New onboard train integrity and train length determination: what are the safety requirements?

Insaf Sassi, El-Miloudi El-Koursi, Salvatore Danilo Iovino, Nicola Ricevuto

Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 00 (2022) 000–000

Transportation Research Procedia

www.elsevier.com/locate/procedia

Transport Research Arena (TRA) Conference

New Onboard Train Integrity and Train Length Determination: What are the Safety Requirements?

Insaf Sassi[a]*, El-Miloudi El-Koursi[b,a], Salvatore Danilo Iovino[c], Nicola Ricevuto[c]

[a] *IRT Railenium, 180 rue Joseph-Louis Lagrange, F-59300 Famars, France*
[b] *COSYS-ESTAS, Univ Gustave Eiffel, IFSTTAR, Univ Lille, France*
[c] *Hitachi Rail STS, Via Paolo Mantovani 3-5, 16151 Genoa, Italy*

Abstract

In the European Train Control System (ETCS) level 3, using on-board control-command systems for the train integrity monitoring and length determination functionalities transfer the train operation safety responsibilities from the infrastructure managers to the railway operators. To ensure the implementation of these safety critical functions, quantitative and qualitative safety requirements shall be specified as stipulated in the railway safety European standards and regulations. These functions must be guaranteed by fulfilling safety integrity level SIL 4 requirements at the system level, independently from trackside infrastructure. The contribution presented in this paper consists in proposing a methodology to determine the safety targets of both functions in terms of Tolerable Hazard Rates (THR). The obtained THRs are then apportioned among the safety related functions to specify the quantitative safety requirements for every functional part.

Keywords: On-board train integrity; train length; Railways signalling; ETCS; urban transport safety; risk from automation

1. Introduction

Traditional signaling systems rely on track circuits or axle counters for train position detection and train integrity determination. This approach requires relevant capital and operational expenses at the trackside level and contributes to limitations in the line capacity. European railway stakeholders have worked to specify the European Train Control System (ETCS) level 3 to cope with these disadvantages to increase the line capacity cost-effectively. The trackside equipment is removed and replaced by on-board modules that ensure the supervision of the safe train journey by

* Corresponding author. Tel.: +000-000-000-0000;
E-mail address: Insaf.sassi@railenium.eu

Peer-review under responsibility of the scientific committee of the Transport Research Arena (TRA) Conference

continuously monitoring its integrity i.e., no wagon is lost, after correctly evaluating the train's length. These functions are critical because a detached vehicle can lead to a train collision. Add to that, in ETCS level 3, where train occupation is determined at the on-board level, train driver involvement in entering train length is now automated to avoid human errors that could lead to collision or derailment accidents because of a wrong length value. With this aim, novel ETCS compliant on-board train integrity (OTI-I) and train length determination (OTI-L) functions are proposed by Shift2Rail partners within Technical Demonstrators 2.5 (on-board train integrity), in X2RAIL-2 and X2RAIL-4 projects. However, using on-board control-command systems for the train integrity monitoring and length determination functionalities transfer the train operation safety responsibilities from the infrastructure managers to the railway operators. To ensure the implementation of these safety critical functions, quantitative and qualitative safety requirements shall be specified as stipulated in the railway safety European standards i.e., CENELEC 50126 (2017) and the European regulation (2013) on Common Safety Methods (CSM). Train integrity monitoring and length determination must be guaranteed by fulfilling safety integrity level SIL 4 requirements at the system level, independent from trackside infrastructure. The contribution presented in this paper consists in proposing a methodology to determine the safety targets of OTI-I and OTI-L functions in terms of Tolerable Hazard Rates (THR). The obtained THRs are then apportioned among the safety related functions of OTI-I and OTI-L to specify the safety requirements for every involved functional part. In this paper, we start in section 2 with defining the systems under consideration and the scope of the analysis. Sections 3 and 4 are devoted for describing the preliminary results concerning the safety requirements of OTI-I and OTI-L by applying methodologies stipulated in standard EN50126 and European regulation on CSM. A conclusion and perspectives are given in section 5.

