous failure of a technical system should be estimated first. The use of techniques such as FMECA or fault tree analysis (FTA) can involve for this purpose. The estimated hazard rate is then compared with the required CSM-DT. If the compliance of the TS with the CSM-DT is not assured, then changes in the safety design must be performed.

4. Regulatory framework for certification of self-driving vehicles

In recent years automotive researchers are looking for possibilities how to utilize knowledge and technologies from railway field, e.g. the ERTMS/ETCS concept, in favour of SDCs and vice versa. It is also the case of the above mentioned safe train position determination based on GNSS developed for ERTMS, which has also a great potential for automated car driving – see Rispoli, Enge et al. (2018). On the contrary, diverse sensors and methods currently utilized in the automotive industry such as cameras, visual odometry, computer vision, etc. could bring benefits to rail sector. It was found such ‘synergy’ effect, reflecting the long-term railway experience with building and operating very safe systems, can be also efficiently utilised in case of defining a safety regulatory framework for automated driving.

As it is mentioned in Section 3, the efficient safety approval process enabling to demonstrate and maintain during operations the highest level of safety (SIL 4; THR ~ $1x10^{-9}$/ h) for complex railway safety-related systems like ERTMS/ETCS has been already used on the European railways. A similar process is to be defined for the type-approval of SDCs with ACSF supported by a digital road-side infrastructure to demonstrate approximately the same safety level for such new road systems. The safety regulatory framework is excepting car manufactures also required by every national approval authority, its technical services and many other actors in road transport. Without this trustworthy proof of safety it would be impossible to convince future customers that SDCs are safe enough.

The reality is that such a key safety approval process is missing. This need is not even defined in the latest EU Regulation 2018/858 of 30 May 2018 on the approval of motor vehicles that repeals the Directive 2007/46EC.

4.1 *Proposed methodology*

Seeking for inspiration for the approval process of SDCs with the required (high) safety level in other transportation modes, only aviation, railway or a few others specific safety standards (i.e. DO-178C, CENELEC EN 5012x, etc.) have been usually considered by different expert teams - see e.g. Edwards et al. (2017). It has been mainly analysed how these single standards could be utilised beyond the automobile functional safety standard ISO 26262 to define an efficient certification process for SDCs with ACSF. However, the above approach could not bring applicable solutions. The main difficulty consisted in the fact that it was only investigated how to apply these single 'non-automotive' safety standards for the car certification. No supporting instruments such as TSIs, EU directives, regulations, guidance documents, etc., which are mandatory e.g. in the railway sector for ERTMS/ETCS have not been considered. Another problem was that the attention regarding the SDC certification was only focused on a car and not on a supporting road-side digital infrastructure, which shall be also assessed within the certification and safety authorization process. In many cases the purpose of the SDC certification has not been explained at all. The certification was required – but why? Issues such as emphasis on interoperability, cross-acceptance and necessary safety monitoring and evaluation during real car operations through hazard management, which should also be addressed in the future concept of automated car driving, have been forgotten. The cross border operation in different EU member states, interoperability between on-board and way-side equipment and also interoperability among subsystems from different manufactures is undoubtedly required. All these features have to be implemented together with fulfilment of very high safety integrity (e.g. ASIL D) and dependability requirements for safety functions in SDC.

Therefore the concept of a framework for certification and safety approval process for self-driving cars supported by a road-side digital infrastructure has been proposed on the basis of the experience with the safety authorization process already applied on European railways. The Common Safety Method for Risk evaluation and Assessment (CSM-RA) has been adopted from the railway sector because it also has a potential to create the fundamental framework for the safety approval process of SDCs. The major advantage of the proposed concept is the ability to implement the whole Risk Management Process in compliance with ISO 26262 and also perform Hazard Management during real SDCs operations. Demonstration and maintenance of the required (high) design safety targets for automated car steering functions belong among the main drivers of the proposed concept.

The advantage of CSM-RA consists in fact that it can cover significant safety-related changes for both (a) small and simple systems, and also (b) large and more complex ones. Important is that CSM-RA enables mutual recognition of the risk assessment outputs using harmonisation of: a) the risk management process, and b) the exchange of safety relevant information among different actors including the evidence resulting from the utilised risk management process.