2. Onboard Train integrity and train length determination specification

2.1. Onboard Train Integrity (OTI-I)

The train integrity monitoring system supervises the status of the train tail by checking the coherence of the last wagon movement. In fact, the last wagon must be regularly advancing with the head of the train. The train integrity status information must be provided by the OTI-I, as an external device, to the ETCS onboard as shown in Fig.1 and then transmitted to the Radio Block Centre (RBC). The OTI-I shall report to the ETCS onboard three possible values: *confirmed, lost or unknown* according to CR940 (2019).

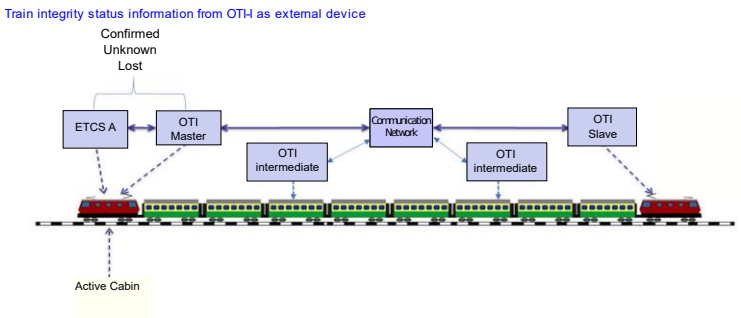

Fig. 1. OTI-I system definition

The proposed OTI-I system is composed of OTI Master functional module connected to ETCS, OTI Slave functional modules located in other waggons, where these modules exchange status data via the communication network to evaluate the train integrity status. The way the integrity is evaluated depends on the technology used for the communication among the OTI-I modules and the train type (passenger or freight). Consequently, three classes of OTI-I are defined and hence the integrity criteria. Product class 1 refers to train with wired communication network where the integrity is evaluated based on the communication liveliness between the OTI-S in tail (last waggon) and the OTI-M, head of the train. Product class 2 refers to trains equipped with wireless communication technology. In this case, the integrity is determined based on comparing kinematic data of train tail and front cabin (e.g., position,

speed, acceleration). For Product Class 3, where OTI-I modules are installed in each waggon, train integrity criterion consists in verifying separation distance between adjacent waggons. More details about the OTI-I specifications can be found in Deliverable 4.1 (2020).

On-Board Train Integrity specification process started with identifying use cases, performed a functional hazard analysis and then specified Finite State Machines (FSMs) that are formally verified (see Sassi et Al. (2021)). Identified use cases includes "OTI-I mastership and identification" in relation to the direction of the movement, "OTI-I system configuration" based on train composition after joining/splitting procedures, "train integrity monitoring" based on criteria for selected product class. OTI-I FSM has three high level states as depicted in Fig.2. The Mastership phase

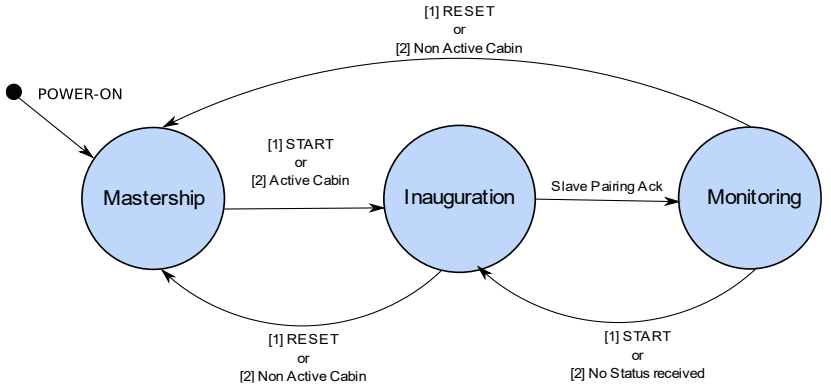

Fig.2. Finite State Machine of the OTI-I

consists in assigning the role to OTI device (i.e., Master role in leading locomotive with active cabin). Then second state manages with an inauguration process the OTI system configuration (e.g., pairing OTI Master with OTI Slave at train tail in Classes 1 and 2). Finally, third state addresses the train integrity monitoring in line with CR940 with three possible values: unknown (during initialization or while filtering false alarms), confirmed and loss. In some cases, OTI-I system can interact with Traffic Management System (TMS) (see Deliverable 6.1 (2020)) during the pairing procedure in product class 2 or during train composition determination in product class 3. Other applications include the possibility of embedding OTI-I within NG-TCMS or integrating OTI-I with Digital Automatic Coupler (DAC).

2.2. Train length determination (OTI-L)

Train length determination function is provided by an additional subsystem OTI-L, independent from OTI-I. The output of this function is needed at each start of mission (SoM) and after each change of the train composition (after joining and intentional splitting) to allow ETCS level 3 operation. OTI-I and OTI-L shall provide their output to ETCS onboard as depicted in Fig.3.

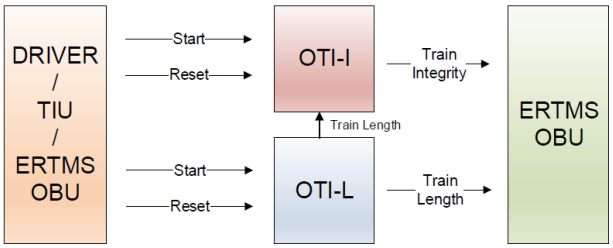

Fig. 3. Functional architecture of OTI-I and OTI-L

The ETCS onboard, Train Interface Unit (TIU) or the driver sends from its side to both systems, command messages of START and RESET to trigger or reconfigure the monitoring and evaluation procedures. Add to that, in case of

product class 2 or 3, to evaluate the train integrity status using the train length determined and provided by OTI-L, OTI-L must continuously provide this information as input to OTI-I. Note that the train length provided by OTI-L is required to ETCS level 3 operation for the calculation of the Safe train length. In addition, RBC assigns movement authorities based on train integrity status and safe train length determined at on-board level, without any trackside contribution (e.g., no axle counter neither track circuits). Therefore, on-board train integrity monitoring and on-board train length determination requires an appropriate safety target according to the analysis described in sections 3 and 4.

3. Safety requirements of OTI-I

The objective of this section is to define the safety target of the OTI-I and the results of the apportionment among its safety related functions: mastership, inauguration or train composition determination and monitoring. So, quantitative safety requirements in terms of THR are specified for the different OTI-I safety related functions.

3.1. Risk analysis and estimation

The OTI-I is considered as a safety function that is used to detect unintended train separation. So, the hazard related to a train accident "incorrect train integrity status information is leading to accident" is the consequence of hazard 1 related to train coupling failure "unintended train separation", and hazard 2 "OTI-I evaluates incorrectly the train integrity as confirmed" related to the failure of OTI-I to detect it. To define the safety target of the OTI-I, explicit risk estimation is chosen as risk acceptance principle (RAP) to determine the THR of "incorrect train integrity status information is leading to accident" as recommended in the CSM. Note that the failure of the OTI-I does not lead directly to accident that requires the simultaneous failure of the OTI-I and the train coupling. So, the considered technical system is a mix of E/E/PE, the OTI and the mechanical and/or pneumatic part which is related to the train coupling. The non-detection of the unintended train separation has the potential to lead to collision accident affecting a large number of people and there is a potential for multiple fatalities. According to CSM, the severity class that can be considered is "catastrophic". Thus, the tolerable hazard rate of 10^{-9} /h is allocated to the top hazard of "incorrect train integrity status information is leading to accident" which represents the event of misdetection of loss of integrity. Then, based on the Fault Tree analysis (FTA) depicted in Fig.4. THR_2 related to hazard 2 of the OTI-I is evaluated by apportioning the top event tolerable hazard rate THR_u according to equation 1 defined in the EN50126 standard. The apportioning of THR_u, in fault tree of Fig.4. starts with applying logical combinations of the functions through logical gate AND. The THR_u is apportioned based on equation 1 using an "AND" gate logic according to the standard EN50126:

$$THR_u = THR_1 \times SDT_1 \times THR_2 \times SDT_2 \times \left(\frac{1}{SDT_1} + \frac{1}{SDT_2}\right) = THR_1 \times THR_2 \times (SDT_1 + SDT_2) \quad (1)$$