4.2 *Certification of automated driving systems*

The concept of the overall regulatory framework for the safety certification and type-approval process for SDCs consisting of CSM-RA including hazard management via a Safety Management System (SMS) is proposed in Fig. 4. The concept reflects needs for cross-acceptable solutions and profits from similarities between interoperable railway and automotive safety systems consisting of many by telecommunications connected on-board and way-side sub-systems. It aims at managing all significant changes safely during both automated driving system development and also SDCs operations.

The safety approval process shall start in early stages of the safety lifecycle – starting from the preliminary system definition. It is followed by the system design, verification & validation (ISO 26262), safety case elaboration for on- board, way-side and integrated solutions, and conformity assessment by a Notified Body (NoBo) through the certification of the proposed solutions in order

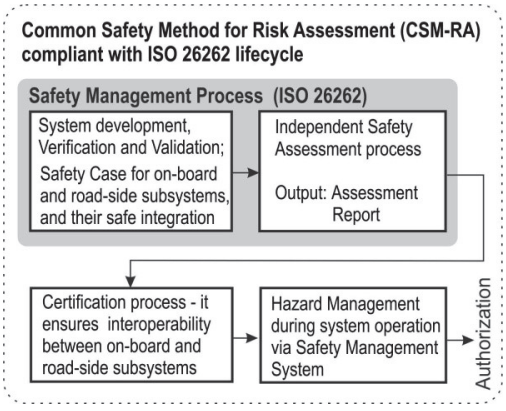

Fig. 4. Proposal of safety regulatory framework for certification and approval of self-driving vehicles.

to demonstrate its cross-acceptance and interoperability.

Excepting this, the operational performance should be monitored by fleet operators and road infrastructure managers via a SMS in order to maintain the required operational safety. At this early development stage the concept doesn't reflect the case of mixed operations, consisting of operations of fully automated cars and cars still requiring some portion of supervision by a human driver.

The role of individual railway actors is clearly defined in the existing certification and safety approval process. A similar allocation of actors and roles should be done within the safety regulatory framework for automated driving. This process will not obviously start from the scratch because existing accreditation schemes for vehicle type-approval can be utilized.

It is expected the SMS will be supported by diagnostic and other operational data utilised within the connected vehicle concept. Finally the proposed solution (or change) should be authorised by National Approval Authorities, as it is already common in the existing type-approval process – see e.g. Regulation (EU) 2018/858. More detailed description of the individual phases of the process can be also found in Filip et al. (2018).

One of critical issues, which shall be also solved within the safety regulatory framework, is related to the cross-acceptance, i.e. mutual recognition of systems. It reflects the intention to use system elements or subsystems that have not been originally developed according to requirements for automotive safety applications. For example GNSS Safety-of-Life (SoL) service, which was originally developed for safety operations in aviation, represents one of them. The railway CENELEC safety standard EN 50129 enables to solve the cross-acceptance issue via Generic Safety Cases – by means of a Generic Product Safety Case and Generic Application Safety Case. It seems GNSS could be cross-accepted by using of CSM-RA supported by Generic Safety Cases. This example shows that the field of railway safety could provide answers to different questions regarding safety of SDCs because of a long-term experience with building of railway systems with high-safety integrity.

4.3 *Harmonised safety requirements for SDC*

System safety requirements shall be specified at the beginning of system lifecycle. These requirements are utilized for system design and later also for system certification and safety authorization. Derivation of each safety requirement should be properly justified. It is perhaps useless to repeat that the requirements must be harmonized (consensus must be achieved) in order to meet requirements for cross-acceptance and interoperability. The safety requirements should result from the socially tolerable risk. This practice is common in the railway sector, e.g. in the field of ERTMS, which is successfully operated in numerous EU Member States. However, this practice is still missing in the field of automated cars.

It has been mentioned in Section 3.2 that the railway community, thanks to its long-term experience with signaling systems design and operations, has clearly defined risk acceptance principles (RAP) and criteria (RAC), which lead to harmonised safety requirements for technical systems (TS). In cases where RAP/RAC cannot be easily defined, then the harmonised CSM Design Targets (CSM-DT) can be used. Both RAP/RAC and CSM-DT reflect needs for socially acceptable risk. Detailed justification of CSM-DT values can be found e.g. in Jovicic (2016).

A different situation is in the field of SDCs because of lack of a sufficient experience with design and operation of high-safety integrity automated steering systems and their interoperability with road-side safety systems. Since there is not available any widely acceptable procedure for clear specification and justification of harmonised safety requirements for automated driving, it is recommended to use a similar concept to the railway CSM-DT in order to specify widely acceptable design targets for technical safety systems in SDCs.

Based on the latest survey regarding the required safety of SDCs from the public side and comparing the tolerable risk for automated driving with e.g. the railway MEM Risk Acceptance Principle, it seems that CSM-DT for automotive safety systems could have similar values as those for rail. The railway CSM Design

Targets can be used as an example for specification of harmonized safety levels for SDCs with ACSF.

4.4 *Standardization: RTCM SC-134 Committee*

On June 2018 RTCM (Radio Technical Commission for Maritime Services), the international organisation working for decades into the field of High Accuracy GNSS Systems standardisation, founded a new Committee SC-134 entitled "Integrity for High Accuracy GNSS-Based Applications".

The main scope of this Committee is to study and develop horizontal standards for the emerging applications needing both High Integrity and High Accuracy navigation. Relevant universities, service providers and manufactures operating in different applications sectors, are present into the Committee. Four Working Groups have been created for this scope:

- WG 1: Automotive
- WG 2: Rail
- WG 3: Other Applications
- WG 4: Harmonization of Requirements and Metrics.

RTCM puts in his work the relevant heritage coming from the RTCM SC-104 standards on Differential GNSS that defined the basis for standards and protocols currently used for Real-Time Kinematics (RTK), Network RTK and Precise Point Positioning (PPP) systems developments. RTCM messages are currently embedded into SAE message #18 for Short Range Communication in the automotive sector. It shows a new emerging roadmap for integration and merging of standards from different application sectors that is in line with inter modality and autonomous mobility (train and cars). Within this framework, standardisation will be relevant, being the input for the certification and safety approval process.

The intention of the Committee is to develop a critical detailed review of relevant Requirements and Standards for each application sector by the end of year 2019 and to proceed with the definition of relevant Augmentation Messages for High Accuracy and High Integrity Systems implementations, Safety concepts and metrics (e.g. THR vs. aviation Integrity Risk) that are integrated into the WGs work for meeting Transport Requirements.

In order to guarantee the backward compatibility with the historical developments in the High Accuracy application sector, the Augmentation Messages will be integrated within the long-standing and consolidated RTCM SC-104 message format structure and protocol – i.e. Networked Transport of RTCM via Internet Protocol (NTRIP). The SC-104 advanced messages development, dealing with both Observables (OSR-Observation Space Representation and SSR-State Space Representation) and the participation in SC-104 and SC-134 of most important GNSS receiver manufacturers, Augmentation Service Providers and Software Developers, as well as Satellite Operators, as well as single applications stakeholders, ensures an agreement of messages contents along the whole Value Chain. The development of liaisons and Cross Tables with single sectors international organisations is a relevant mission for ensuring the horizontal standardization perspectives of the Committee.

4.5 *Next steps forward*

This paper outlines the first fundamental concept of the safety regulatory framework for automated car driving based on the experience with a similar safety approval process which has been already utilised for interoperable safety-related systems on the European railways. Next development of the framework should also take into account:

- Dissimilarities and differences between safety concepts for self-driving cars and railway signaling and train control systems based on telecommunications including ERTMS – e.g. guided vs. non-guided transport modes, fail-safe (fail-stop) and fail-operational principles, different operational scenarios, environments, etc.;
- Differences between the existing automobile type-approval and railway certification and safety authorization processes according to relevant regulations;
- Safety gaps in the type-approval with respect to SDCs operated on a way-side digital infrastructure;
- All benefits resulting from the use of Common Safety Method for Risk Assessment (CSM-RA), Common Safety Targets (CST) and system CSM Design Targets (CSM-DT) for technical systems that have been originally employed for management of significant changes in a railway system during its whole lifecycle;
- Roles of actors in the individual tasks within all phases of the risk management process - i.e. Validation & Verification, Safety Cases elaboration, conformity assessment, cross-acceptance, operational performance monitoring, etc.;
- Expected outputs from the safety regulation framework.