Where THR_u is tolerable hazard rate for train integrity status information, THR_1 is tolerable hazard rate for train coupling, SDT_1 is Safe Down Time of train coupling defined as the detection time of the train decoupling by the OTI-I, THR_2 is tolerable hazard rate for OTI-I and SDT_2 is Safe Down Time for OTI-I that can be set as the testing period of this function.

The first step of the quantitative approach consists in determining THR_1 based on Infrastructure Managers (IMs) data about train separation events related to broken coupling or wrong adjusted draw hook. The numbers recorded in the period of the analysis include the known separation events reported in compliance with requirements of the appendix B of CENELEC standard EN50126, noting that "THR cannot be calculated from accident statistics unless rigorously collected statistics models are available". Based on the actual frequency of occurrence of unintended train separation, i.e., the accident and near miss statistics provided by DB, NR, SBB and OBB, THR_1 is calculated, per train, as follows:

$$THR_1(per\ train) = \frac{N_{TS}}{N_{unit} \times H \times N_{years}} \quad (2)$$

Where: N_{TS} is the number of dangerous failures i.e., trains separation that have occurred during the years of recording across the railway network, N_{unit} is the number of trains in the railway network to calculate the average hazardous failure rate per train, H is the number of train operational hours per year, N_{years} the number of years where the train separation events have been recorded.

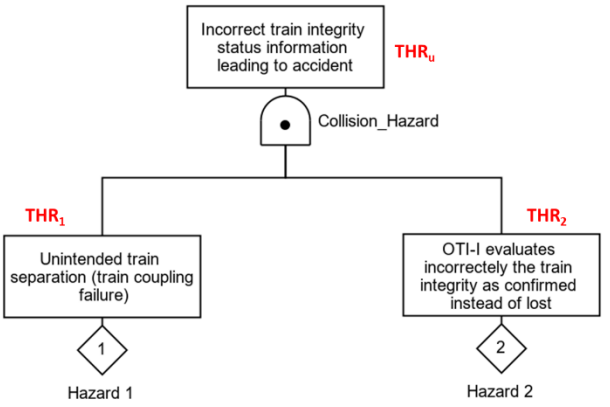

Fig. 4. Fault Tree of undetected unintended train separation

All the safety analysis concludes that the THR related to "unintended train separation" can be attributed for freight trains at around 2.16×10^{-5}/h and around 6.98×10^{-6}/h for passengers' trains. The preliminary results regarding the safety requirements of the OTI-I are shown in Table 1 assuming and considering that:

- All recorded unintended separation events are considered as potentially serious.
- OTI-I and train coupling shall be fully independent.
- Operational rules shall be defined to fix SDT values. SDT_1 (for train coupling) can be set to some seconds, the time needed to detect a loss of integrity and report it to RBC in case immediate actions are taken to reach a safe state after the train separation. SDT_2 can be set to the value of the testing period of the OTI-I.

The preliminary results regarding the safety requirements of the OTI-I are shown in Table 1 as follows, considering the higher SIL, SIL 2, to reduce the risk of unintended train separation guaranteeing the SIL 4 requirement at system level.