5. Conclusions

In this paper we proposed to use the certification process adopted for the ERTMS train control to contribute to the preparation of the safety regulatory framework for certification and safety type-approval process of self-driving cars (SDCs) with Automatically Commanded Safety Functions (ACSF) requiring the highest automotive safety integrity level (ASIL D). Its novelty consists in exploiting the synergy between train and car automation - both based on a connected vehicle interacting with a centralised system. The pillar is the unprecedented experience of the European railways stake holders with regard of standardising the safety approval process ensuring speed supervision and braking control functions to fulfil the SIL 4 objective. The concept profits from the synergy between interoperable ERTMS, consisting of on-board, track-side and communication equipment, and self-driving vehicles with ACSF operated on a digital road-side infrastructure. Similarities between railway and automotive safety concepts resulting from railway CENELEC and automobile ISO safety standards have been utilized as well.

The proposed framework is based on a so-called Common Safety Method for Risk evaluation and Assessment (CSM-RA), which was originally set up for the management of significant safety changes in complex railway safety-related systems including ERTMS. In case of self-driving car this significant safety change can represent e.g. the introduction of an ACSF. This approach can bring to the automobile industry many benefits. The most important being the recognized trustiness having the railways safety approval process already been standardized and applied on operational trains cumulating hundreds billion km. Furthermore, having the ERTMS eliminated *de facto* the potential driver's errors, is possible to achieve the highest safety level (SIL 4 with THR < 1e-9/ h) for a transportation means, justified by harmonised safety and dependability requirements (RAMS).

Current international standardization activities regarding the use of precise and high integrity GNSS position determination within the RTCM SC-134 committee are briefly mentioned because for the first time, the needs of rail and road applications including self-driving cars are discussed by a team of experts and this paper will be also utilized for these RTCM standardization activities.

The references included in this paper are the basis forming and supporting the certification and authorization process of railway safety-related systems in Europe and could be utilised as examples and inspiration for setting up a similar safety regulatory framework for self-driving cars.

Acknowledgement

The work was supported 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', No. CZ.02.1.01/0.0/0.0/17_049/ 0008394.

References

Liu, P., R. Yang and Z. Xu (2019). How Safe Is Safe Enough for Self-Driving Vehicles? *Risk Analysis 39(3)*, 315-325.

Rispoli, F., A. Neri, C. Stallo, P. Salvatori and F. Santucci (2018). Synergies for trains and cars era of virtual networking automation in the era of virtual networking. *J. Transp. Tech 8*, 175-193.

ERSAT GGC project (2019). Available at: http://www.ersat-ggc.eu/

Filip, A., S. Sabina and F. Rispoli (2018). A Framework for Certification of Train Location Determination System Based on GNSS for ERTMS/ETCS. *Int. J. Transp. Dev. Integr. 2(3)*, 284–297.

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, OJ L121/pp. 8-25.

Griffin, D. J. K. and G. Bearfield (2016). The use of design targets in harmonization of safety management in the European rail industry. *Proc. of the ESREL 2016*, 1299-1305.

Jovicic, D. (2016). Guideline for the application of harmonised design targets (CSM-DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013. European Railway Agency, doc. ref. ERA-REC-116-2015-GUI.

Rispoli, F., P. Enge, A. Neri and F. Senesi (2018). GNSS for rail automation & driverless cars: a Give and Take paradigm. *Proc. of ION GNSS+ 2018*.

Edwards, M., M. Seidl, M. Tress, A. Pressley and S. Mohan (2017). Study on the assessment and certification of automated vehicles. The European Commission, Directorate C — Industrial Transformation and Advanced Value Chains.