Table 1. OTI-I safety target possible values

SDT_1 (train coupling)	SDT_2 (OTI-I)	THR_2 (passengers train)	THR_2 (freight trains)	OTI-I SIL
Some seconds (e.g., 10 s)	1 h (hourly testing)	$3{,}82 \times 10^{-4}$/h	$1{,}42 \times 10^{-5}$/h	SIL 1
	10 h (at the end of every daily mission)	$3{,}83 \times 10^{-5}$/h	$1{,}43 \times 10^{-6}$/h	SIL 1
	24h (daily testing)	$1{,}59 \times 10^{-5}$/h	$5{,}96 \times 10^{-7}$/h	SIL 2
	30h (daily testing)	$1{,}28 \times 10^{-5}$/h	$5{,}00 \times 10^{-7}$/h	SIL 2

3.2. OTI-I safety analysis

The scope of the analysis is limited to the OTI-I safety analysis which shall satisfy SIL 2 requirements. The considered THR for the top event is evaluated between 10^{-7}/h and 10^{-6}/h. The top-event that must be taken into consideration is associated to the defined hazard OTI_HZ_002-1 as defined in Table 2. The proposed FTA of Fig.5. is limited to the functional level. This first level of THR allocation corresponding to this FT provides an overview of the approach to

be used to apportion the safety target among the safety related functions of the OTI-I: mastership, identification, pairing and monitoring.

Table 2. THR allocation values for OTI-I.

Fault Tree Base event	Description	Affected OTI Functions/data	Apportioned THR	Notes
HZ_OTI_002-1	OTI-M sends incorrect Train integrity information to ETCS (corrupted message): confirmed instead of lost or unknown	Monitoring function Data: train integrity status information	$6*10^{-7}$/h	
Triggering_event_hazards	Wrong start/reset command	Monitoring function Data: train integrity status information	10^{-9}/h	This event represents the triggering to the OTI reconfiguration modules following a change in train composition. It is a common input to both train integrity OTI-I and train length OTI-L. Therefore, the lower THR is considered.
OTI_HZ_010	OTI-M receives incorrect change of cabin status and becomes slave	Mastership: Input acquisition to determine the OTI module role (MASTER)	10^{-9}/h	For OTI_HZ_010, a wrong definition of the Master can result in giving wrong evaluation of the train integrity: the wrong OTI module can give corrupted data about train integrity unknown or confirmed instead of Lost.
OTI_HZ_014	Incorrect train composition: OTI Master considers an OTI Slave as TAIL when it is not. A waggon/car that belongs to a consist it is erroneously considered as not part of it. This function is equivalent to identification and pairing in class 1 and 2.	Identification and train composition: Identification of adjacent OTIs and sending of this information to OTI Master and Determination of train composition at OTI-M level	10^{-9}/h	These functions are common functions with train length determination function which is SIL 4. The defined THR is chosen according to the most constrained safety requirements. The function consisting in determining the train composition is performed at SoM. The discovered train composition, evaluated onboard, is compared to the planned one, provided by TMS at SoM.
OTI_HZ_MONITORING	Incorrect train integrity monitoring: confirmed instead of unknown or lost	Monitoring function: Train integrity status information	$6*10^{-7}$/h	
OTI_HZ_013	The OTI Master receives incorrect OTI Slave status ("coupled" instead of "separated") or does not receive the status from at least one OTI Slave	Monitoring function: Determination of the status (coupled or separated) and sending this information to OTI Master	$4*10^{-7}$/h	
OTI_HZ_013-1	OTI-M receives incorrect separation distance data at head of the train level	Monitoring function: Determination of the status (coupled or separated) and sending this information to OTI Master	$2*10^{-7}$/h	
HZ_001	The ERTMS/ETCS onboard does not receives Train length value by OTI-L or receives it late or uses a wrong value (less or greater than physical one)	Monitoring function: train length determination (if it is used in the evaluation of train integrity)	$3*10^{-9}$/h	The THR of this hazard is evaluated according to the FT results of the train length determination function in section 4.

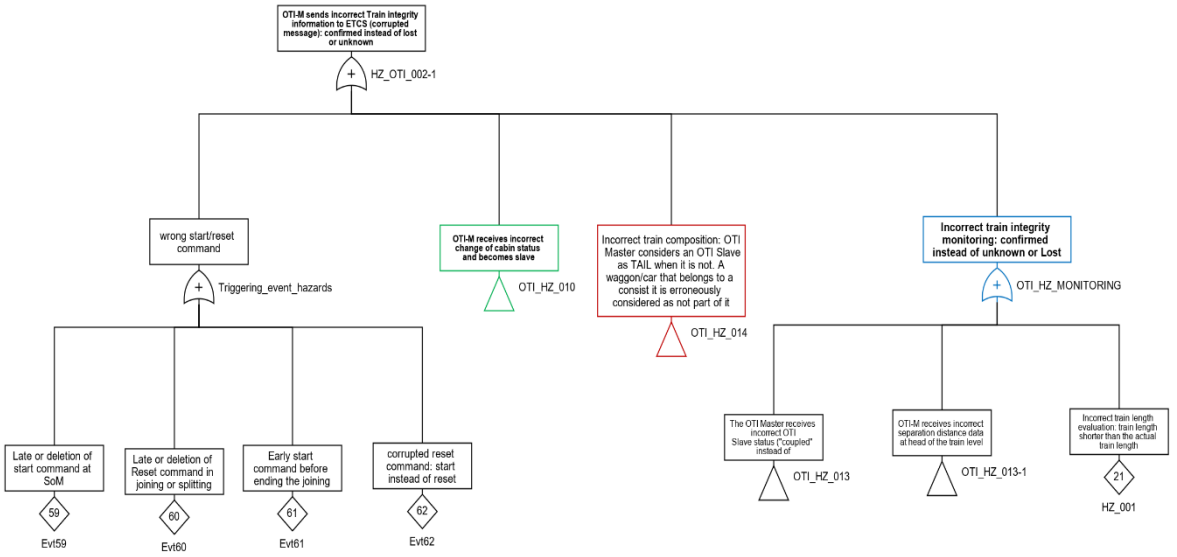

Fig. 5. Fault tree page 1 of OTI-I for product class 3

4. Safety requirements of OTI-L

Regarding OTI-L, the train length determination is SIL 4 function i.e., THR=3*10^{-9}/h. This value of THR is allocated to the identified top hazard HZ_001 "the ERTMS/ETCS On-board does not receive the Train Length value by OTI-L or receives it too late or uses a wrong value (less or greater than physical one)". In addition, the function titled determination of train composition is a common function between OTI-I product class 3 and OTI-L. Thus, hazard OTI_HZ_14 is evaluated based on the most constrained requirements in section 3. In the same way, hazard "*Triggering_event_hazards"* is evaluated by determining the most constrained requirements.

Table 3. THR allocation values for OTI-L.

Fault Tree Base event	Description	Affected OTI Functions/data	Apportioned THR	Notes
HZ_001	The ERTMS/ETCS onboard does not receives Train length value by OTI-L or receives it late or uses a wrong value (less or greater than physical one)	Train length determination	3*10^{-9}/h	Train length determination is a SIL 4 function
HZ_001_1	corruption hazard: Erroneous train length value: (less or greater than physical one)	Train length determination	0.33*10^{-9}/h	This THR value will be apportioned between an onboard function and another fully independent one implemented by TMS which is used for comparison.
HZ_001_2	deletion hazard: The ERTMS/ETCS does not receive the train length value	Train length determination	0.33*10^{-9}/h	Based on equiprobable apportionment
HZ_001_3	late hazard: The ERTMS/ETCS receives Train length value late	Train length determination	0.33*10^{-9}/h	Based on equiprobable apportionment

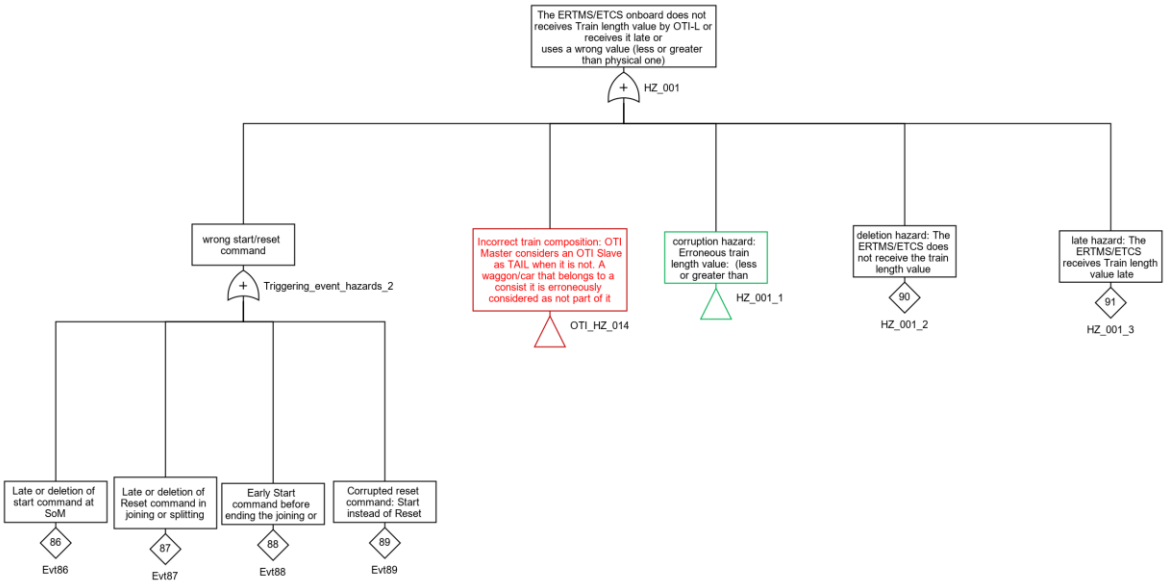

Fig. 6. Fault Tree page 1 for OTI-L

5. Conclusion and perspectives

This work proposes a methodology to specify the safety requirements of the new on-board solutions for train integrity monitoring and length determination in coherence with ETCS specification. Explicit risk estimation is conducted to quantify the safety targets of the OTI-L and OTI-I in terms of THR using field data related to unintended train separation. Three product classes are identified to address different technological constraints and to cover all railways applications. A safety analysis based on FTA is proposed to give preliminary results of the safety requirements of the functional modules contributing to both functions and product classes. This work represents a paramount step for the safety assessment to prepare the certification process.

Acknowledgements

This work is supported by the X2RAIL-4 project, part of the Shift2Rail Innovation Program 2. We would like to thank our X2RAIL-4 WP6-7 partners Alstom Transport Sa, AZD Praha Sro, Bombardier Transportation Sweden, CAF Signalling S.L., Ceit-IK4, Deutsche Bahn AG, Deutsches Zentrum Fuer Luft-Und Raumfahrt Ev, Hitachi RAIL STS SPA, INDRA SISTEMAS SA, IRT Railenium, Mermec Spa, Network Rail Infrastructure Limited, OBB-Infrastruktur AG, Siemens Aktiengesellschaft, SNCF RESEAU.

References

CENELEC, EN50126, 2017, Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety.

CR940, 2019, Minimum Safe Rear End position and position reporting ambiguities.

Deliverable 4.1, 2020, Train integrity concept and functional requirements specifications. Shift2Rail, X2RAIL-2 WP4 project.

Deliverable 6.1, 2020, System requirement Specification (SRS) for the Integration Layer. Shift2Rail, X2RAIL-2 WP6 project.

ERA, UNISIG, and EEIG-ERTMS-Users-Group, 2016, Ertms/etcs-system requirement specification-rev.3.6.0. SUBSET-026.

European-Commission, 2013, Common safety method for risk evaluation and assessment and repealing regulation (ec)352/2009, document regulation (eu) 402/2013, 30th commission implementing regulation.

Sassi, I., Ghazel, M., & El-Koursi, E. M. (2021). Formal modeling of a new On-board Train integrity System ETCS Compliant. In ESREL 2021, 31st European Safety and Reliability Conference (p. 9p).